



# CompTIA

## Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

## About ExamBible

### *Your Partner of IT Exam*

## Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

## Our Advances

### \* 99.9% Uptime

All examinations will be up to date.

### \* 24/7 Quality Support

We will provide service round the clock.

### \* 100% Pass Rate

Our guarantee that you will pass the exam.

### \* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

#### NEW QUESTION 1

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 manager/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 2

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

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

**Answer: B**

#### NEW QUESTION 3

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 4

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: A**

#### NEW QUESTION 5

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

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

**Answer: C**

#### NEW QUESTION 6

A penetration tester wants to perform reconnaissance without being detected. Which of the following activities have a MINIMAL chance of detection? (Choose two.)

- A. Open-source research
- B. A ping sweep
- C. Traffic sniffing
- D. Port knocking
- E. A vulnerability scan
- F. An Nmap scan

**Answer: AC**

#### NEW QUESTION 7

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 8

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 9

A new security firm is onboarding its first client. The client only allowed testing over the weekend and needed the results Monday morning. However, the assessment team was not able to access the environment as expected until Monday. Which of the following should the security company have acquired BEFORE the start of the assessment?

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

**Answer: B**

#### NEW QUESTION 10

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 10

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 15

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

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

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

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

**Answer: C**

#### NEW QUESTION 16

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 17

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**

#### NEW QUESTION 21

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

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

**Answer: D**

#### NEW QUESTION 22

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 26

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

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**

#### NEW QUESTION 30

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 34

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 38

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

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

**Answer: A**

#### NEW QUESTION 40

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 44

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 47

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 50

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

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

**Answer:** A

#### NEW QUESTION 53

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 56

A penetration tester conducts an Nmap scan against a target and receives the following results:

```
Port      State  Service
1080/tcp  open  socks
```

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?

- A. Nessus
- B. ProxyChains
- C. OWASPZAP
- D. Empire

**Answer:** B

#### NEW QUESTION 57

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

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

**Answer:** D

#### Explanation:

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

#### NEW QUESTION 58

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:** A

#### NEW QUESTION 60

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 65

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 69

A software development team is concerned that a new product's 64-bit Windows binaries can be deconstructed to the underlying code. Which of the following tools can a penetration tester utilize to help the team gauge what an attacker might see in the binaries?

- A. Immunity Debugger
- B. OllyDbg
- C. GDB
- D. Drozer

**Answer:** B

#### NEW QUESTION 74

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

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

**Answer:** B

#### NEW QUESTION 75

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 79

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

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

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

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

**Answer:** C

**NEW QUESTION 82**

A penetration tester found the following valid URL while doing a manual assessment of a web application: <http://www.example.com/product.php?id=123987>. Which of the following automated tools would be best to use NEXT to try to identify a vulnerability in this URL?

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

**Answer: B**

**NEW QUESTION 83**

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 85**

A penetration tester performs the following command: `curl -I -http2 https://www.comptia.org`  
 Which of the following snippets of output will the tester MOST likely receive?

- A. 

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

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

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

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

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

**Answer: A**

**NEW QUESTION 88**

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 89**

.....

## Relate Links

**100% Pass Your PT0-002 Exam with ExamBible Prep Materials**

<https://www.exambible.com/PT0-002-exam/>

## Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>