

DUMPS ARENA

CompTIA PenTest+ Certification Exam

CompTIA PT0-002

Version Demo

Total Demo Questions: 15

Total Premium Questions: 278

Buy Premium PDF

<https://dumpsarena.co>

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

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: B D

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.

QUESTION NO: 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

ANSWER: A B**Explanation:**

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 NO: 3

Which of the following concepts defines the specific set of steps and approaches that are conducted during a penetration test?

- A. Scope details
- B. Findings
- C. Methodology
- D. Statement of work

ANSWER: C

QUESTION NO: 4 - (DRAG DROP)

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.



ANSWER:

QUESTION NO: 5

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

QUESTION NO: 6

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

QUESTION NO: 7

A penetration tester is testing a new API for the company's existing services and is preparing the following script:

```
#!/bin/bash
for each in GET POST PUT TRACE CONNECT OPTIONS;
do
printf "Seach / HTTP/1.1\nHost:www.comptia.org\r\n\r\n" | nc www.comptia.org 80
```

Which of the following would the test discover?

- A. Default web configurations
- B. Open web ports on a host
- C. Supported HTTP methods
- D. Listening web servers in a domain

ANSWER: C

QUESTION NO: 8

A penetration tester downloaded a Java application file from a compromised web server and identifies how to invoke it by looking at the following log:

```
17:34:23 - F - Info: New connection established :8443
17:34:23 - F - User: bmarney
17:34:23 - F - PW length 15
17:34:23 - F - login exec (/www/app/jre/bin/java -cp ./commapp.jar approval 192.168.0.1 bmarney
17:34:23 - F - login rc:0
```

Which of the following is the order of steps the penetration tester needs to follow to validate whether the Java application uses encryption over sockets?

- A. Run an application vulnerability scan and then identify the TCP ports used by the application.
- B. Run the application attached to a debugger and then review the application's log.
- C. Disassemble the binary code and then identify the break points.
- D. Start a packet capture with Wireshark and then run the application.

ANSWER: D

QUESTION NO: 9

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

QUESTION NO: 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	NMAP Scan Output
Using the output, identify potential attack vectors that should be further investigated.	<pre>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</pre>
<input type="checkbox"/> Weak SMB file permissions	
<input type="checkbox"/> FTP anonymous login	
<input type="checkbox"/> Webdav file upload	
<input type="checkbox"/> Weak Apache Tomcat Credentials	
<input type="checkbox"/> Null session enumeration	
<input type="checkbox"/> Fragmentation attack	
<input type="checkbox"/> SNMP enumeration	
<input type="checkbox"/> ARP spoofing	

ANSWER: See explanation below.

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-os-and-services-running-on-a-target-host>

QUESTION NO: 11

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: A F

QUESTION NO: 12

Which of the following describe the GREATEST concerns about using third-party open-source libraries in application code? (Choose two.)

- A. The libraries may be vulnerable
- B. The licensing of software is ambiguous
- C. The libraries' code bases could be read by anyone
- D. The provenance of code is unknown
- E. The libraries may be unsupported
- F. The libraries may break the application

ANSWER: A C

Explanation:

Reference: <https://www.infosecurity-magazine.com/opinions/third-party-libraries-the-swiss/>

QUESTION NO: 13

Given the following script:

```
Line 1 #!/usr/bin/python3
Line 2 from scapy.all import *
Line 3 IP(dst='10.10.10.10')/UDP(dport=53)/DNS(rd=1,qd=DNSQR(qname='www.comptia.org'))
Line 4 b = srl(a, verbose=0)
Line 5 for x in range(b[DNS].count):
Line 6     print(b[DNSRR][x].rdata
```

Which of the following BEST characterizes the function performed by lines 5 and 6?

- A. Retrieves the start-of-authority information for the zone on DNS server 10.10.10.10
- B. Performs a single DNS query for www.comptia.org and prints the raw data output
- C. Loops through variable b to count the results returned for the DNS query and prints that count to screen

D. Prints each DNS query result already stored in variable b

ANSWER: D

QUESTION NO: 14

A penetration tester is preparing to perform activities for a client that requires minimal disruption to company operations. Which of the following are considered passive reconnaissance tools? (Choose two.)

- A. Wireshark
- B. Nessus
- C. Retina
- D. Burp Suite
- E. Shodan
- F. Nikto

ANSWER: A E

Explanation:

Reference: <https://resources.infosecinstitute.com/topic/top-10-network-recon-tools/>

QUESTION NO: 15

Which of the following types of information would MOST likely be included in an application security assessment report addressed to developers? (Choose two.)

- A. Use of non-optimized sort functions
- B. Poor input sanitization
- C. Null pointer dereferences
- D. Non-compliance with code style guide
- E. Use of deprecated Javadoc tags
- F. A cyclomatic complexity score of 3

ANSWER: B C