



# CompTIA

## Exam Questions PT0-002

CompTIA PenTest+ Certification Exam

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

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

**Answer:** AC

#### NEW QUESTION 3

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 4

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 5

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

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

**Answer:** B

#### NEW QUESTION 6

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 7

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 8

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 9

A penetration tester was brute forcing an internal web server and ran a command that produced the following output:

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 10

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 10

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 15

A penetration tester has gained access to a network device that has a previously unknown IP range on an interface. Further research determines this is an always-on VPN tunnel to a third-party supplier.

Which of the following is the BEST action for the penetration tester to take?

- A. Utilize the tunnel as a means of pivoting to other internal devices.
- B. Disregard the IP range, as it is out of scope.
- C. Stop the assessment and inform the emergency contact.
- D. Scan the IP range for additional systems to exploit.

**Answer:** D

#### NEW QUESTION 18

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 20

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 23

A penetration tester runs a scan against a server and obtains the following output: 21/tcp open ftp Microsoft ftpd

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

| 03-12-20 09:23AM 331 index.aspx

| ftp-syst:

135/tcp open msrpc Microsoft Windows RPC

139/tcp open netbios-ssn Microsoft Windows netbios-ssn 445/tcp open microsoft-ds Microsoft Windows Server 2012 Std 3389/tcp open ssl/ms-wbt-server

| rdp-ntlm-info:

| Target Name: WEB3

| NetBIOS\_Computer\_Name: WEB3

| Product\_Version: 6.3.9600

|\_ System\_Time: 2021-01-15T11:32:06+00:00

8443/tcp open http Microsoft IIS httpd 8.5

| http-methods:

|\_ Potentially risky methods: TRACE

|\_ http-server-header: Microsoft-IIS/8.5

|\_ http-title: IIS Windows Server

Which of the following command sequences should the penetration tester try NEXT?

- A. ftp 192.168.53.23
- B. smbclient \\\\WEB3\\IPC\$ -I 192.168.53.23 -U guest
- C. ncrack -u Administrator -P 15worst\_passwords.txt -p rdp 192.168.53.23
- D. curl -X TRACE https://192.168.53.23:8443/index.aspx
- E. nmap --script vuln -sV 192.168.53.23

**Answer: A**

#### NEW QUESTION 28

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 32

A company that requires minimal disruption to its daily activities needs a penetration tester to perform information gathering around the company's web presence. Which of the following would the tester find MOST helpful in the initial information-gathering steps? (Choose two.)

- A. IP addresses and subdomains
- B. Zone transfers
- C. DNS forward and reverse lookups
- D. Internet search engines
- E. Externally facing open ports
- F. Shodan results

**Answer: AB**

#### NEW QUESTION 33

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 38

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

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

**Answer:** D

**NEW QUESTION 43**

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 48**

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 52**

During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

**INSTRUCTIONS**

Analyze the code segments to determine which sections are needed to complete a port scanning script. Drag the appropriate elements into the correct locations to complete the script.

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

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

A picture containing shape Description automatically generated

A picture containing treemap chart Description automatically generated

Text Description automatically generated

Graphical user interface Description automatically generated

#### NEW QUESTION 57

A penetration tester received a .pcap file to look for credentials to use in an engagement. Which of the following tools should the tester utilize to open and read the .pcap file?

- A. Nmap
- B. Wireshark
- C. Metasploit
- D. Netcat

**Answer: B**

#### NEW QUESTION 59

A security engineer identified a new server on the network and wants to scan the host to determine if it is running an approved version of Linux and a patched version of Apache. Which of the following commands will accomplish this task?

- A. nmap -f -sV -p80 192.168.1.20
- B. nmap -sS -sL -p80 192.168.1.20
- C. nmap -A -T4 -p80 192.168.1.20
- D. nmap -O -v -p80 192.168.1.20

**Answer: C**

#### NEW QUESTION 61

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 64

A consulting company is completing the ROE during scoping. Which of the following should be included in the ROE?

- A. Cost of the assessment
- B. Report distribution
- C. Testing restrictions
- D. Liability

**Answer: B**

#### NEW QUESTION 69

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

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

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

**Answer: B**

#### NEW QUESTION 73

A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?

- A. Manually check the version number of the VoIP service against the CVE release
- B. Test with proof-of-concept code from an exploit database
- C. Review SIP traffic from an on-path position to look for indicators of compromise
- D. Utilize an nmap -sV scan against the service

**Answer: D**

#### NEW QUESTION 74

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 79**

A penetration tester was able to gather MD5 hashes from a server and crack the hashes easily with rainbow tables. Which of the following should be included as a recommendation in the remediation report?

- A. Stronger algorithmic requirements
- B. Access controls on the server
- C. Encryption on the user passwords
- D. A patch management program

**Answer: C**

**NEW QUESTION 83**

You are a penetration tester reviewing a client's website through a web browser. INSTRUCTIONS  
Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate, source, or cookies.  
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Graphical user interface Description automatically generated

**NEW QUESTION 86**

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 90**

A red-team tester has been contracted to emulate the threat posed by a malicious insider on a company's network, with the constrained objective of gaining access to sensitive personnel files. During the assessment, the red-team tester identifies an artifact indicating possible prior compromise within the target environment.

Which of the following actions should the tester take?

- A. Perform forensic analysis to isolate the means of compromise and determine attribution.
- B. Incorporate the newly identified method of compromise into the red team's approach.
- C. Create a detailed document of findings before continuing with the assessment.
- D. Halt the assessment and follow the reporting procedures as outlined in the contract.

Answer: C

#### NEW QUESTION 91

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

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 96

A penetration tester was able to gain access successfully to a Windows workstation on a mobile client's laptop. Which of the following can be used to ensure the tester is able to maintain access to the system?

- A. `schtasks /create /sc /ONSTART /tr C:\Temp\WindowsUpdate.exe`
- B. `wmic startup get caption,command`
- C. `crontab -l; echo "@reboot sleep 200 && ncat -lvp 4242 -e /bin/bash" | crontab 2>/dev/null`
- D. `sudo useradd -ou 0 -g 0 user`

Answer: B

#### NEW QUESTION 101

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 102

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 105

A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial data. Which of the following should the tester do with this information to make this a successful exploit?

- A. Perform XSS.
- B. Conduct a watering-hole attack.
- C. Use BeEF.
- D. Use browser autopwn.

Answer: A

#### NEW QUESTION 109

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 110**

.....

## Thank You for Trying Our Product

### We offer two products:

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

2nd - Questions 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 First Try
- \* PT0-002 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

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