CompTIA PenTest+ PT0-003 Practice Questions

Shared by Shields on 13-08-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A penetration tester writes a Bash script to automate the execution of a ping command on a Class C network:

bash

for var in ---MISSING TEXT---

do

ping -c 1 192.168.10.$var

done

Which of the following pieces of code should the penetration tester use in place of the ---MISSING TEXT--- placeholder?

Options:

A- crunch 1 254 loop
B- seq 1 254
C- echo 1-254
D- {1.-254}

Answer:

B

Explanation:

Correct Syntax for a Range Loop in Bash:

The seq command generates a sequence of numbers in a specified range, which is ideal for iterating over IP addresses in a Class C subnet (1--254).

Example: seq 1 254 will output numbers 1, 2, ..., 254 sequentially.

Explanation of Other Options:

A (crunch): The crunch command is used for wordlist generation and is unrelated to looping in Bash.

C (echo 1-254): This would output '1-254' as a string instead of generating a numeric range.

D ({1.-254}): This is incorrect Bash syntax and would result in a script error.

Final Script:

bash

for var in $(seq 1 254)

do

ping -c 1 192.168.10.$var

done

CompTIA Pentest+ Reference:

Domain 4.0 (Penetration Testing Tools)

Bash Scripting and Automation

Question 2

Question Type: MultipleChoice

A penetration tester exports the following CSV data from a scanner. The tester wants to parse the data using Bash and input it into another tool.

CSV data before parsing:

cat data.csv

Host, IP, Username, Password

WINS212, 10.111.41.74, admin, Spring11

HRDB, 10.13.9.212, hradmin, HRForTheWin

WAS01, 192.168.23.13, admin, Snowfall97

Intended output:

admin Spring11

hradmin HRForTheWin

admin Snowfall97

Which option best will provide the intended output?

Options:

A- cat data.csv | grep -v 'IP' | cut -d',' -f 3,4 | sed -e 's/,/ /'
B- cat data.csv | find . -iname Username,Password
C- cat data.csv | grep 'username|Password'
D- cat data.csv | grep -i 'admin' | grep -v 'WINS212\|HRDB\|WAS01\|10.111.41.74\|10.13.9.212\|192.168.23.13'

Answer:

A

Explanation:

Option A correctly performs the standard Bash text-processing sequence PenTest+ expects testers to use when transforming scan output into tool-ready input. First, grep -v 'IP' removes the header line by excluding the row containing ''IP'' (the CSV header includes ''Host, IP, Username, Password''). Next, cut -d',' -f 3,4 splits each remaining line on commas and selects fields 3 and 4, which correspond to Username and Password in the exported format. Finally, sed -e 's/,/ /' replaces the remaining comma between those two fields with a space, producing the intended two-column output suitable for piping into password auditing, spraying, or validation tooling.

The other choices do not correctly parse CSV columns: find searches filenames, not CSV content; the grep expression in C does not extract fields and would only match lines; and D attempts to filter text by excluding hostnames/IPs rather than selecting the required columns. This makes A the only option that reliably yields ''username password'' per line from the CSV.

Question 3

Question Type: MultipleChoice

A penetration tester would like to collect permission details for objects within the domain. The tester has a valid AD user and access to an internal PC. Which of the following sets of steps is the best way for the tester to accomplish the desired outcome?

Options:

A- Escalate privileges.Execute Rubeus.Run a Cypher query on Rubeus to get the results.
B- Run SharpHound.Install CrackMapExec.Perform a CrackMapExec database query on CME to get the results.
C- Run SharpHoundInstall BloodHoundPerform a Cypher query on BloodHound to get the results.

D- Escalate privileges.Get Windows Registry data.Perform a query to get results.

Answer:

C

Explanation:

To collect permission details for objects within an Active Directory domain, the PenTest+ workflow most closely aligns with using SharpHound (the BloodHound data collector) followed by BloodHound analysis. SharpHound is executed from a domain-joined or internally reachable system using a valid AD account to enumerate domain relationships, including group membership, sessions, local admin rights, and---most importantly for this question---object control and ACL-based permissions (for example, rights that allow modifying users, resetting passwords, adding group members, or controlling GPOs). BloodHound then imports this collected graph data and allows the tester to run Cypher queries to identify effective privileges, abuse paths, and misconfigurations that enable privilege escalation or lateral movement.

Rubeus is primarily focused on Kerberos ticket operations (TGT/TGS manipulation, roasting, delegation abuse) and is not a Cypher-query permission-mapping platform. CrackMapExec supports network/AD operations, but it is not the standard toolchain for graph-based permission path analysis described in PenTest+. Registry collection is unrelated to enumerating domain object permissions.

Question 4

Question Type: MultipleChoice

A penetration tester is performing network reconnaissance. The tester wants to gather information about the network without causing detection mechanisms to flag the reconnaissance activities. Which option best techniques should the tester use?

Options:

A- Sniffing
B- Banner grabbing
C- TCP/UDP scanning
D- Ping sweeps

Answer:

A

Explanation:

To gather information about the network without causing detection mechanisms to flag the reconnaissance activities, the penetration tester should use sniffing.

Sniffing:

Definition: Sniffing involves capturing and analyzing network traffic passing through the network. It is a passive reconnaissance technique that does not generate detectable traffic on the network.

Tools: Tools like Wireshark and tcpdump are commonly used for sniffing. They capture packets and provide insights into network communications, protocols in use, devices, and potential vulnerabilities.

Advantages:

Stealthy: Since sniffing is passive, it does not generate additional traffic that could be detected by intrusion detection systems (IDS) or other monitoring tools.

Information Gathered: Sniffing can reveal IP addresses, MAC addresses, open ports, running services, and potentially sensitive information transmitted in plaintext.

Comparison with Other Techniques:

Banner Grabbing: Active technique that sends requests to a target service to gather information from banners, which can be detected.

TCP/UDP Scanning: Active technique that sends packets to probe open ports and services, easily detected by network monitoring tools.

Ping Sweeps: Active technique that sends ICMP echo requests to determine live hosts, also detectable by network monitoring.

Pentest Reference:

Reconnaissance Phase: Using passive techniques like sniffing during the initial reconnaissance phase helps gather information without alerting the target.

Network Analysis: Understanding the network topology and identifying key assets and vulnerabilities without generating traffic that could trigger alarms.

By using sniffing, the penetration tester can gather detailed information about the network in a stealthy manner, minimizing the risk of detection.

======

Question 5

Question Type: MultipleChoice

A penetration tester wants to send a specific network packet with custom flags and sequence numbers to a vulnerable target. Which of the following should the tester use?

Options:

A- tcprelay
B- Bluecrack
C- Scapy
D- tcpdump

Answer:

C

Explanation:

Scapy is a powerful interactive Python-based packet manipulation tool used by penetration testers to create, modify, send, and analyze custom packets. It supports many protocols and allows you to set TCP flags, sequence numbers, and more.

tcprelay is used to redirect TCP traffic, not to craft packets.

Bluecrack is used for cracking Bluetooth encryption, irrelevant in this context.

tcpdump is a packet capture tool, not suitable for crafting or injecting packets.

Question 6

Question Type: MultipleChoice

During an assessment, a penetration tester plans to gather metadata from various online files, including pictures. Which option best standards outlines the formats for pictures, audio, and additional tags that facilitate this type of reconnaissance?

Options:

A- EXIF
B- GIF
C- COFF
D- ELF

Answer:

A

Explanation:

Metadata extraction allows attackers to collect sensitive information from digital files.

EXIF (Exchangeable Image File Format) (Option A):

EXIF metadata contains camera details, GPS coordinates, timestamps, and software versions used to edit the file.

Attackers use tools like ExifTool to extract metadata for reconnaissance.

Incorrect options:

Option B (GIF): A file format for images, but not a metadata standard.

Option C (COFF): Common Object File Format, related to executable files, not images.

Option D (ELF): Executable and Linkable Format, used for Linux binaries, not metadata analysis.

Question 7

Question Type: MultipleChoice

During an assessment, a penetration tester runs the following command:

dnscmd.exe /config /serverlevelplugindll C:\users\necad-TA\Documents\adduser.dll

Which option best is the penetration tester trying to achieve?

Options:

A- DNS enumeration
B- Privilege escalation

C- Command injection
D- A list of available users

Answer:

B

Explanation:

The tester is attempting to register a malicious DLL as a server-level plugin to escalate privileges.

Privilege escalation (Option B):

The command uses dnscmd.exe, a legitimate Windows tool for managing DNS servers.

By setting a malicious DLL (adduser.dll) as a server-level plugin, attackers can gain SYSTEM-level privileges.

This technique is a DLL hijacking attack.

Incorrect options:

Option A (DNS enumeration): The command modifies DNS settings rather than querying them.

Option C (Command injection): The attacker is not injecting arbitrary shell commands.

Option D (List of users): The command does not retrieve user information.et unauthorized access to

Question 8

Question Type: MultipleChoice

A penetration tester wants to create a malicious QR code to assist with a physical security assessment. Which of the following tools has the built-in functionality most likely needed for this task?

Options:

A- BeEF
B- John the Ripper
C- ZAP

D- Evilginx

Answer:

A

Explanation:

BeEF (Browser Exploitation Framework) is a penetration testing tool that focuses on web browsers. It has built-in functionality for generating malicious QR codes, which can be used to direct users to malicious websites, execute browser-based attacks, or gather information.

Understanding BeEF:

Purpose: BeEF is designed to exploit vulnerabilities in web browsers and gather information from compromised browsers.

Features: Includes tools for generating malicious payloads, QR codes, and social engineering techniques.

Creating Malicious QR Codes:

Functionality: BeEF has a feature to generate QR codes that, when scanned, redirect the user to a malicious URL controlled by the attacker.

Command: Generate a QR code that directs to a BeEF hook URL.

Step-by-Step Explanationbeef -x --qr

Usage in Physical Security Assessments:

Deployment: Place QR codes in strategic locations to test whether individuals scan them and subsequently compromise their browsers.

Exploitation: Once scanned, the QR code can lead to browser exploitation, information gathering, or other payload execution.

Reference from Pentesting Literature:

BeEF is commonly discussed in penetration testing guides for its browser exploitation capabilities.

HTB write-ups and social engineering exercises often mention the use of BeEF for creating malicious QR codes and exploiting browser vulnerabilities.

Penetration Testing - A Hands-on Introduction to Hacking

HTB Official Writeups

======

Question 9

Question Type: MultipleChoice

A penetration tester has adversely affected a critical system during an engagement, which could have a material impact on the organization. Which option best should the penetration tester do to address this issue?

Options:

A- Restore the configuration.
B- Perform a BIA.
C- Follow the escalation process.
D- Select the target.

Answer:

C

Explanation:

If a penetration tester unintentionally disrupts a critical system, they must immediately follow the client's escalation process to ensure proper handling.

Follow the escalation process (Option C):

The penetration testing engagement follows a predefined incident response and escalation plan.

The tester documents the issue, informs stakeholders, and works with IT teams to minimize impact.

Incorrect options:

Option A (Restore the configuration): Unauthorized changes could violate the engagement scope.

Option B (Perform a BIA): Business Impact Analysis (BIA) is for risk management, not an immediate response.

Option D (Select the target): The target was already chosen; this option is irrelevant.