PassQueen
a.k.a dumpsqueen.com

CompTIA PenTest+ Exam

CompTIA PT0-003

Version Demo

Total Demo Questions: 56

Total Premium Questions: 561

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Engagement Management	26
Topic 2, Reconnaissance and Enumeration	143
Topic 3, Vulnerability Discovery and Analysis	78
Topic 4, Attacks and Exploits	183
Topic 5, Post-exploitation and Lateral Movement	89
Topic 6, Reporting and Communication	42
Total	561

QUESTION NO: 1

A penetration tester conducts OSINT for a client and discovers the robots.txt file explicitly blocks a major search engine. Which of the following would most likely help the penetration tester achieve the objective?

A. Modifying the WAF

B. Utilizing a CSRF attack

C. Changing the robots.txt file

D. Leveraging a competing provider

ANSWER: D

Explanation:

Leveraging a competing provider is correct because OSINT relies on collecting information from publicly available sources without modifying the target environment. A `robots.txt` file communicates crawler preferences to specific web crawlers, including directives that can prevent a particular search engine from indexing all or portions of a site. If the file blocks one major search engine, another search engine may use a different crawler and may not be subject to the same user-agent-specific directive. It may also have previously indexed material, cached content, or distinct data sources that provide useful reconnaissance findings.

Using multiple search engines and public data providers is a practical reconnaissance approach because each provider has different crawling schedules, indexes, cache behavior, and search syntax. The tester can continue looking for exposed documents, subdomains, archived URLs, usernames, metadata, and other passive intelligence while staying within the authorized scope and preserving the non-intrusive nature of OSINT. The Robots Exclusion Protocol is a voluntary crawler-control standard rather than an access-control mechanism, as described by RFC 9309. Google also documents that robots rules are crawler-specific and control crawling behavior, supporting the use of alternative public search sources where authorized: Google Search Central: Introduction to robots.txt.

QUESTION NO: 2

[Post-Engagement Activities]

At the end of an authorized penetration test, a tester must perform cleanup on systems where temporary access was established. Which of the following actions should be completed? (Select two).

A. Remove test accounts and temporary credentials.

B. Remove uploaded tools and persistence mechanisms.

C. Leave a backdoor for future retesting.

D. Delete the client's security logs.

E. Retain collected client data indefinitely.

ANSWER: A B

Explanation:

The tester should **remove test accounts and temporary credentials** and **remove uploaded tools and persistence mechanisms**. Temporary accounts, API keys, SSH keys, scheduled tasks, services, and uploaded utilities can create an unnecessary security exposure if they remain after the engagement. Removing them restores the environment to the agreed state and prevents unintended future access.

Cleanup should also be verified and recorded. The tester should confirm that assessment artifacts are no longer present, any configuration changes are reverted where required, and client data is handled according to the engagement's retention and destruction requirements. NIST identifies restoration and cleanup as important activities following security testing in NIST SP 800-115. The Penetration Testing Execution Standard also discusses post-exploitation and cleanup considerations.

QUESTION NO: 3

A penetration tester enumerates a legacy Windows host on the same subnet. The tester needs to select exploit methods that will have the least impact on the host ' s operating stability. Which of the following commands should the tester try first?

A. responder -I eth0 john responder_output.txt < rdp to target >

B. hydra -L administrator -P /path/to/pwlist.txt -t 100 rdp:// < target_host >

C. msf > use < module_name > msf > set < options > msf > set PAYLOAD windows/meterpreter/reverse_tcp msf > run

D. python3 ./buffer_overflow_with_shellcode.py < target > 445

ANSWER: A

Explanation:

The command sequence beginning with `responder -I eth0` is the best first choice because it primarily performs network-based name-resolution poisoning and credential capture rather than attempting to execute code, alter memory, or heavily authenticate against the legacy host. Responder listens for protocols such as LLMNR, NBT-NS, and mDNS on the selected interface and can answer requests in a way that causes a client to attempt NTLM authentication. Any captured challenge-response material can then be assessed offline, which minimizes additional interaction with the target and helps preserve host availability and stability during an authorized engagement.

This approach aligns with a cautious penetration-testing workflow: gather evidence and potential credentials through the least invasive feasible technique before considering actions that directly engage a service or operating-system process. Although Responder's responses are an active network action and must be explicitly authorized in the rules of engagement, it does not inherently require deploying an exploit payload to the legacy Windows system. The Responder project documents its supported poisoning and credential-capture functions at Responder on GitHub. MITRE ATT&CK also documents LLMNR/NBT-NS poisoning as an adversary-in-the-middle credential-access technique at T1557.001.

QUESTION NO: 4

During a vulnerability assessment, a penetration tester configures the scanner sensor and performs the initial vulnerability scanning under the client's internal network. The tester later discusses the results with the client, but the client does not accept the results. The client indicates the host and assets that were within scope are not included in the vulnerability scan results. Which of the following should the tester have done?

A. Rechecked the scanner configuration.

B. Performed a discovery scan.

C. Used a different scan engine.

D. Configured all the TCP ports on the scan.

ANSWER: B

Explanation:

Performed a discovery scan. is correct because asset discovery is a necessary validation step before conducting a full vulnerability assessment. The tester must first identify reachable, live hosts and compare the discovered asset inventory against the client-approved scope. This establishes that the scanner sensor has network visibility to the intended systems and that the targets' addresses, routes, VLANs, and relevant network segments are represented in the scan target list.

A discovery scan commonly uses techniques such as ARP requests on local networks, ICMP probes, and limited TCP or UDP probing to determine which systems are active. The resulting host list allows the tester and client to reconcile discrepancies before deeper vulnerability checks begin. This is particularly important for internal assessments, where segmentation, filtering, isolated subnets, and incomplete target inventories can prevent a scanner from seeing otherwise in-scope assets.

Performing discovery first supports accurate scoping, reduces the chance of reporting incomplete results, and provides an opportunity to resolve visibility issues while the assessment is underway. Nmap documents host discovery methods at Nmap Host Discovery, and Tenable discusses the importance of asset discovery at Active vs. Passive Network Discovery.

QUESTION NO: 5 - (HOTSPOT)

HOTSPOT

[Attacks and Exploits]

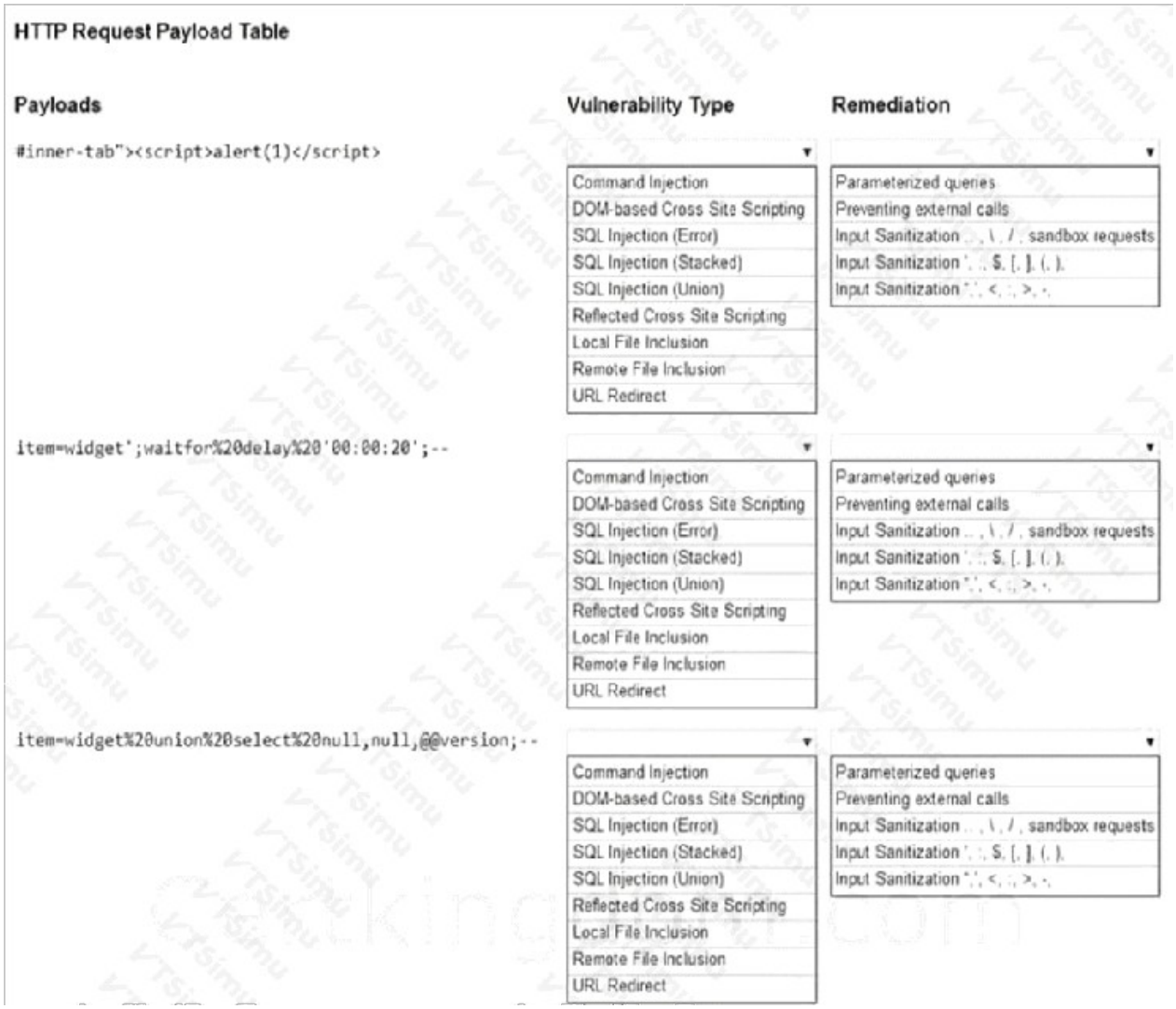
You are a security analyst tasked with hardening a web server.

You have been given a list of HTTP payloads that were flagged as malicious.

INSTRUCTIONS

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

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



ANSWER:



Explanation:

The payload beginning with `#inner-tab` and containing `<script>alert(1)</script>` is DOM-based cross-site scripting because the hash fragment is interpreted within the browser's document environment. JavaScript that reads a URL fragment and places it into the page without safe handling can turn that fragment into executable markup. The appropriate remediation is input sanitization of HTML-sensitive characters, particularly characters such as < and >, together with context-aware output encoding before untrusted data is inserted into the DOM. OWASP describes DOM XSS as client-side code processing attacker-controlled data into an unsafe sink and recommends safe DOM APIs and context-appropriate encoding: OWASP DOM-based XSS Prevention Cheat Sheet.

The `waitfor delay` payload appends a separate SQL action after ending the original value, making it a stacked SQL injection attempt. Parameterized queries keep user input separate from the SQL command structure, so supplied text remains data instead of becoming executable SQL. The `union select` payload is a union SQL injection attempt because it tries to combine query output with database version information. Parameterized queries are also the correct control for this pattern, since bound parameters prevent injected query operators, clauses, and expressions from changing the intended statement. OWASP recommends prepared statements with parameterized queries as a primary SQL injection defense: OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 6

A penetration tester writes the following script to enumerate a network:

1 #!/bin/bash

2 for i in {1..254}

3 ping -c1 192.168.1.$i

4 done

The tester executes the script, but it fails with the following error:

-bash: syntax error near unexpected token 'ping'

Which of the following should the tester do to fix the error?

A. Add do after line 2

B. Replace {1..254} with $(seq 1 254)

C. Replace bash with zsh

D. Replace $i with ${i}

ANSWER: A

Explanation:

Add do after line 2 is correct because Bash requires the `do` reserved word to begin the command body of a `for` loop. The loop declaration supplies the variable and the list of values, but it does not itself establish where the commands to repeat begin. In this script, Bash parses `for i in {1..254}` and then expects `do`; instead, it encounters `ping`, producing the reported syntax error. The corrected structure is `for i in {1..254}; do` followed by `ping -c1 192.168.1.$i` and closed with `done`. Alternatively, `do` can be placed on its own line immediately after the loop declaration. Bash supports brace expansion, so `{1..254}` supplies the intended sequence of host-number values in a Bash script. Each iteration assigns one value to `i`, allowing the command to probe addresses from `192.168.1.1` through `192.168.1.254`. The Bash Reference Manual defines the required `for ... [;] do ... done` syntax under looping constructs: GNU Bash Manual: Looping Constructs. Its brace-expansion behavior is also documented by GNU: GNU Bash Manual: Brace Expansion.

QUESTION NO: 7

A penetration tester presents the following findings to stakeholders:

Control | Number of findings | Risk | Notes

Encryption | 1 | Low | Weak algorithm noted

Patching | 8 | Medium | Unsupported systems

System hardening | 2 | Low | Baseline drift observed

Secure SDLC | 10 | High | Libraries have vulnerabilities

Password policy | 0 | Low | No exceptions noted

Based on the findings, which of the following recommendations should the tester make? (Select two).

A. Develop a secure encryption algorithm.

B. Deploy an asset management system.

C. Write an SDLC policy.

D. Implement an SCA tool.

E. Obtain the latest library version.

F. Patch the libraries.

ANSWER: D E

Explanation:

The appropriate recommendations are **Implement an SCA tool.** and **Obtain the latest library version.** The most significant issue is the Secure SDLC finding category because it has the highest number of findings and is assigned high risk. The stated condition, vulnerable libraries, indicates exposure introduced through third-party, open-source, or otherwise externally maintained software components used by the application.

Software composition analysis (SCA) provides ongoing visibility into an application's dependency inventory. It can identify component versions, map them to publicly disclosed vulnerabilities, alert development teams when new issues affect existing dependencies, and support governance of approved components. This makes SCA an effective control improvement for preventing recurrence throughout the development lifecycle.

Obtaining the latest library version addresses the immediate remediation need by moving affected dependencies to vendor-supported versions that contain security fixes. Updates should be evaluated and tested through the organization's normal build, compatibility, and release processes before deployment. Together, continuous dependency identification through SCA and timely adoption of supported library versions reduce the likelihood that known vulnerable components remain in production. OWASP describes dependency analysis at OWASP Component Analysis and recommends maintaining supported, up-to-date components at OWASP: Vulnerable and Outdated Components.

QUESTION NO: 8

During an engagement, a penetration tester wants to enumerate users from Linux systems by using finger and rwho commands. However, the tester realizes these commands alone will not achieve the desired result. Which of the following is the best tool to use for this task?

A. Nikto

B. Burp Suite

C. smbclient

D. theHarvester

ANSWER: C

Explanation:

`smbclient` is the best choice because it is a command-line client for interacting with SMB/CIFS services, including Samba services commonly deployed on Linux and UNIX hosts. In a penetration test, SMB enumeration can reveal information useful for identifying users and accounts when a target exposes Samba file-sharing or related SMB services. For example, a tester can connect to an accessible SMB server, list available shared resources, authenticate with authorized test credentials where applicable, and gather service information that helps map the system's users and access model. This makes it a practical complementary enumeration utility when the legacy Finger and rwho mechanisms do not provide sufficient results.

The approach also reflects a core PenTest+ principle: select enumeration tooling based on the services actually exposed by the target rather than relying on one protocol or command. SMB remains relevant in mixed Windows/Linux enterprise environments because Samba implements SMB network services on Linux systems. The `smbclient` manual documents its use for accessing SMB servers and listing available services, while Samba's documentation describes its role in providing file and print services to SMB clients. See the Samba smbclient manual and Samba documentation.

QUESTION NO: 9

In a file stored in an unprotected source code repository, a penetration tester discovers the following line of code:

sshpass -p donotchange ssh admin@192.168.6.14

Which of the following should the tester attempt to do next to take advantage of this information? (Select two).

A. Use Nmap to identify all the SSH systems active on the network.

B. Take a screen capture of the source code repository for documentation purposes.

C. Investigate to find whether other files containing embedded passwords are in the code repository.

D. Confirm whether the server 192.168.6.14 is up by sending ICMP probes.

E. Run a password-spraying attack with Hydra against all the SSH servers.

F. Use an external exploit through Metasploit to compromise host 192.168.6.14.

ANSWER: B C

Explanation:

“Take a screen capture of the source code repository for documentation purposes.” is appropriate because the exposed SSH password is a reportable credential-management finding. Capturing the relevant code, repository location, and surrounding context preserves evidence of the condition as observed. This evidence supports accurate reporting, validation with the engagement stakeholders, and remediation such as revoking the exposed credential, removing it from repository history, and adopting secure secret storage. Penetration-test reporting should communicate findings clearly and provide evidence that enables the client to reproduce and correct the issue.

“Investigate to find whether other files containing embedded passwords are in the code repository.” is also appropriate because one hard-coded credential is a strong indicator that additional secrets may have been committed. Within the authorized assessment scope, the tester should review the repository and its relevant history for similar embedded SSH credentials, API keys, tokens, connection strings, and private keys. A systematic secret search increases the completeness of the assessment and helps establish the extent of credential exposure. OWASP recommends keeping secrets out of source code and using appropriate secret-management controls; its guidance is available in the OWASP Secrets Management Cheat Sheet. Secure coding practices related to exposed credentials are also covered by CWE-798: Use of Hard-coded Credentials.

QUESTION NO: 10

While performing a penetration testing exercise, a tester executes the following command:

bash

Copy code

PS c:\tools > c:\hacks\PsExec.exe \\server01.comptia.org -accepteula cmd.exe

Which of the following best explains what the tester is trying to do?

A. Test connectivity using PSExec on the server01 using CMD.exe.

B. Perform a lateral movement attack using PsExec.

C. Send the PsExec binary file to the server01 using CMD.exe.

D. Enable CMD.exe on the server01 through PsExec.

ANSWER: B

Explanation:

Perform a lateral movement attack using PsExec is correct. PsExec is a Sysinternals utility designed to execute a process on a remote Windows computer. In this command, `\\server01.comptia.org` identifies the remote target, `-accepteula` accepts the PsExec license agreement without prompting, and `cmd.exe` is the process the tester wants PsExec to start on that target. If the tester has credentials with the necessary administrative privileges on the remote host, this provides remote command execution through a Windows command shell.

During an authorized penetration test, remote command execution on another host represents lateral movement: the tester is using access obtained in one context to operate on an additional system in the environment. PsExec commonly uses administrative shares and the Service Control Manager to deploy and run its service component remotely, making it a well-known technique for administering systems as well as for post-compromise movement. Microsoft documents PsExec as a tool for executing processes on remote computers: PsExec - Sysinternals. This activity also aligns with MITRE ATT&CK’s Remote Services technique, including SMB/Windows Admin Shares: T1021.002.

QUESTION NO: 11

A penetration tester performs the following scan:

nmap -sU -p 53,161,162 192.168.1.51

PORT | STATE

53/udp | open|filtered

161/udp | open|filtered

162/udp | open|filtered

The tester then manually uses snmpwalk against port 161 and receives valid SNMP responses. Which of the following best explains the scan result for port 161?

A. The SNMP daemon delayed its response beyond Nmap's UDP scan timeout.

B. Nmap marked the port as open|filtered because no response was received.

C. The scanned host applied rate limiting to its responses to prevent UDP fingerprinting.

D. The Nmap scan lacked root privileges, which reduced packet inspection accuracy.

ANSWER: B

Explanation:

Nmap marked the port as open|filtered because no response was received. UDP does not use a connection handshake comparable to TCP's three-way handshake, so determining a UDP port's state often depends on the response to a probe. When Nmap receives an ICMP "port unreachable" message, it can identify the port as closed. Conversely, when it receives a UDP response from the target application, it can identify the port as open. If neither response arrives, Nmap cannot distinguish between a service that is listening but does not answer that particular probe and a firewall or filtering device silently discarding the traffic. It therefore reports the indeterminate `open|filtered` state.

The successful `snmpwalk` result establishes that UDP port 161 is in fact open and that the SNMP service accepts the properly constructed SNMP request and credentials or community string used by the tester. That later validation does not conflict with the earlier scan result: Nmap's initial UDP probe simply did not elicit a reply that allowed it to conclusively classify the port. Nmap documents this UDP scan behavior and the meaning of the `open|filtered` state at Nmap Network Scanning: UDP Scan and Nmap Port Scanning Basics.

QUESTION NO: 12

[Planning and Scoping]

A client authorizes a penetration test of its public web application but does not authorize testing against third-party payment services integrated into the application. Which of the following actions should the tester take? (Select two).

A. Exclude the third-party payment endpoints from active testing.

B. Document the limitation in the scope and final report.

C. Test the payment provider because it is linked from the client application.

D. Conduct denial-of-service testing against the payment API.

E. Use discovered payment credentials to validate the provider environment.

ANSWER: A B

Explanation:

The tester should **exclude the third-party payment endpoints from active testing** and **document the limitation in the scope and final report**. Authorization is limited to the systems and services explicitly identified by the client. Even if a third-party endpoint is accessible through the client application, testing it without written authorization from the service owner could exceed the agreed scope.

Documenting the exclusion provides transparency about the assessment boundary and helps stakeholders understand that the payment integration was not technically assessed. If testing is needed, the client should obtain approval from the third-party provider or arrange for an authorized assessment through the provider's established process. NIST emphasizes defining authorized targets and test limitations before beginning an assessment in NIST SP 800-115. The Penetration Testing Execution Standard Rules of Engagement also addresses defining scope and authorization boundaries.

QUESTION NO: 13

[Reporting and Communication]

A penetration tester is documenting a critical finding involving unrestricted access to a cloud storage bucket. Which of the following should be included in the detailed finding? (Select two).

A. Evidence that demonstrates unauthorized access

B. Specific remediation guidance

C. The tester's complete password wordlist

D. Unredacted contents of all exposed customer files

E. A list of unrelated low-risk findings

ANSWER: A B

Explanation:

The detailed finding should include **evidence that demonstrates unauthorized access** and **specific remediation guidance**. Evidence allows technical stakeholders to validate the issue and understand the scope of exposure. For a cloud storage finding, appropriate evidence might include the affected bucket identifier, the tested access method, the permissions observed, and sanitized proof that an unauthorized principal could list or retrieve an approved test object.

Specific remediation guidance gives the client a practical path to reduce risk. This may include removing public access, applying least-privilege identity policies, reviewing access-control lists, enabling logging, and validating the revised configuration after remediation. Detailed findings should also communicate impact and affected assets, but they should avoid including unnecessary sensitive data or full contents of exposed files. NIST describes documenting findings, evidence, and recommendations in NIST SP 800-115. AWS provides guidance for restricting public S3 access at Blocking public access to Amazon S3 storage.

QUESTION NO: 14

The following file was obtained during reconnaissance:

```
# adduser.conf
DSHELL=/bin/zsh
DHOME=/home
GROUPHOMES=no
LETTERHOMES=no
SKEL=/etc/systemd-conf/temp-skeleton
FIRST_SYSTEM_UID=100
LAST_SYSTEM_UID=999
FIRST_SYSTEM_GID=100
LAST_SYSTEM_GID=999
FIRST_UID=1000
LAST_UID=2999
FIRST_GID=1000
LAST_GID=2499
USERGROUPS=yes
USERS_GID=100
DIR_MODE=0777
SETGID_HOME=no
QUOTAUSER=""
SKEL_IGNORE_REGEX="dpkg-(old|new|dist|save)"
```

Which of the following is most likely to be successful if a penetration tester achieves non-privileged user access?

A. Exposure of other users' sensitive data

B. Unauthorized access to execute binaries via sudo

C. Hijacking the default user login shells

D. Corrupting the skeleton configuration file

ANSWER: A

Explanation:

Exposure of other users' sensitive data is the most likely successful outcome because the reconnaissance file specifies `DIR_MODE=0777`. In Linux account-creation configuration, `DIR_MODE` defines the permission mode used when a new user's home directory is created. A mode of `0777` grants read, write, and search/execute permissions to the owner, group, and all other local users. Therefore, after obtaining any ordinary account, a penetration tester could traverse other users' home directories, enumerate their contents, and access files that have not been separately restricted. The write permission also creates a serious integrity risk, since a user could alter or place files in another user's home directory.

Directory permissions are particularly important: read permission permits listing directory entries, while execute (search) permission permits accessing objects within the directory when their names are known. With both permissions available to every user, private home-directory data is no longer protected by the directory boundary that normally isolates user content. Actual access to an individual file can still depend on that file's own permissions or access-control lists, but the globally permissive home-directory mode makes sensitive-data discovery and exposure highly feasible. The `login.defs` documentation describes `DIR_MODE`, and Linux permission behavior is documented in the login.defs manual and the chmod manual.

QUESTION NO: 15

A penetration testing team wants to conduct DNS lookups for a set of targets provided by the client. The team crafts a Bash script for this task. However, they find a minor error in one line of the script:

1 #!/bin/bash

2 for i in $(cat example.txt); do

3 curl $i

4 done

Which of the following changes should the team make to line 3 of the script?

A. resolvconf $i

B. rndc $i

C. systemd-resolve $i

D. host $i

ANSWER: D

Explanation:

`host $i` is the appropriate replacement because the script's stated purpose is to perform DNS lookups on each target listed in `example.txt`. During each loop iteration, the variable `$i` contains one target value, such as a hostname or domain. The `host` command accepts that value as its argument and queries DNS to return relevant records, commonly including address records and authoritative-name-server information. This makes it suitable for lightweight, repeatable DNS enumeration in a penetration-testing workflow. For example, if a line contains `www.example.com`, the command runs as `host www.example.com` and displays the DNS resolution results. The loop therefore applies the same lookup consistently to every supplied target without manually entering each name. The `host` utility is part of the BIND DNS tools and supports querying specific record types and alternate DNS servers when additional investigation is authorized. Its standard usage and query behavior are documented in the BIND 9 host manual page. DNS reconnaissance is also a recognized information-gathering activity; see the CISA overview of DNS for background on DNS's role in resolving domain names to network information.

QUESTION NO: 16

Which of the following is the most likely LOLBin to be used to perform an exfiltration on a Microsoft Windows environment?

A. procdump.exe

B. msbuild.exe

C. bitsadmin.exe

D. cscript.exe

ANSWER: C

Explanation:

bitsadmin.exe is the best answer because it is a native command-line interface for the Background Intelligent Transfer Service (BITS), which supports moving files between a Windows host and a remote server using HTTP or HTTPS. In particular, BITS supports upload jobs, allowing a local file to be transferred to a remote destination. This makes it directly applicable to exfiltration: an operator can stage collected data locally and use a BITS job to send that data outside the environment through commonly permitted web protocols.

BITS was designed for reliable background transfers, including retry behavior and asynchronous operation, characteristics that can make a transfer less conspicuous than a newly introduced third-party file-transfer utility. Its legitimate administrative and operating-system role also makes it a classic living-off-the-land technique when it is present on the target Windows version. Microsoft documents the `bitsadmin transfer` command and its upload capability, while MITRE ATT&CK identifies BITS jobs as a technique that can be abused to transfer files and communicate with remote infrastructure. See Microsoft's Bitsadmin transfer documentation and MITRE ATT&CK: BITS Jobs.

QUESTION NO: 17

[Attacks and Exploits]

During a discussion of a penetration test final report, the consultant shows the following payload used to attack a system:

html

Copy code

7/aLeRt('pwned')

Based on the code, which of the following options represents the attack executed by the tester and the associated countermeasure?

A. Arbitrary code execution: the affected computer should be placed on a perimeter network

B. SQL injection attack: should be detected and prevented by a web application firewall

C. Cross-site request forgery: should be detected and prevented by a firewall

D. XSS obfuscated: should be prevented by input sanitization

ANSWER: D

Explanation:

XSS obfuscated: should be prevented by input sanitization is the correct answer. The payload is intended to inject JavaScript into web content so that a victim's browser executes `alert('pwned')`. This is characteristic of cross-site scripting (XSS), in which attacker-controlled input reaches an HTML or JavaScript rendering context without being safely handled. The mixed capitalization in `aLeRt` and the altered script-tag spelling reflect attempts to evade simplistic, signature-based filtering that may only search for exact strings. Such tests help a penetration tester demonstrate whether an application can be induced to interpret supplied data as active client-side code.

Effective XSS prevention starts with context-appropriate output encoding: untrusted values must be encoded for the specific HTML, attribute, JavaScript, URL, or CSS context in which they are rendered. Input validation and sanitization are also important defense-in-depth controls, especially where limited HTML is intentionally accepted. Secure frameworks and templating engines should retain automatic escaping, and a restrictive Content Security Policy can reduce impact if an injection defect remains. OWASP describes XSS and its prevention guidance at OWASP Cross Site Scripting and OWASP Cross Site Scripting Prevention Cheat Sheet.

QUESTION NO: 18

[Attacks and Exploits]

Which of the following technologies is most likely used with badge cloning? (Select two).

A. NFC

B. RFID

C. Bluetooth

D. Modbus

E. Zigbee

F. CAN bus

ANSWER: A B

Explanation:

Badge cloning concerns duplicating the credential data carried by a physical access-control badge so that a second card, fob, or compatible emulator can present the same identifier or credential to a reader. RFID is a core technology used by

many proximity-card systems. These systems use radio-frequency tags and readers, and insecure or legacy implementations may expose a static card identifier that can be captured and copied to suitable media. RFID therefore directly applies to common badge-cloning assessments.

NFC is also used with tap-based credentials, particularly in modern high-frequency badge deployments and mobile-access implementations. NFC operates at very short range and is based on the same high-frequency radio ecosystem used by contactless smart cards. Where the credential design permits reading, emulation, or duplication, an assessor may use NFC-capable tools to evaluate whether the badge can be cloned or replayed. The exact feasibility depends on the card type, cryptographic protections, reader configuration, and whether credentials use diversified keys or dynamic authentication rather than a static identifier.

For background on RFID-based identification systems, see NIST's Guide to RFID Security. The NFC Forum also describes NFC technology and its contactless communication model at What is NFC?.

QUESTION NO: 19

[Attacks and Exploits]

A client recently hired a penetration testing firm to conduct an assessment of their consumer-facing web application. Several days into the assessment, the clients networking team observes a substantial increase in DNS traffic. Which of the following would most likely explain the increase in DNS traffic?

A. Covert data exfiltration

B. URL spidering

C. HTML scraping

D. DoS attack

ANSWER: A

Explanation:

Covert data exfiltration is the most likely explanation because a penetration tester can use DNS tunneling to transfer collected data through DNS requests. In this technique, data is encoded into DNS query labels, commonly appearing as a high volume of unusually long or randomized subdomain requests sent to a domain controlled by the tester. The authoritative DNS server for that domain can receive, reconstruct, and decode the embedded information. This produces a conspicuous increase in DNS traffic even when the assessed application itself is not receiving an equivalent increase in normal web requests.

DNS is a useful channel when validating egress controls because organizations commonly permit DNS resolution through internal resolvers and perimeter devices. A test may therefore use DNS-based transfer to demonstrate whether outbound DNS is restricted to approved resolvers, inspected for anomalous query patterns, and monitored for excessive query rates or high-entropy labels. MITRE ATT&CK identifies this behavior as application-layer protocol use over DNS and notes that adversaries may encode and transmit data in DNS traffic: MITRE ATT&CK: DNS. CISA also describes DNS tunneling as a method that can bypass conventional controls and enable data exfiltration: CISA: DNS Tunneling.

QUESTION NO: 20

A penetration tester is evaluating a company ' s cybersecurity preparedness. The tester wants to acquire valid credentials using a social engineering campaign. Which of the following tools and techniques are most applicable in this scenario? (Select two).

A. TruffleHog for collecting credentials

B. Shodan for identifying potential targets

C. Gophish for sending phishing emails

D. Maltego for organizing targets

E. theHarvester for discovering additional targets

F. Evilginx for handling legitimate authentication requests through a proxy

ANSWER: C F

Explanation:

Gophish for sending phishing emails and **Evilginx for handling legitimate authentication requests through a proxy** are the most applicable choices for an authorized social-engineering assessment intended to obtain valid credentials. Gophish is purpose-built for conducting controlled phishing simulations: a tester can create email templates, target groups, sending profiles, landing pages, and campaign tracking. Its reporting helps measure whether recipients opened messages, followed links, and submitted test data, providing evidence of user-awareness and email-security control effectiveness. The project documentation describes these phishing-campaign management capabilities in detail: GoPhish Documentation.

Evilginx is an adversary-in-the-middle reverse-proxy framework that can relay a target's authentication interaction to a legitimate service while capturing credentials and session-related authentication artifacts during an approved engagement. This makes it relevant when the assessment scope includes evaluating resilience to modern credential-phishing techniques, including scenarios involving multifactor authentication and session cookies. Use requires explicit authorization, carefully defined rules of engagement, secure handling of any collected data, and prompt cleanup after testing. Its implementation and stated reverse-proxy phishing functionality are documented at Evilginx GitHub repository.

QUESTION NO: 21

[Attacks and Exploits]

A penetration tester gains initial access to a target system by exploiting a recent RCE vulnerability. The patch for the vulnerability will be deployed at the end of the week. Which of the following utilities would allow the tester to reenter the system remotely after the patch has been deployed? (Select two).

A. schtasks.exe

B. rundll.exe

C. cmd.exe

D. chgusr.exe

E. sc.exe

F. netsh.exe

ANSWER: A E

Explanation:

schtasks.exe and **sc.exe** support authorized post-exploitation persistence on Windows. A scheduled task created with **schtasks.exe** can be configured to run a permitted assessment payload at system startup, user logon, or on a recurring schedule. If that payload is configured to communicate back to the tester's authorized infrastructure, it provides a means of regaining remote access that does not depend on the original remote-code-execution flaw remaining unpatched. Scheduled tasks can also be configured to execute under a specified account, subject to the tester's privileges and the engagement's rules of engagement.

sc.exe is the Windows Service Controller command-line utility. With sufficient privileges, it can create and configure a service that starts automatically during system boot. A service runs independently of an interactive user session and can launch an approved remote-management or callback component after restarts. Because both techniques establish execution mechanisms on the target itself, deploying the patch for the initial access vulnerability does not remove those mechanisms. In a legitimate penetration test, creating either mechanism must be explicitly authorized, documented, monitored, and removed during cleanup. Microsoft documents scheduled-task management at schtasks and Windows service control at sc.

QUESTION NO: 22

[Information Gathering and Vulnerability Scanning]

A penetration tester is conducting an authenticated vulnerability scan of Windows servers. The scan completes successfully, but the results contain only network-service findings and do not include installed patches or local configuration details. Which of the following should the tester verify? (Select two).

A. The scan account has local administrative privileges.

B. The required remote-management service is accessible.

C. The servers allow anonymous FTP access.

D. The scanner uses UDP port 53 for all checks.

E. The client has disabled DNSSEC validation.

ANSWER: A B

Explanation:

The tester should verify that the **scan account has local administrative privileges** and that the **required remote-management service is accessible**. Authenticated scanning requires the scanner to establish a permitted remote session and collect local information from the target. On Windows systems, local administrative privileges are commonly required to enumerate installed updates, registry settings, local policy, and other configuration data needed for accurate credentialed checks.

The relevant remote-management path must also be available. Depending on the scanner configuration, this can include SMB, Windows Management Instrumentation, or WinRM. If a firewall blocks the selected protocol or the service is unavailable, the scanner may reach the host over the network but cannot perform local authenticated checks. Microsoft documents remote management through Windows Remote Management and Windows Management Instrumentation. NIST also discusses authenticated scanning considerations in NIST SP 800-115.

QUESTION NO: 23

Which of the following are valid reasons for including base, temporal, and environmental CVSS metrics in the findings section of a penetration testing report? (Select two).

A. Providing details on how to remediate vulnerabilities

B. Helping to prioritize remediation based on threat context

C. Including links to the proof-of-concept exploit itself

D. Providing information on attack complexity and vector

E. Prioritizing compliance information needed for an audit

F. Adding risk levels to each asset

ANSWER: B D

Explanation:

Helping to prioritize remediation based on threat context is correct because CVSS is designed to provide a consistent severity assessment that can be refined for the organization receiving the report. Base metrics establish the vulnerability's intrinsic technical characteristics, while temporal metrics account for changing conditions such as exploit-code maturity, remediation level, and report confidence. Environmental metrics then tailor the score to the affected organization's security requirements and modified impact or exploitability considerations. Presenting these metrics helps stakeholders make informed, risk-based remediation decisions rather than treating every finding with the same urgency.

Providing information on attack complexity and vector is correct because these are explicit CVSS Base metric elements. Attack Vector describes the context required to exploit the vulnerability, such as network, adjacent, local, or physical access. Attack Complexity communicates whether conditions beyond the attacker's control must exist for exploitation. Including this information in a penetration-testing finding gives technical and business stakeholders meaningful context about how exposure may occur and supports accurate severity communication. CVSS documentation defines the metric groups and their intended use in vulnerability assessment and prioritization. See FIRST CVSS Specification Document and FIRST CVSS User Guide.

QUESTION NO: 24

As part of a security audit, a penetration tester finds an internal application that accepts unexpected user inputs, leading to the execution of arbitrary commands. Which of the following techniques would the penetration tester most likely use to access the sensitive data?

A. Logic bomb

B. SQL injection

C. Brute-force attack

D. Cross-site scripting

E. Command injection

ANSWER: E

Explanation:

Command injection is the most appropriate technique because the defining condition in the scenario is that attacker-controlled input causes the application or underlying host to execute arbitrary commands. A penetration tester would validate this condition in an authorized, controlled manner by determining whether input reaches an operating-system command interpreter or an unsafe command-execution function without effective input validation, allowlisting, or parameterization. Once command execution is established, the tester may be able to run commands in the security context of the affected application, enumerate accessible files and services, and retrieve sensitive data that the application account is permitted to read. This is commonly categorized as OS command injection (CWE-78), in which externally influenced input is improperly incorporated into an OS command. The essential distinction is the execution of system commands, rather than manipulation of a database query. Findings should be documented with the minimal proof necessary, including the affected input, execution context, data exposure impact, and remediation guidance such as avoiding shell invocation, using safe APIs with fixed arguments, and applying strict server-side allowlists. OWASP describes command injection risks and defenses in its Command Injection resource, while MITRE's CWE-78 entry defines improper neutralization of special elements used in an OS command.

QUESTION NO: 25

[Reporting and Communication]

Which of the following are valid reasons for including base, temporal, and environmental CVSS metrics in the findings section of a penetration testing report? (Select two).

A. Providing details on how to remediate vulnerabilities

B. Helping to prioritize remediation based on threat context

C. Including links to the proof-of-concept exploit itself

D. Providing information on attack complexity and vector

E. Prioritizing compliance information needed for an audit

F. Adding risk levels to each asset

ANSWER: B D

Explanation:

Helping to prioritize remediation based on threat context is a valid reason because CVSS combines different types of information that support risk-based decision-making. Base metrics establish the intrinsic technical characteristics of a vulnerability, while temporal metrics account for factors that change over time, such as exploit maturity or remediation availability. Environmental metrics then tailor the assessment to the organization's deployment, security requirements, and potential impact. Together, these metrics give report readers a consistent basis for ranking findings and directing remediation effort toward the issues posing the greatest practical risk in that environment.

Providing information on attack complexity and vector is also valid because these are core CVSS Base metric elements. Attack Vector identifies the access path required to exploit a vulnerability, such as network, adjacent, local, or physical access. Attack Complexity communicates whether conditions beyond the attacker's control must be present for successful exploitation. Including these details in a finding helps stakeholders understand the vulnerability's technical exposure and exploitability characteristics, supporting an accurate interpretation of its severity. The CVSS specification defines these metric groups and their intended use in communicating vulnerability severity consistently. See the FIRST CVSS Specification Document and the NIST National Vulnerability Database CVSS guidance.

QUESTION NO: 26

A penetration tester is researching a path to escalate privileges. While enumerating current user privileges, the tester observes the following:

SeAssignPrimaryTokenPrivilege Disabled

SeIncreaseQuotaPrivilege Disabled

SeChangeNotifyPrivilege Enabled

SeManageVolumePrivilege Enabled

SeImpersonatePrivilege Enabled

SeCreateGlobalPrivilege Enabled

SeIncreaseWorkingSetPrivilege Disabled

Which of the following privileges should the tester use to achieve the goal?

A. SeImpersonatePrivilege

B. SeCreateGlobalPrivilege

C. SeChangeNotifyPrivilege

D. SeManageVolumePrivilege

ANSWER: A

Explanation:

`SeImpersonatePrivilege` is the appropriate enabled privilege for pursuing Windows privilege escalation through token impersonation. Windows access tokens define a security context, including the account identity, group memberships, and privileges under which a process or thread acts. This privilege permits a process to impersonate the security token of a client after authentication, allowing an attacker who controls a suitably positioned service or process to potentially execute actions in the context of a more privileged account. In authorized testing, this condition is commonly investigated for named-pipe or COM-based impersonation paths, often referred to as "Potato"-family techniques, subject to the Windows version, service configuration, token type, and available high-privilege client interaction.

Microsoft documents this user right as allowing processes to impersonate the security context of a client. Its API documentation also notes that impersonation enables a thread to adopt a client token for access checks and subsequent operations. Therefore, the presence of `SeImpersonatePrivilege` in an enabled state provides the most directly relevant privilege-escalation avenue among the enumerated rights. This aligns with MITRE ATT&CK's token-impersonation

technique, which covers adversarial abuse of access tokens to operate under another user's context. See Microsoft's Windows security documentation and MITRE ATT&CK: Access Token Manipulation.

QUESTION NO: 27

[Attacks and Exploits]

A penetration tester is assessing a wireless network and captures an authentication exchange when a client joins a WPA2-Personal network. Which of the following can the tester attempt offline to validate the strength of the wireless password?

A. Offline dictionary attack against the captured handshake

B. ARP cache poisoning

C. DNS zone transfer

D. Kerberoasting

ANSWER: A

Explanation:

An **offline dictionary attack against the captured handshake** is correct. In WPA2-Personal networks, a captured authentication exchange can be used to test password candidates offline. The tester derives values from each candidate passphrase and compares the result with the captured exchange. A matching value demonstrates that the candidate is the network passphrase.

This approach differs from repeatedly attempting to authenticate to the wireless access point, because the validation occurs against the captured data rather than requiring a new association attempt for every password guess. During an authorized assessment, the tester should use an approved wordlist, observe wireless-testing restrictions, and document only the evidence necessary to demonstrate password strength risk. NIST provides wireless security guidance in SP 800-153, Guidelines for Securing Wireless Local Area Networks.

QUESTION NO: 28

Which of the following best describes the importance of including the attack steps in a penetration test report?

A. It easily provides the recommended mitigations.

B. It ensures results can be independently verified.

C. It proves the penetration tester's competency to the customer.

D. It demonstrates the difficulty of exploiting specific vulnerabilities in the kill chain.

ANSWER: B

Explanation:

It ensures results can be independently verified. Including clear attack steps documents the reproducible path used to validate a finding: the relevant preconditions, actions performed, tools or commands used where appropriate, observed outputs, and evidence demonstrating impact. This enables the client's technical staff, auditors, or a subsequent assessor to confirm that the reported issue exists and to understand the conditions under which it was successfully exploited. Reproducible steps also support efficient remediation validation, because the organization can repeat the documented procedure after applying a fix to determine whether the vulnerability has actually been resolved. In a penetration test report, this technical evidence connects the finding to a defensible conclusion about risk and impact, rather than leaving the result as an unsupported assertion. CompTIA's PenTest+ objectives emphasize communicating findings through reports and providing appropriate remediation guidance, which depends on accurate documentation of test results and supporting evidence. The NIST Technical Guide to Information Security Testing likewise identifies documentation and reporting as essential test activities, with results recorded so they can be analyzed, communicated, and acted upon. See the CompTIA exam objectives page and NIST SP 800-115.

QUESTION NO: 29

During a testing engagement, a penetration tester compromises a host and locates data for exfiltration. Which of the following are the best options to move the data without triggering a data loss prevention tool? (Select two).

A. Move the data using a USB flash drive.

B. Compress and encrypt the data.

C. Rename the file name extensions.

D. Use FTP for exfiltration.

E. Encode the data as Base64.

F. Send the data to a commonly trusted service.

ANSWER: B E

Explanation:

“Compress and encrypt the data.” and “Encode the data as Base64.” are the intended techniques because they transform collected content before transfer, potentially reducing detection by controls that depend on recognizable file contents, sensitive-data patterns, or simple signatures. Archiving first also consolidates numerous files into a smaller number of objects, while encryption makes the archive contents unavailable to an inspection engine unless the organization has access to the decryption material and performs appropriate encrypted-traffic or endpoint inspection. MITRE ATT&CK identifies archiving collected data, including encryption of archives, as a technique used to prepare data for exfiltration. See MITRE ATT&CK: Archive Collected Data.

“Encode the data as Base64.” converts binary data into text characters. In an authorized penetration test, this demonstrates whether a defensive control can normalize encoded material and apply content inspection after decoding. MITRE identifies encoding as a data-obfuscation approach that can alter a payload’s apparent representation during transfer. See MITRE ATT&CK: Data Encoding. These techniques should be performed only when explicitly authorized in the engagement scope and with safeguards for handling client data.

QUESTION NO: 30

[Information Gathering and Vulnerability Scanning]

A penetration tester receives a vulnerability-scanner finding that an internet-facing server supports TLS 1.0. Which of the following actions should the tester take to validate the finding before reporting it? (Select two).

A. Attempt a TLS connection that explicitly offers TLS 1.0.

B. Review the negotiated protocol and cipher details.

C. Assume the scanner result is sufficient without validation.

D. Disable TLS on the production server.

E. Perform password spraying against the service.

ANSWER: A B

Explanation:

Attempting a TLS connection that explicitly offers TLS 1.0 is an appropriate validation step because it confirms whether the service will actually negotiate the deprecated protocol version. A scanner finding can be affected by a stale banner, a load balancer, or an incomplete handshake, so direct protocol validation improves report accuracy.

Reviewing the negotiated protocol and cipher details is also appropriate. Evidence showing the protocol version accepted by the service and the resulting cipher suite supports the finding and helps the remediation team identify the affected endpoint

and configuration. OpenSSL documents its s_client diagnostic client, which can be used to test TLS negotiation in an authorized assessment.

QUESTION NO: 31

After obtaining a reverse shell, a penetration tester identifies a locally cloned Git repository that contains thousands of files and directories on a Windows machine. The tester suspects there could be sensitive information related to “ProjectX.” Which of the following commands should the tester use in a script to identify potential files to produce the best results?

A. gc * | select " ProjectX "

B. dir /R | findstr " ProjectX "

C. Get-ChildItem * | Select-String " ProjectX "

D. gci -Path . -Recurse -File | Select-String -Pattern "ProjectX"

ANSWER: D

Explanation:

`gci -Path . -Recurse -File | Select-String -Pattern "ProjectX"` is the appropriate PowerShell pipeline for locating content related to the project throughout a large cloned repository. `gci` is the standard alias for `Get-ChildItem`; using `-Path .` starts enumeration in the current repository directory, while `-Recurse` traverses all nested folders. This is essential for a Git working tree, where source code, configuration, historical artifacts, and generated files may be distributed across a deep directory structure. Adding `-File` limits the pipeline to files, avoiding unnecessary attempts to search directory objects. The resulting file objects are passed to `Select-String`, which searches their contents for the specified literal pattern and returns matching lines with useful file-path and line-number information. Searching for `"ProjectX"` without added spaces ensures matches are found regardless of the characters immediately before or after the project name. This supports efficient identification of potentially relevant source files, configuration data, documentation, or embedded secrets for subsequent authorized review. Microsoft documents recursive file enumeration in Get-ChildItem and content-pattern searching in Select-String.

QUESTION NO: 32

During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network ' s authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

A. KARMA attack

B. Beacon flooding

C. MAC address spoofing

D. Eavesdropping

ANSWER: C

Explanation:

MAC address spoofing is correct because it can defeat a wireless deployment that treats a device’s MAC address as an authentication factor or uses MAC filtering as an admission-control mechanism. A tester who identifies an authorized client MAC address can configure their wireless interface to present that address, impersonating the authorized device when associating to the wireless network. Since MAC addresses are transmitted in management and data frames and are not cryptographic credentials, they can be observed and reproduced by an attacker within radio range. This makes MAC-based access control unsuitable as a standalone wireless authentication method. In an authorized assessment, demonstrating this weakness shows that network admission depends on an easily copied hardware identifier rather than on strong, unique user or device credentials. The finding should be documented with the affected SSID, the observed access-control behavior, and a recommendation to use WPA2-Enterprise or WPA3-Enterprise with 802.1X/EAP authentication instead of relying on MAC

filtering. Cisco also notes that MAC filtering is a limited control because MAC addresses can be spoofed. See Cisco's wireless MAC filtering guidance and the CISA guidance on stronger authentication practices.

QUESTION NO: 33

[Attacks and Exploits]

A penetration tester gains access to the target network and observes a running SSH server.

Which of the following techniques should the tester use to obtain the version of SSH running on the target server?

A. Network sniffing

B. IP scanning

C. Banner grabbing

D. DNS enumeration

ANSWER: C

Explanation:

Banner grabbing is the appropriate technique because SSH begins with a clear-text protocol-version exchange before authentication and before the encrypted session is established. When a client connects to TCP port 22, the server sends an identification string in the form `SSH-protoversion-softwareversion`. In many common deployments, that string discloses the implementation and release, such as `SSH-2.0-OpenSSH_9.6`. A tester can collect this information by making a connection to the SSH service or by using an approved service-version detection scan. The result supports service enumeration, vulnerability research, and validation of whether the exposed implementation is within the authorized assessment scope.

The SSH protocol specification defines the identification exchange and requires both sides to send their identification strings at the start of the connection. Nmap also documents version detection as a means of probing open services to identify the application and version exposed by a port. Because the goal is specifically to identify the SSH service version, banner grabbing directly obtains the relevant protocol and software identification information. References: RFC 4253, Section 4.2: Protocol Version Exchange and Nmap Reference Guide: Service and Version Detection.

QUESTION NO: 34

[Reporting and Communication]

A penetration tester is preparing evidence for a finding involving excessive permissions on a network share. Which of the following items should be included to support reproducibility and remediation? (Select two).

A. The affected share path and observed permissions

B. The account context used for validation

C. The tester's personal workstation serial number

D. All unrelated files located on accessible shares

E. The customer's complete network diagram

ANSWER: A B

Explanation:

The affected share path and the permissions observed should be included because remediation teams need to identify the exact resource and access-control condition that created the exposure. Clear evidence of the granted permissions, such as write or modify access for an inappropriate group, enables administrators to validate and correct the configuration.

The account context used for validation should also be documented. Identifying whether access was demonstrated as an unauthenticated user, a standard domain user, or another approved test account establishes the practical impact of the finding and enables the client to reproduce the result safely. NIST SP 800-115 describes the importance of documenting assessment results and evidence in Technical Guide to Information Security Testing and Assessment.

QUESTION NO: 35 - (SIMULATION)

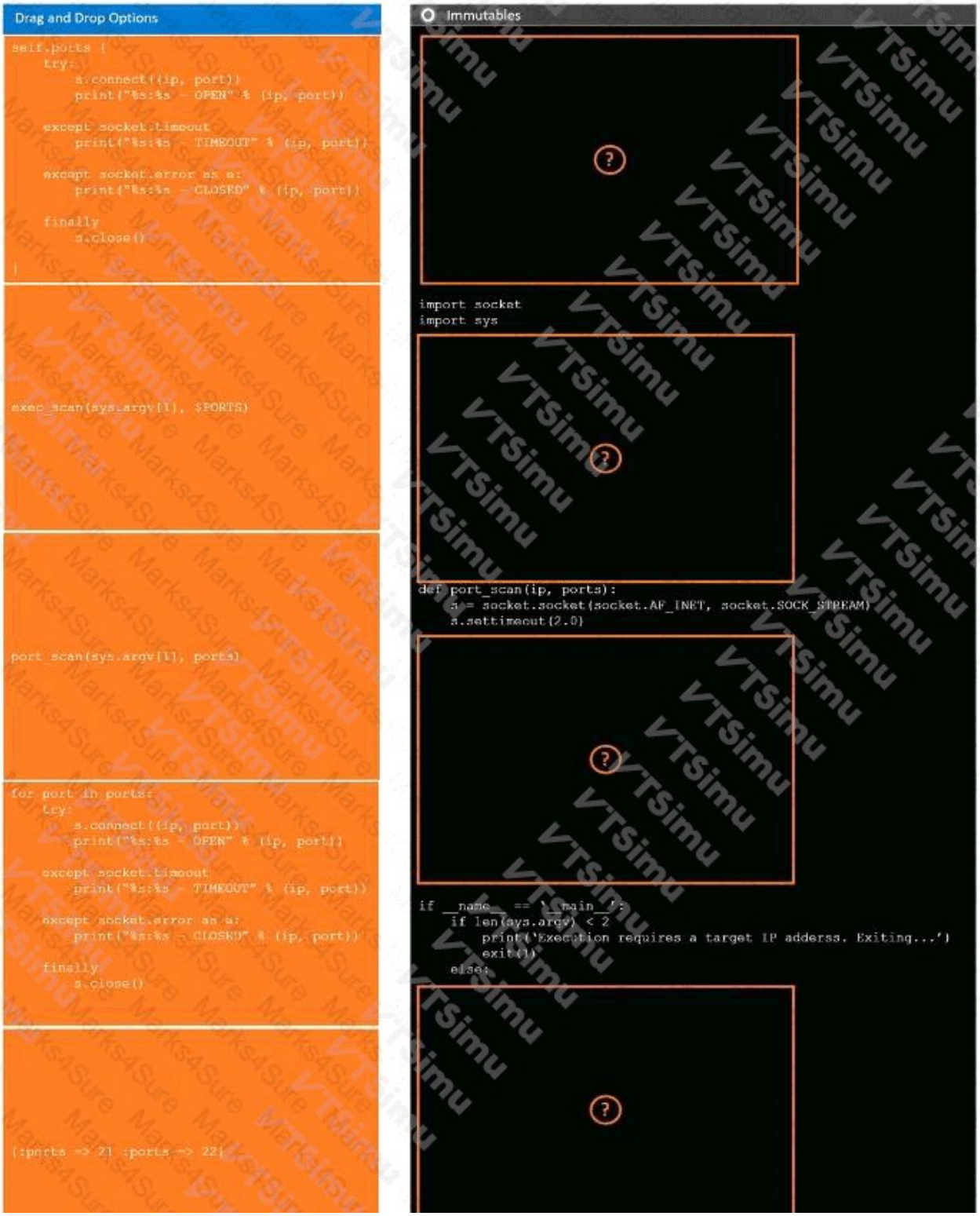
During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

INSTRUCTIONS

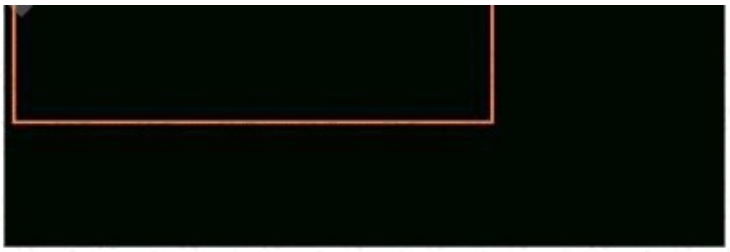
Analyze the code segments to determine which sections are needed to complete a port scanning script.

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.


Drag and Drop Options
self.ports {
try:
s.connect((ip, port))
print("%s:%s - OPEN" % (ip, port))
except socket.timeout
print("%s:%s - TIMEOUT" % (ip, port))
except socket.error as e:
print("%s:%s - CLOSED" % (ip, port))
finally
s.close()
}
exec_scan(sys.argv[1], $PORTS)
port_scan(sys.argv[1], ports)
for port in ports:
try:
s.connect((ip, port))
print("%s:%s - OPEN" % (ip, port))
except socket.timeout
print("%s:%s - TIMEOUT" % (ip, port))
except socket.error as e:
print("%s:%s - CLOSED" % (ip, port))
finally
s.close()
[:ports => 2] :ports => 22]
Immutables
import socket
import sys
def port_scan(ip, ports):
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.settimeout(2.0)
if __name__ == '__main__':
if len(sys.argv) < 2
print('Execution requires a target IP address. Exiting...')
exit(1)
else:

```
[:ports => 21 :ports => 22]
```



```
#!/usr/bin/python
```

```
ports = [21,22]
```

```
#!/usr/bin/ruby
```

```
run_scan(sys.argv[1],ports)
```

```
#!/usr/bin/bash
```



ANSWER: See the explanation for the answer

Explanation:

Place the code blocks in the following order to form the Python port-scanning script:

In the first blank (before the imports), place:

After `import socket` and `import sys`, place:

Inside `port_scan(ip, ports)`, after the socket creation and timeout lines, place the Python `for port in ports:` block:

In the `else:` section at the bottom, place:

The completed script uses the target IP supplied as the first command-line argument and scans TCP ports 21 and 22. Select the blocks using Python syntax (`ports` and `port`), not distractors that use shell-style variables such as `$PORT` or `$PORTS`.

QUESTION NO: 36

A penetration testing company is defining the rules of engagement with a client. Which of the following should the company include?

A. Non-disclosure agreement

B. Escalation process

C. URL list

D. Authorization letter

ANSWER: D

Explanation:

An authorization letter should be included because it documents the client's explicit permission for the penetration testing company to conduct testing against the agreed environment. Written authorization is a foundational planning-and-scoping control: it identifies the authorized parties, establishes that the client has approved the activity, and supports the legal and operational boundaries under which testing may occur. The document should align with the engagement scope and rules of engagement, including the assets or environments covered, permitted testing period, approved testing activities, and relevant limitations. Having this authorization in place before any reconnaissance, scanning, exploitation, or other assessment activity helps ensure the work is distinguishable from unauthorized access and gives both the tester and client a clear record of consent. CompTIA's PenTest+ exam objectives place written authorization within planning and scoping activities, alongside defining scope, constraints, and engagement requirements. The NIST technical guide for security testing likewise emphasizes obtaining authorization and defining the scope before a test begins. See the CompTIA exam objectives resource and NIST SP 800-115.

QUESTION NO: 37

A penetration tester is conducting an assessment of a web application ' s login page. The tester needs to determine whether there are any hidden form fields of interest. Which of the following is the most effective technique?

A. XSS

B. On-path attack

C. SQL injection

D. HTML scraping

ANSWER: D

Explanation:

HTML scraping is the most effective technique because hidden form controls are delivered in the web page's HTML even though they are not displayed in the browser interface. A tester can retrieve the login page response and inspect its source or parsed Document Object Model for elements such as `<input type="hidden" name="..." value="...">`. This reveals field names, default values, anti-forgery tokens, workflow identifiers, redirect parameters, and client-supplied state that may merit further validation during the assessment. The activity can be performed manually with browser developer tools or an intercepting proxy, or automated by parsing the returned HTML. The key benefit is direct visibility into the form structure and values sent by the client when authentication is submitted. OWASP notes that hidden fields are client-side controls and therefore must not be relied on for security-sensitive enforcement; their values can be viewed and modified by a user. A penetration tester should document any fields discovered, determine whether they influence authorization or application behavior, and verify that the server independently validates them. See the OWASP guidance on manipulating hidden fields and the MDN reference for hidden input elements.

QUESTION NO: 38

[Attacks and Exploits]

A penetration tester is reviewing an Active Directory environment after obtaining access as a standard domain user. Which of the following actions would help identify paths that could lead to elevated privileges? (Select two).

A. Enumerate group memberships and delegated permissions.

B. Review service accounts with SPNs.

C. Disable domain-controller auditing.

D. Delete inactive user accounts.

E. Change the domain password policy.

ANSWER: A B

Explanation:

Enumerating group memberships and delegated permissions is appropriate because Active Directory privilege paths frequently result from nested group membership, excessive access-control entries, delegated administration, and permissions over organizational units, groups, or computer objects. These relationships can allow a low-privileged account to modify an object or gain membership in a more privileged group.

Reviewing service accounts with SPNs is also appropriate. User-backed service accounts with registered service principal names can be candidates for Kerberos service-ticket requests in an authorized assessment. The resulting information helps identify accounts whose password management and privileges warrant further review. MITRE documents Domain Groups discovery and Kerberoasting.

QUESTION NO: 39

[Post-Engagement Activities]

After completing an authorized assessment, a penetration tester must preserve evidence while protecting client data. Which of the following actions should the tester take? (Select two).

A. Encrypt evidence at rest.

B. Follow the agreed retention and destruction requirements.

C. Upload all collected evidence to a public file-sharing site.

D. Retain client data indefinitely for future testing.

E. Send credentials in an unencrypted email message.

ANSWER: A B

Explanation:

Encrypting evidence at rest is appropriate because screenshots, scan results, logs, and proof-of-concept output may contain sensitive client information, credentials, internal hostnames, or regulated data. Encryption helps protect that material from unauthorized disclosure while it is retained for reporting and validation.

Following the agreed retention and destruction requirements is also appropriate. The rules of engagement or statement of work should define how long evidence may be retained, who may access it, and when it must be securely destroyed or returned. These procedures support confidentiality and demonstrate that testing artifacts are handled consistently after the engagement. NIST SP 800-115 provides guidance on handling assessment data and reporting activities in SP 800-115.

QUESTION NO: 40

[Tools and Code Analysis]

In a file stored in an unprotected source code repository, a penetration tester discovers the following line of code:

sshpass -p donotchange ssh admin@192.168.6.14

Which of the following should the tester attempt to do next to take advantage of this information? (Select two).

A. Use Nmap to identify all the SSH systems active on the network.

B. Take a screen capture of the source code repository for documentation purposes.

C. Investigate to find whether other files containing embedded passwords are in the code repository.

D. Confirm whether the server 192.168.6.14 is up by sending ICMP probes.

E. Run a password-spraying attack with Hydra against all the SSH servers.

F. Use an external exploit through Metasploit to compromise host 192.168.6.14.

ANSWER: B C

Explanation:

Taking a screen capture of the source code repository for documentation purposes is appropriate because the tester has identified a hard-coded credential in an unprotected repository. Capturing clear evidence—including the affected file, repository location, exposed username, target reference, and relevant revision information where available—preserves the finding for reporting, validation, remediation, and retesting. Evidence handling should follow the engagement's rules of engagement and protect the exposed secret from unnecessary disclosure.

Investigating whether other files containing embedded passwords are in the code repository is also appropriate because exposed credentials commonly indicate a broader secret-management weakness. A scoped review of the repository can identify additional hard-coded passwords, private keys, API tokens, connection strings, and historical secrets in committed files. This enables the tester to determine the full impact of the issue and provide actionable remediation guidance, such as removing secrets from source control, rotating exposed credentials, and using an approved secrets-management system. OWASP identifies hard-coded credentials as a relevant software security concern in its guidance on hard-coded passwords. GitHub also documents secret scanning, which illustrates the value of systematically identifying exposed secrets in repositories.

QUESTION NO: 41

[Tools and Code Analysis]

A penetration tester is reviewing a client-provided container image before it is deployed to production. Which of the following activities would help identify software supply-chain risk within the image? (Select two).

A. Generate an SBOM for the image.

B. Scan installed packages for known vulnerabilities.

C. Change the container hostname.

D. Disable image version tags.

E. Increase the container memory limit.

ANSWER: A B

Explanation:

Generating an SBOM and **scanning installed packages for known vulnerabilities** help identify software supply-chain risk. An SBOM provides an inventory of components, versions, and dependency relationships included in the image. This inventory enables the tester and development team to identify direct and transitive packages that may be outdated, unsupported, or subject to published vulnerabilities.

Scanning the installed packages and libraries against vulnerability data identifies components that are associated with known CVEs. The results should be validated for exploitability in the deployed environment, including whether a vulnerable package is reachable and whether a fixed version is available. CISA describes an SBOM as a formal record of software-component details and supply-chain relationships at CISA Software Bill of Materials. OWASP also provides guidance on component analysis at OWASP Component Analysis.

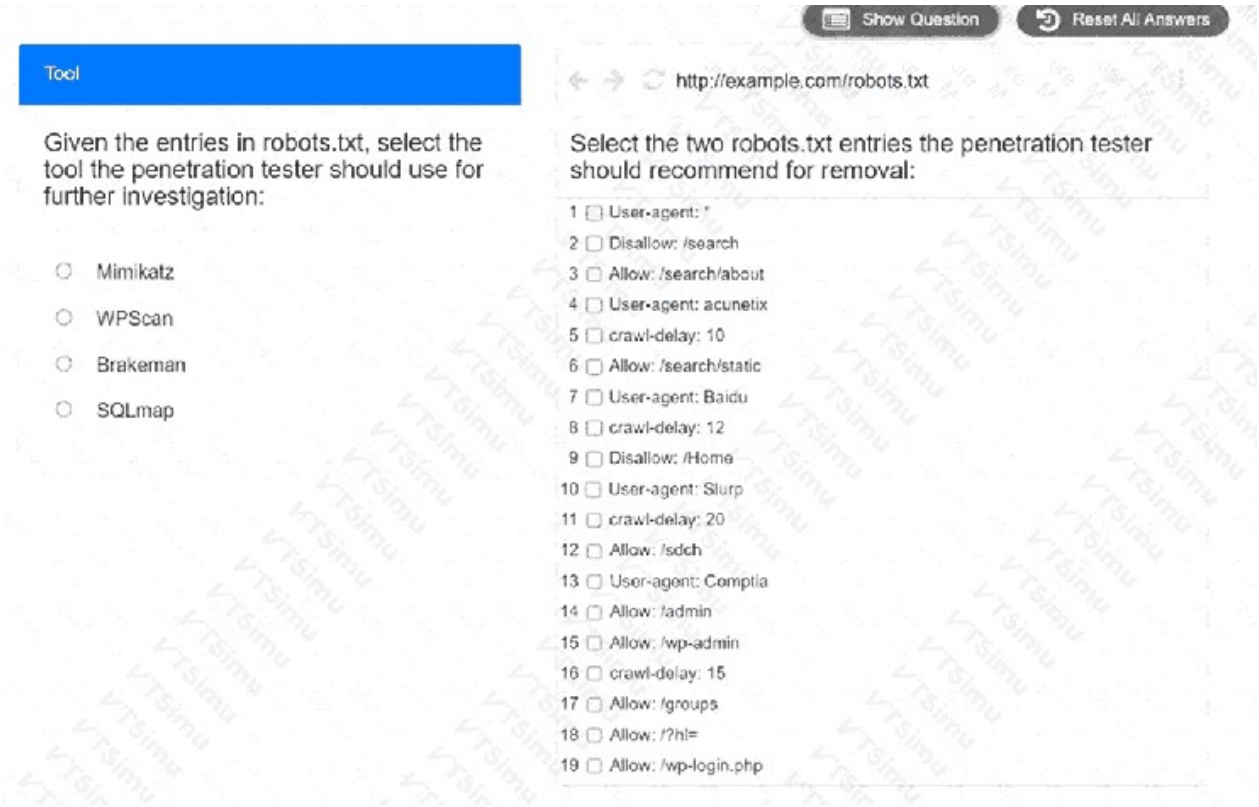
QUESTION NO: 42 - (SIMULATION)

A penetration tester is performing reconnaissance for a web application assessment. Upon investigation, the tester reviews the robots.txt file for items of interest.

INSTRUCTIONS

Select the tool the penetration tester should use for further investigation.

Select the two entries in the robots.txt file that the penetration tester should recommend for removal.



ANSWER: See the explanation for the answer

Explanation:

Select: `WPScan`

Recommend removing these two robots.txt entries:

The `/wp-admin` path identifies a WordPress administrative area, making `WPScan` the appropriate tool for further WordPress enumeration and vulnerability assessment. The `/admin` and `/wp-admin` entries unnecessarily advertise administrative locations to crawlers and attackers. Removing them reduces information disclosure, although proper authentication, authorization, MFA, and access restrictions are still required because robots.txt is not an access-control mechanism.

QUESTION NO: 43

A penetration tester gains initial access to a target system by exploiting a recent RCE vulnerability. The patch for the vulnerability will be deployed at the end of the week. Which of the following utilities would allow the tester to reenter the system remotely after the patch has been deployed? (Select two).

A. schtasks.exe

B. rundll.exe

C. cmd.exe

D. chgusr.exe

E. sc.exe

F. netsh.exe

ANSWER: A E

Explanation:

schtasks.exe and **sc.exe** are appropriate Windows-native utilities for establishing authorized persistence during a penetration test. A scheduled task created with schtasks.exe can execute a designated command or program on a schedule, at system startup, or when a specified event occurs. If configured to invoke an approved remote-access agent or callback mechanism, it can provide a way to regain access independently of the original RCE flaw after that flaw is remediated. Microsoft documents scheduled-task management and creation through SchTasks at Microsoft Learn: schtasks create.

sc.exe interacts with the Windows Service Control Manager. In an authorized assessment, a tester can use it to create or configure a service that starts automatically and launches an approved persistence payload or management agent. Because services can be configured to start during boot, this mechanism remains available after reboot and does not depend on the vulnerable application or RCE path remaining unpatched. This directly demonstrates the importance of post-exploitation validation and cleanup within the agreed rules of engagement. Microsoft's service-management command documentation is available at Microsoft Learn: sc create.

QUESTION NO: 44

Which of the following technologies is most likely used with badge cloning? (Select two).

A. NFC

B. RFID

C. Bluetooth

D. Modbus

E. Zigbee

F. CAN bus

ANSWER: A B

Explanation:

NFC and **RFID** are the technologies most associated with cloning physical access-control badges. RFID access systems use radio-frequency communication between a credential and a reader. Depending on the system, the credential may expose an identifier or other stored data that can be read and reproduced onto a compatible programmable credential. During an authorized penetration test, testing the resistance of badge systems to unauthorized reading, emulation, or duplication may identify weaknesses in physical access controls.

NFC is a short-range, high-frequency RFID technology commonly implemented in contactless cards, mobile credentials, and modern proximity-access deployments. Its close operating range does not eliminate cloning risk; the relevant security characteristics depend on the card or device protocol, mutual authentication design, encryption, key management, and whether the credential uses static or protected values. A tester assessing an authorized environment may therefore encounter either conventional RFID badges or NFC-capable badges and readers. NIST's RFID security guidance discusses risks and protections for RFID systems, while the NFC Forum provides technical information on NFC's contactless communication technology: NIST SP 800-98, Guidelines for Securing Radio Frequency Identification Systems and NFC Forum: What Is NFC?.

QUESTION NO: 45

[Planning and Scoping]

A penetration tester is planning a social-engineering engagement that includes simulated phishing messages. Which of the following items should be established before the campaign begins? (Select two).

A. An approved target population

B. Campaign dates and testing hours

C. A list of production administrator passwords

D. Authorization to contact any external organization

E. A requirement to deploy malware to recipients

ANSWER: A B

Explanation:

An approved target population and campaign dates must be established before the campaign begins. The approved population defines which users, departments, or groups may receive messages, preventing accidental contact with excluded personnel. Campaign dates establish the authorized testing window and allow the client to avoid periods such as major business events, emergency operations, or other sensitive activities.

Social-engineering rules of engagement should also identify approved pretexts, data-collection limits, notification and escalation contacts, and conditions for pausing the activity. These safeguards permit realistic testing while maintaining client authorization and minimizing operational risk. NIST discusses planning and rules for security testing in SP 800-115.

QUESTION NO: 46

A penetration tester has discovered sensitive files on a system. Assuming exfiltration of the files is part of the scope of the test, which of the following is most likely to evade DLP systems?

A. Encoding the data and pushing through DNS to the tester's controlled server.

B. Padding the data and uploading the files through an external cloud storage service.

C. Obfuscating the data and pushing through FTP to the tester's controlled server.

D. Hashing the data and emailing the files to the tester's company inbox.

ANSWER: A

Explanation:

Encoding the data and pushing through DNS to the tester's controlled server is the best answer because DNS is a commonly permitted network service that can be used as an application-layer channel for transferring small pieces of encoded data. A tester can place encoded data within DNS query names directed to a domain under the tester's control; the authoritative DNS infrastructure for that domain can then receive and reconstruct the transmitted content. This technique is commonly called DNS tunneling.

From a defensive perspective, data loss prevention controls often concentrate inspection and policy enforcement on high-volume, business-oriented egress paths such as web uploads, email attachments, file-transfer protocols, and sanctioned cloud-storage applications. DNS traffic may receive less content-aware inspection because name resolution is essential to normal network operation and is frequently allowed through network boundaries. That characteristic can make DNS-based exfiltration more likely to bypass a DLP implementation that lacks DNS-specific monitoring or tunneling detection. The technique is not inherently undetectable: security teams can identify it through DNS logging, query-length analysis, unusual subdomain entropy, anomalous request volume, and restrictions on external DNS resolvers. MITRE ATT&CK documents DNS as an application-layer protocol that adversaries may use for command-and-control communications and identifies exfiltration over an alternative protocol as a relevant technique: MITRE ATT&CK: DNS and MITRE ATT&CK: Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol.

QUESTION NO: 47

A penetration tester needs to exploit a vulnerability in a wireless network that has weak encryption to perform traffic analysis and decrypt sensitive information. Which of the following techniques would best allow the penetration tester to have access to the sensitive information?

A. Bluejacking

B. SSID spoofing

C. Packet sniffing

D. ARP poisoning

ANSWER: C

Explanation:

Packet sniffing is correct because it directly enables the collection of wireless frames needed for traffic analysis. During an authorized penetration test, the tester places a compatible wireless adapter into monitor mode and captures traffic transmitted over the target wireless channel. The captured frames can then be examined to identify protocols, metadata, authentication exchanges, and potentially sensitive content. Where the wireless security implementation uses weak or obsolete encryption, the capture provides the material needed to assess whether the encryption can be broken and whether protected traffic can be recovered or decrypted. Packet capture is therefore the foundational technique: without collecting the relevant wireless traffic, there is no data set to analyze for weak-encryption exposure. The testing process should remain within the agreed scope and authorization, and findings should document the affected wireless configuration, the evidence collected, the impact of exposed data, and remediation such as replacing obsolete wireless security with modern WPA2 or WPA3 configurations. NIST describes the security risks associated with wireless networks and the need to protect wireless transmissions in its Guidelines for Securing Wireless Local Area Networks. Wireshark also documents the packet-capture process and analysis capabilities in its User's Guide.

QUESTION NO: 48

A penetration tester gains access to the target network and observes a running SSH server.

Which of the following techniques should the tester use to obtain the version of SSH running on the target server?

A. Network sniffing

B. IP scanning

C. Banner grabbing

D. DNS enumeration

ANSWER: C

Explanation:

Banner grabbing is correct because SSH servers normally transmit an identification string immediately after a client establishes a TCP connection to the SSH service, conventionally on port 22. This banner follows the SSH protocol format and includes the protocol version plus a software-version identifier, such as `SSH-2.0-OpenSSH_9.6`. A tester can safely collect this information during service enumeration by connecting to the service with an appropriate tool, such as Netcat or Nmap version detection, and recording the returned identification string. Knowing the SSH implementation and version helps the tester accurately identify applicable vendor advisories, known vulnerabilities, insecure legacy versions, and configuration issues for validation within the authorized assessment scope. The SSH protocol specification explicitly defines the server identification exchange at the beginning of an SSH transport connection, before key exchange occurs. This makes banner grabbing a direct and reliable technique for discovering the version information exposed by an SSH service. See RFC 4253, section 4.2 for the SSH protocol version exchange and Nmap Reference Guide: Service and Version Detection for practical version-detection methodology.

QUESTION NO: 49

A penetration tester executes multiple enumeration commands to find a path to escalate privileges. Given the following command:

find / -user root -perm -4000 -exec ls -ldb {} \; 2 > /dev/null

Which of the following is the penetration tester attempting to enumerate?

A. Attack path mapping

B. API keys

C. Passwords

D. Permission

ANSWER: D

Explanation:

Permission is correct because this command searches the entire filesystem for files owned by the root user that have the set-user-ID (SUID) permission bit set. In Unix-like systems, the SUID bit is represented by the octal value `4000`. When an executable with this bit is run, it executes with the effective privileges of its file owner rather than the privileges of the user who launched it. Root-owned SUID executables are therefore highly relevant to privilege-escalation enumeration, since a vulnerable, misconfigured, or abusable executable could potentially permit elevated access.

The `find /` portion starts searching at the filesystem root. The `-user root` predicate limits results to root-owned files, while `-perm -4000` identifies files with the SUID bit present. For every match, `-exec ls -ldb {} \;` displays a detailed listing, including its permission mode and pathname. Finally, `2 > /dev/null` suppresses error messages such as permission-denied notices, making the enumeration output easier to review. GNU Findutils documents permission-mode matching at its Find manual, and SUID behavior is described in the Linux setuid documentation.

QUESTION NO: 50

[Attacks and Exploits]

A penetration tester identifies an exposed corporate directory containing first and last names and phone numbers for employees. Which of the following attack techniques would be the most effective to pursue if the penetration tester wants to compromise user accounts?

A. Smishing

B. Impersonation

C. Tailgating

D. Whaling

ANSWER: A

Explanation:

Smishing is the most effective technique because the exposed directory supplies precisely the data needed to deliver targeted SMS phishing messages: employees' names and mobile phone numbers. During an authorized penetration test, the tester can use those details to create a credible pretext, such as an account-security notification, password-expiration alert, MFA request, or help-desk message. The message can direct a recipient to a controlled credential-harvesting page or an approved testing workflow that measures whether the recipient submits credentials or an authentication code. Personalization with a real name makes a message more believable than an untargeted text campaign, while phone numbers provide a direct delivery channel. This approach therefore connects the discovered information to the stated objective of compromising user accounts. CISA identifies phishing through text messages as smishing and notes that social-engineering messages commonly attempt to induce targets to reveal sensitive information or visit malicious links. See CISA guidance on recognizing and reporting phishing. The FTC also describes text-message phishing as "smishing" and advises users not to click unexpected links in texts, illustrating the account-compromise risk presented by this channel: FTC consumer alert on text-message scams.

QUESTION NO: 51 - (DRAG DROP)

DRAG DROP

[Information Gathering and Vulnerability Scanning]

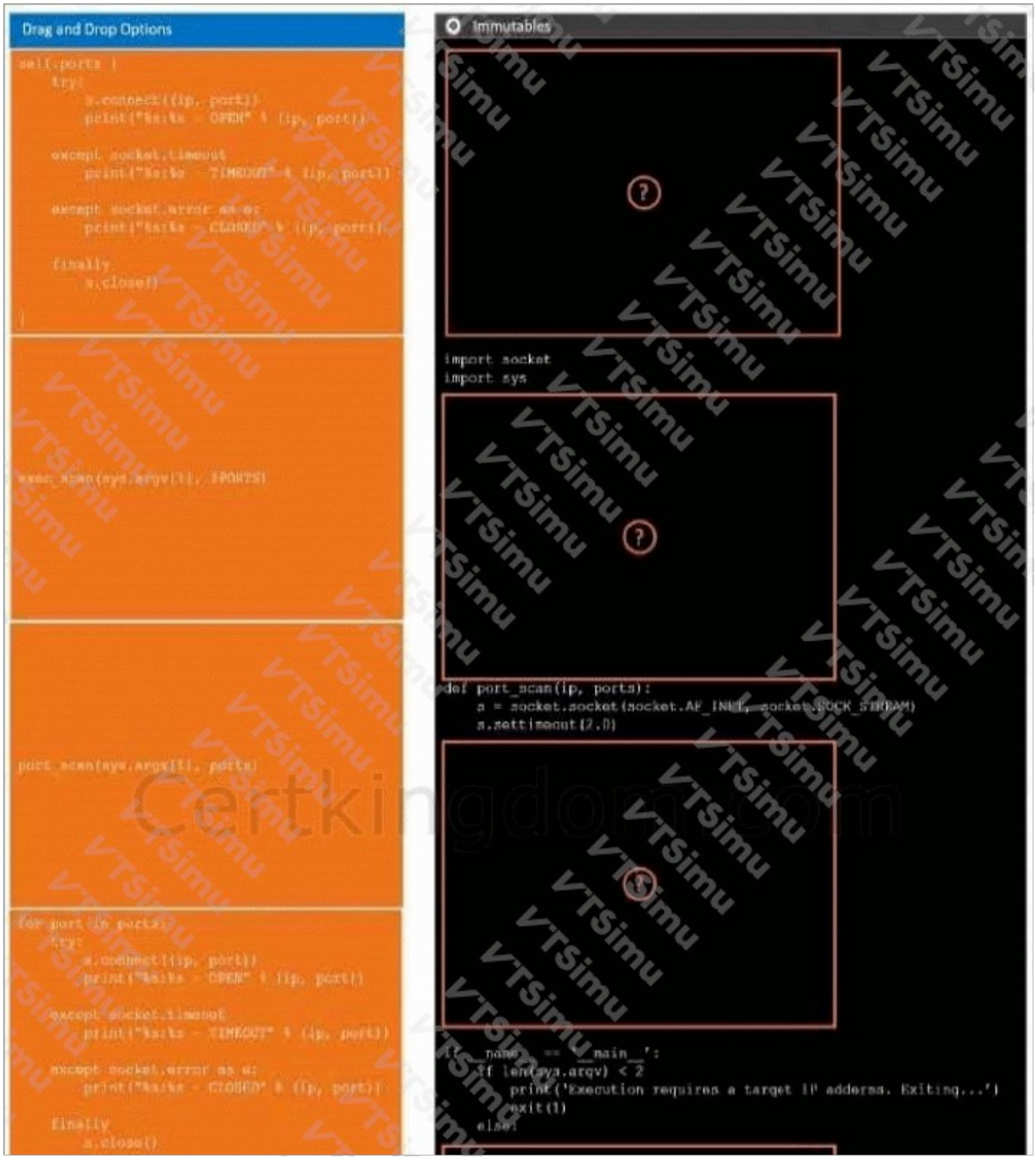
During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

INSTRUCTIONS

Analyze the code segments to determine which sections are needed to complete a port scanning script.

Drag the appropriate elements into the correct locations to complete the script.

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



ANSWER:



Explanation:

A working Python TCP connect scanner needs its code segments arranged according to variable scope and execution flow. The interpreter directive belongs at the very beginning of the file, before imports, so that a Unix-like operating system can identify the Python interpreter when the script is executed directly. Python documents this conventional script layout in its Python on Unix platforms documentation.

After importing `socket` and `sys`, the script should define the `ports` collection. Defining it at module level makes the selected port numbers available when the program reaches its command-line execution block. The `port_scan(sys.argv[1], ports)` call then belongs beneath the `else:` branch of the `__main__` check. At that point, the script has confirmed that a target IP address was supplied and can pass both the command-line target and the configured ports list into the scan function.

The port-iteration and exception-handling segment belongs inside `port_scan(ip, ports)`, directly after socket creation and the timeout setting. Each iteration uses `s.connect((ip, port))` to attempt a TCP connection to the target and port. A successful connection identifies a reachable listening service, while timeout and socket-error handling allow scanning to

continue cleanly through the remaining ports. The `finally` block closes the socket during every iteration, ensuring network resources are released even if an exception occurs. Python’s socket module documentation describes TCP stream sockets and connection operations, and the try statement documentation explains why a `finally` suite is appropriate for guaranteed cleanup.