PassQueen
a.k.a dumpsqueen.com

GIAC Penetration Tester

GIAC GPEN

Version Demo

Total Demo Questions: 37

Total Premium Questions: 371

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	108
Topic 2, Volume B	108
Topic 3, Volume C	79
Topic 4, Volume D	56
Total	371

QUESTION NO: 1

Which of the following United States laws protects stored electronic information?

A. Title 18, Section 1029

B. Title 18, Section 1362

C. Title 18, Section 2701

D. Title 18, Section 2510

ANSWER: C

Explanation:

Title 18, Section 2701 is correct because it is the principal unauthorized-access provision of the Stored Communications Act, which is codified within the Electronic Communications Privacy Act. This section makes it an offense to intentionally access, without authorization, a facility through which an electronic communication service is provided, or to intentionally exceed authorization to access that facility, when doing so obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage. In penetration-testing work, this legal boundary is especially important when systems contain retained emails, cloud-hosted messages, queued communications, or other communications held by a service provider. Authorization must explicitly cover the target systems and the permitted actions; technical capability alone does not establish legal authority to access stored communications. The statute also defines limited exceptions, including conduct authorized by the relevant service and access authorized under other provisions of the chapter, but these exceptions do not replace the need for clear written rules of engagement. The statutory text is available through Cornell Law School's U.S. Code page for 18 U.S.C. § 2701. Additional ECPA and Stored Communications Act guidance is provided by the U.S. Department of Justice.

QUESTION NO: 2

Which of the following statements are true about the Enum tool?

Each correct answer represents a complete solution. Choose all that apply.

A. It is capable of performing brute force and dictionary attacks on individual accounts of Windows NT/2000.

B. One of the countermeasures against the Enum tool is to disable TCP port 139/445.

C. It is a console-based Win32 information enumeration utility.

D. It uses NULL and User sessions to retrieve user lists, machine lists, LSA policy information, etc.

ANSWER: A B C D

Explanation:

The Enum utility is a legacy, console-based Win32 reconnaissance and information-enumeration tool associated with assessing Windows NT and Windows 2000 systems. It can query information exposed through Windows networking and security interfaces, including account names, machine lists, share-related information, and Local Security Authority policy data. A key feature of tools in this category is their ability to use anonymous (NULL) sessions where a target permits them, as well as authenticated user sessions, to collect information useful during a penetration test. Enum also includes password-auditing functionality that can attempt dictionary-based and brute-force password guesses against individual accounts, subject to the target's authentication behavior and account-lockout controls. Because its remote enumeration commonly relies on SMB/NetBIOS services, restricting access to TCP ports 139 and 445 is an effective network-level mitigation: it reduces exposure of the SMB and NetBIOS session services that support this type of remote interrogation. Microsoft documents SMB use over TCP port 445 and NetBIOS session service use over TCP port 139 in its service overview and network port requirements. Microsoft also provides guidance on protecting SMB services through its SMB security documentation.

QUESTION NO: 3

What problem occurs when executing the following command from within a netcat raw shell? sudo cat /etc/shadow

A. Sudo does not work at all from a shell

B. Sudo works fine if the user and command are both in the /etc/sudoers file

C. The display blanks after typing the sudo command

D. You will not be able to type the password at the password prompt

E. Sudo cannot prompt for a password because a netcat raw shell has no controlling TTY.

ANSWER: E

Explanation:

Sudo cannot normally perform an interactive password authentication from a basic netcat raw shell because that shell does not provide a controlling terminal (TTY). A netcat connection commonly supplies network-backed standard input and output, but it does not allocate the pseudo-terminal that interactive programs expect. When sudo needs to authenticate the invoking user, it attempts to conduct its password conversation through a terminal; without one, it cannot safely display and read an interactive password prompt. The practical result is typically an error such as “no tty present and no askpass program specified,” rather than a usable password prompt. This limitation applies when sudo must request a password. It may not occur when the applicable sudoers policy authorizes the command with `NOPASSWD`, or when a proper PTY has been allocated after obtaining the shell. Sudo’s documentation describes its terminal-based authentication behavior and the alternative askpass mechanism, while the Linux PTY documentation explains that a pseudo-terminal supplies the terminal interface needed by interactive applications. See the sudo manual and the Linux PTY manual page.

QUESTION NO: 4

Ryan wants to create an ad hoc wireless network so that he can share some important files with another employee of his company. Which of the following wireless security protocols should he choose for setting up an ad hoc wireless network?

Each correct answer represents a part of the solution. Choose two.

A. WPA2 -EAP

B. WPA-PSK

C. WPA-EAP

D. WEP

ANSWER: B D

Explanation:

For the legacy Wi-Fi ad hoc (IBSS) scenario described, **WPA-PSK** and **WEP** are the applicable choices. WPA-PSK uses a pre-shared passphrase, allowing the two participants to establish encryption without deploying an enterprise authentication service. This makes it suitable for a small, temporary peer-to-peer wireless network in which both users can agree on and configure the same keying material. WEP was also supported by legacy ad hoc implementations and likewise uses a manually shared key, so it meets the historical protocol-selection requirement in this question.

In a real engagement or corporate environment, WPA-PSK should be preferred over WEP whenever the platform supports it. WEP has well-known cryptographic weaknesses and can be compromised quickly; it should not be used to protect important company files except where a legacy testing scenario explicitly requires it. The Wi-Fi Alliance’s WPA3 migration guidance discusses the retirement of obsolete WEP and legacy WPA security, while Microsoft’s Wi-Fi documentation distinguishes pre-shared-key authentication from enterprise authentication designs. See Wi-Fi Alliance security information and Microsoft’s 802.1X wireless deployment guidance.

QUESTION NO: 5

A penetration tester obtains telnet access to a target machine using a captured credential. While trying to transfer her exploit to the target machine, the network intrusion detection systems keeps detecting her exploit and terminating her connection. Which of the following actions will help the penetration tester transfer an exploit and compile it in the target system?

A. Use the http service's PUT command to push the file onto the target machine.

B. Use the scp service, protocol SSHv2 to pull the file onto the target machine.

C. Use the telnet service's ECHO option to pull the file onto the target machine

D. Use the ftp service in passive mode to push the file onto the target machine.

ANSWER: B

Explanation:

Use the scp service, protocol SSHv2 to pull the file onto the target machine. SCP transfers files through an SSH connection, so the file contents and session commands are encrypted in transit. If the tester can run an SCP client from the established target shell and authenticate to a reachable source host, the target can retrieve the exploit source without placing the exploit's recognizable content in plaintext on the network. This reduces the ability of a network IDS relying on content signatures to identify the exploit during transfer. Once the source file is present locally, the tester can use the target's compiler and build tools to compile it, avoiding the need to transmit the resulting executable over the monitored path. SCP's use of SSH also provides integrity protection for the transfer, helping ensure that the retrieved source is not modified while in transit. The OpenSSH documentation describes SCP as securely copying files between hosts using SSH for transport; see the OpenBSD scp manual. This approach aligns with GPEN's focus on practical penetration-testing techniques, including transferring tools while accounting for network defenses; see the GIAC GPEN certification page.

QUESTION NO: 6

You work as a Network Administrator in the Secure Inc. Your company is facing various network attacks due to the insecure wireless network. You are assigned a task to secure your wireless network. For this, you have turned off broadcasting of the SSID. However, the unauthorized users are still able to connect to the wireless network. Which of the following statements can be the reason for this issue?

Each correct answer represents a complete solution. Choose all that apply.

A. You have forgotten to turn off DHCP.

B. You are using WPA2 security scheme.

C. The SSID is still sent inside both client and AP packets.

D. You are using the default SSID.

ANSWER: A C D

Explanation:

"The SSID is still sent inside both client and AP packets." is correct because suppressing beacon SSID broadcasts does not make a wireless network undiscoverable. A client configured for the network sends probe requests that identify the network, and association-related traffic also exposes the SSID. Anyone passively monitoring wireless traffic can capture this information and then attempt to join the network. "You are using the default SSID." is also a reason because default network names are predictable and commonly known; hiding such a name provides little barrier to a user who can configure a client manually or has already learned the network identity. "You have forgotten to turn off DHCP." can enable an unauthorized client that has associated with the WLAN to receive usable IP configuration automatically, including an address, gateway, and DNS settings, allowing practical access to network services. DHCP should not be treated as an authentication control, but leaving it available makes access easier once wireless association is possible. Effective WLAN security requires strong authentication and encryption, such as WPA2/WPA3 Enterprise with appropriate credential controls, rather than relying on SSID suppression. The CISA guidance on hidden Wi-Fi networks explains that hidden SSIDs do not provide meaningful security, and the NIST WLAN security guidelines emphasize authentication and encryption controls.

QUESTION NO: 7

Which of the following statements are true about NTLMv1?

Each correct answer represents a complete solution. Choose all that apply.

A. It uses the LANMAN hash of the user's password.

B. It is mostly used when no Active Directory domain exists.

C. It is a challenge-response authentication protocol.

D. It uses the MD5 hash of the user's password.

ANSWER: A C

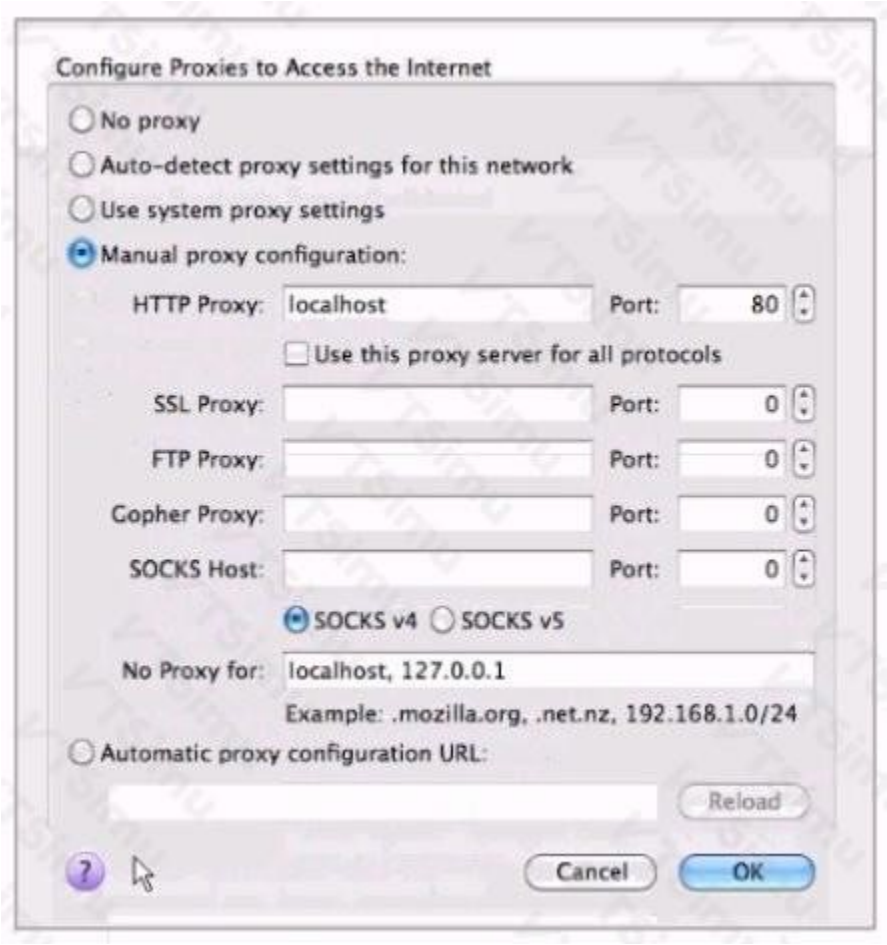
Explanation:

NTLMv1 is a challenge-response authentication protocol: the server supplies an 8-byte challenge, and the client derives response material from password-hash data rather than transmitting the clear-text password. In the legacy NTLMv1 exchange, an LM response can be produced using the LAN Manager (LANMAN) password hash, while the NTLM response is based on the NT password hash. Therefore, it is accurate that NTLMv1 uses the LANMAN hash of the user's password, particularly in configurations where LM authentication/LM responses remain enabled, and that it is a challenge-response authentication protocol.

These legacy mechanisms have important security implications. LANMAN hashes use weak, legacy processing and NTLMv1's challenge-response construction is susceptible to efficient offline cracking and relay-related risks. Microsoft consequently recommends restricting or eliminating LM and NTLMv1 traffic and moving to stronger authentication methods, such as Kerberos for domain environments or NTLMv2 only where NTLM remains necessary. Microsoft's protocol specification documents the NTLM challenge-message and authenticate-message exchange, including the legacy response formats: MS-NLMP: NT LAN Manager Protocol. Microsoft's security guidance on auditing and restricting NTLM is available at NTLM overview and security guidance.

QUESTION NO: 8

A junior penetration tester at your firm is using a non-transparent proxy for the first time to test a web server. He sees the web site In his browser but nothing shows up In the proxy. He tells you that he just installed the non-transparent proxy on his computer and didn't change any defaults. After verifying the proxy is running, you ask him to open up his browser configuration, as shown in the figure, which of the following recommendations will correctly allow him to use the transparent proxy with his browser?



A. He should change the PORT: value to match the port used by the non-transparentproxy.

B. He should select the checkbox "use this proxy server for all protocols" for theproxy to function correctly.

C. He should change the HTTP PROXY value to 127.0.0.1 since the non-transparentproxy is running on the same machine as the browser.

D. He should select NO PROXY instead of MANUAL PROXY CONFIGURATION as thissetting is only necessary to access the Internet behind protected networks.

ANSWER: C

Explanation:

He should change the HTTP PROXY value to 127.0.0.1 since the non-transparentproxy is running on the same machine as the browser. A non-transparent (explicit) interception proxy receives traffic only when the client is configured to send requests to its listening address. Because the browser and proxy are running on the same computer, the loopback address `127.0.0.1` directs the browser's HTTP requests back to the local proxy process rather than directly to the target web server. Once the browser is pointed at that local listener, the proxy can receive, display, and intercept the requests. The configured port must also correspond to the proxy listener, as depicted in the browser configuration; the necessary correction identified here is the proxy host address. Mozilla documents that manual proxy configuration requires specifying the proxy host and port for the relevant protocol. PortSwigger likewise instructs users configuring Firefox for an intercepting proxy to enter `127.0.0.1` as the HTTP proxy host when the proxy runs locally. This configuration is fundamental during web penetration testing because it ensures the browser traffic is routed through the testing tool for inspection and modification. See Mozilla's Firefox connection-settings guidance and PortSwigger's Firefox proxy configuration documentation.

QUESTION NO: 9

Which of the following are the countermeasures against WEP cracking?

Each correct answer represents a part of the solution. Choose all that apply.

A. Using a 16 bit SSID.

B. Changing keys often.

C. Using the longest key supported by hardware.

D. Using a non-obvious key.

ANSWER: B C D

Explanation:

Changing keys often, using the longest key supported by hardware, and using a non-obvious key are all measures that can raise the effort required to compromise a WEP-protected network or reduce the useful lifetime of compromised keying material. Frequent key changes limit how long an obtained key remains valuable and can reduce an attacker's opportunity to collect traffic associated with a single static key. Selecting the longest WEP key size available increases the keyspace relative to shorter WEP configurations, which provides more resistance to simple key-search approaches. A non-obvious, randomly generated key avoids predictable words, organization names, and common patterns that could be recovered through guessing or wordlist-based attempts.

These are risk-reduction practices rather than a durable security architecture. WEP has fundamental design weaknesses involving its RC4 use and initialization vectors, so key length and key-selection hygiene cannot fully remediate it. NIST advises organizations to use current Wi-Fi security mechanisms rather than relying on deprecated wireless protections; see NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks. In a real environment, migration to WPA2 or WPA3 with strong authentication and encryption is the appropriate long-term corrective action.

QUESTION NO: 10

Which of the following techniques are NOT used to perform active OS fingerprinting?

Each correct answer represents a complete solution. Choose all that apply.

A. Analyzing email headers

B. Sniffing and analyzing packets

C. ICMP error message quoting

D. Sending FIN packets to open ports on the remote system

ANSWER: A B

Explanation:

Active OS fingerprinting identifies a target operating system by deliberately transmitting specially constructed network probes and evaluating the target's responses. In contrast, *Analyzing email headers* relies on metadata already present in email messages, such as mail-transfer path information and mail-client identifiers. It does not require sending network probes to the host being assessed, so it is not an active OS-fingerprinting technique.

Sniffing and analyzing packets is likewise a passive approach when the assessor observes traffic already traversing a network. Packet fields and protocol behavior—such as TCP window sizes, TCP options, TTL values, and timestamp behavior—can reveal characteristics associated with an operating system without directly interacting with the observed system. Passive fingerprinting is particularly useful where probes are undesirable or where stealth is important.

Nmap's OS-detection documentation describes active detection as using TCP, UDP, and ICMP probes and response characteristics, which distinguishes it from passive traffic observation. See Nmap OS Detection documentation. For background on passive TCP/IP fingerprinting from captured traffic, see the p0f project documentation.

QUESTION NO: 11

Which of the following describes the direction of the challenges issued when establishing a wireless (IEEE 802.11) connection?

A. One-way, the client challenges the access point

B. One-way, the access point challenges the client

C. No challenges occur during a wireless connection

D. Two-way, both the client and the access point challenge each other

ANSWER: B

Explanation:

One-way, the access point challenges the client describes the IEEE 802.11 Shared Key authentication exchange. In this legacy 802.11 authentication method, the station first requests authentication from the access point. The access point then generates and sends a plaintext challenge to the station. The station encrypts that challenge using the configured shared WEP key and returns the encrypted result. The access point decrypts the response and compares it with its original challenge to determine whether the station possesses the required key material. Thus, the challenge originates at the access point and is answered by the client; it is not a mutual challenge exchange. This distinction is useful in penetration-testing contexts because the challenge and encrypted response historically provided material that could assist attacks against weak or legacy WEP deployments. NIST's WLAN security guidance describes 802.11 Shared Key authentication as an access-point-issued challenge that the client encrypts and returns. See NIST SP 800-97: Establishing Wireless Robust Security Networks and Cisco's 802.11 authentication overview.

QUESTION NO: 12

Which of the following commands can be used for port scanning?

A. nc -z

B. nc -t

C. nc -w

D. nc –g

ANSWER: A

Explanation:

`nc -z` is correct because Netcat's `-z` option enables "zero-I/O" mode: it attempts to establish connections to target ports without sending application data. This makes it useful for basic TCP port-scanning and service-availability checks when paired with a host and a port or port range, such as `nc -zv target.example 1-1024`. A successful TCP connection indicates that the tested port is reachable and accepting connections; verbose mode (`-v`) is commonly added to display the results. Port scanning is a core reconnaissance activity in an authorized penetration test, helping the tester identify exposed network services for subsequent validation. Netcat implementations can differ slightly by operating system, so testers should consult the local `nc` manual page before use and ensure written authorization defines the allowed targets and scope. The OpenBSD Netcat manual documents `-z` as scanning for listening daemons without sending data, and Nmap's reference guide provides useful context on the purpose and interpretation of port-state discovery. See the OpenBSD nc manual and Nmap port-scanning basics.

QUESTION NO: 14

When you conduct the XMAS scanning using Nmap, you find that most of the ports scanned do not give a response. What can be the state of these ports?

A. Closed

B. Open

C. Filtered

D. Open or filtered

ANSWER: D

Explanation:

Open or filtered is the accurate Nmap result for an XMAS scan that receives no response. An XMAS scan is a TCP flag scan that sends a packet with the FIN, PSH, and URG flags set. Under the expected TCP behavior used by this technique, a closed port returns a TCP RST packet, while an open port silently drops the unexpected probe. However, a packet-filtering firewall may also silently discard the probe before it reaches the target service. Because both an open port and a filtered port can produce the same observable result—no reply—Nmap cannot reliably distinguish between those states and reports the port as `open|filtered`. This distinction is important during penetration testing: the lack of a response is not affirmative proof that a service is listening, but it does identify a port whose status warrants validation through additional scan types, service checks, or packet analysis. Nmap documents this classification for FIN, NULL, and XMAS scans in its port-state discussion and scan-technique reference: Nmap Port Scanning Basics and TCP NULL, FIN, and XMAS Scans.

QUESTION NO: 15

Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

A. Man-in-the-middle

B. ARP spoofing

C. Port scanning

D. Session hijacking

ANSWER: B

Explanation:

ARP spoofing is correct because it exploits the Address Resolution Protocol's lack of authentication on an Ethernet LAN. Hosts use ARP to map an IPv4 address to a MAC address and cache the mapping. An attacker can send forged ARP replies that associate the attacker-controlled MAC address with the IP address of a victim, the default gateway, or both. Once affected systems accept the poisoned cache entry, frames intended for the legitimate destination are sent to the attacker instead. The attacker can enable IP forwarding to relay the traffic while inspecting captured packets, placing themselves in the communications path. This supports sniffing of traffic that would otherwise be switched only to the legitimate destination. Alternatively, the attacker can decline to forward the received packets, interrupting communications and producing a denial-of-service condition. This is particularly relevant to local-network penetration testing because the attacker must generally be on the same broadcast domain as the systems whose ARP caches are being targeted. The MITRE ATT&CK technique entry describes ARP cache poisoning as a method for redirecting traffic, including adversary-in-the-middle activity: MITRE ATT&CK: ARP Cache Poisoning. Cisco also explains ARP's IP-to-MAC resolution role on local networks: Cisco ARP fundamentals.

QUESTION NO: 16

A penetration tester used a client-side browser exploit from metasploit to get an unprivileged shell prompt on the target Windows desktop. The penetration tester then tried using the getsystem command to perform a local privilege escalation which failed. Which of the following could resolve the problem?

A. Load priv module and try getsystem again

B. Run getuid command, then getpriv command, and try getsystem again

C. Run getuid command and try getsystem again

D. Use getprivs command instead of getsystem

ANSWER: A

Explanation:

Loading the `priv` module and then retrying `getsystem` is the appropriate corrective action. In Meterpreter's traditional extension model, Windows privilege-escalation functionality is provided by the `priv` extension. Loading it makes the privilege-related functionality available to the active Meterpreter session, including the techniques invoked by `getsystem`. Those techniques attempt to obtain a SYSTEM-level token through supported local escalation approaches, such as service or named-pipe impersonation methods, when the host and session context permit them.

The key operational point is that an unprivileged Meterpreter session alone does not guarantee that the privilege-escalation extension has been loaded. The tester should load the extension into the current session before rerunning the escalation attempt. Once it is loaded, Meterpreter can execute the `getsystem` workflow using the capabilities implemented for Windows privilege operations. Rapid7's Meterpreter command reference documents session commands and extension-based functionality, while the Metasploit Framework source shows the Windows privilege support used by post-exploitation operations. See the Meterpreter command reference and the Metasploit Windows privilege-support source.

QUESTION NO: 17

You've been contracted by the owner of a secure facility to try and break into their office in the middle of the night. Your client requested photographs of any sensitive information found as proof of your accomplishments. The job you've been hired to perform is an example of what practice?

A. Penetration Testing

B. Ethical Hacking

C. Vulnerability Assessing

D. Security Auditing

ANSWER: B

Explanation:

Ethical Hacking is correct because the activity is expressly authorized by the facility owner and is performed to identify and demonstrate real security weaknesses for the client's benefit. Ethical hacking applies adversarial techniques in a controlled engagement with defined permission, scope, and evidence requirements. In this scenario, the permitted attempt to enter the office after hours tests physical safeguards, such as access controls, locks, alarms, visitor procedures, and protection of sensitive material. Photographing exposed sensitive information provides evidence that the agreed-upon objective was achieved and enables the client to validate and remediate the finding. Authorization is the essential factor: the tester is not acting for personal gain or malicious purposes, but on behalf of the asset owner to improve security. GIAC's GPEN certification describes penetration testing work as planning and conducting penetration tests and documenting findings; authorized ethical-hacking engagements can include physical security testing where that activity is included in the approved rules of engagement. See the GIAC GPEN certification overview and NIST's Technical Guide to Information Security Testing and Assessment for guidance on authorized testing, planning, and reporting.

QUESTION NO: 18

Which of the following tools can be used by a user to hide his identity?

Each correct answer represents a complete solution. Choose all that apply.

A. IPchains

B. Rootkit

C. Proxy server

D. War dialer

E. Anonymizer

ANSWER: A C E

Explanation:

IPchains, when configured for IP masquerading, can conceal hosts on a private network behind a different externally visible source address. IP masquerading is a form of address translation: outbound traffic is presented as originating from the gateway rather than from the individual internal system. The historical IPchains documentation describes the `MASQ` target used for this purpose. Although IPchains is obsolete on modern Linux systems, its masquerading capability fits the question's identity-hiding context. See the IPchains manual page.

A **Proxy server** acts as an intermediary between a client and a destination service. When the proxy makes the outbound request, the destination normally sees the proxy's network address rather than the client's direct address. This can hide the client's network identity from the destination, subject to the proxy configuration and any identifying application-layer data forwarded in requests. The HTTP standard defines proxies as intermediaries that forward requests and responses; see RFC 9110, Intermediaries.

An **Anonymizer** is specifically intended to reduce linkability between a user and their network activity, commonly by routing traffic through intermediary systems or privacy-focused networks. It can therefore obscure the source identity visible to a target service, making it a direct match for the stated objective.

QUESTION NO: 19

Which of the following is the correct syntax to create a null session?

A. c:\>net view \\IP_addr\IPC$ "" /u: ""

B. c:\>net view \\IPC$\IP_addr "" /u: ""

C. c:\>net use \\IP_addr\IPC$ "" /u: ""

D. c:\>net use \\IPC$\IP_addr "" /u: ""

ANSWER: C

Explanation:

The command `c:\>net use \\IP_addr\IPC$ "" /u: ""` is the correct syntax for attempting to establish a null session to a remote Windows host. `net use` creates, manages, or removes a connection to a shared network resource. In this case, `\\IP_addr\IPC$` identifies the remote host's Interprocess Communication share, a special administrative share used for named pipes and remote service communication. Supplying an empty password (`""`) and an empty user name (`/u:""`) requests authentication without explicit credentials—the traditional null-session form. If the target permits anonymous access, Windows may establish the IPC$ connection under an anonymous security context, allowing the tester to evaluate what unauthenticated SMB/RPC information or services are exposed. The command's purpose is to create the connection; enumeration, where permitted, is a subsequent activity. Modern Windows versions and hardened environments commonly restrict anonymous IPC$ access through SMB and security-policy settings, so successful execution depends on the target configuration and authorization. Microsoft documents `net use` syntax and its role in connecting to shared resources at Net use. Microsoft's discussion of anonymous-access restrictions is available in SMB security guidance.

QUESTION NO: 21

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following pre-attack phases while testing the security of the server:

Footprinting Scanning Now he wants to conduct the enumeration phase. Which of the following tools can John use to conduct it?

Each correct answer represents a complete solution. Choose all that apply.

A. PsFile

B. PsPasswd

C. UserInfo

D. WinSSLMiM

ANSWER: A C

Explanation:

PsFile and **UserInfo** are appropriate for enumeration because they gather useful information about a Windows host, its users, and accessible resources without being exploitation tools. PsFile is a Microsoft Sysinternals utility that displays files opened remotely on a computer. During an authorized assessment, this can reveal active SMB file sharing activity, remotely accessed files, user names associated with connections, and potentially interesting shares or systems for further validation. Microsoft documents its remote-open-file listing capability in the PsFile documentation.

UserInfo is used to retrieve details associated with user accounts, supporting account and user enumeration. Identifying account names and related account attributes is a core enumeration activity because it helps an assessor understand the target's identity structure and evaluate exposure in a controlled, authorized manner. MITRE ATT&CK categorizes this type of activity as Account Discovery, describing the collection of account information from a local system or domain at MITRE ATT&CK: Account Discovery. Together, these tools support the enumeration objective of collecting actionable information about users and network-accessible resources after initial footprinting and scanning.

QUESTION NO: 22

John works as a Professional Penetration Tester. He has been assigned a project to test the Website security of www.we-are-secure Inc. On the We-are-secure Website login page, he enters ='or''=' as a username and successfully logs on to the user page of the Web site. Now, John asks the we-are-secure Inc. to improve the login page PHP script. Which of the following suggestions can John give to improve the security of the we-are-secure Website login page from the SQL injection attack?

A. Use the escapeshellarg() function

B. Use the session_regenerate_id() function

C. Use the mysql_real_escape_string() function for escaping input

D. Use the escapeshellcmd() function

E. Use prepared statements with parameterized queries for all user input.

ANSWER: E

Explanation:

Use prepared statements with parameterized queries for all login inputs. This approach separates the SQL command structure from user-supplied data: the database receives the query template first and receives the username and password values as bound parameters. Consequently, an input such as `='or''='` is handled strictly as a literal value rather than being interpreted as SQL syntax that can alter the authentication query's logic. In PHP, implementations should use a supported database interface such as PDO or MySQLi and bind every externally supplied value, including values that are expected to be numeric. Prepared statements should be combined with secure password storage and verification, for example PHP's `password_hash()` and `password_verify()`, but parameterization is the direct control that addresses this SQL injection condition. Escaping functions are not a preferred primary defense: correct escaping is database- and context-dependent, while the legacy MySQL extension containing `mysql_real_escape_string()` has been removed from modern PHP. The PHP PDO documentation describes preparing a statement and binding input parameters at PHP:

PDO::prepare. OWASP likewise identifies parameterized queries as the primary defense against SQL injection in its SQL Injection Prevention Cheat Sheet.

QUESTION NO: 23

You've been asked to test a non-transparent proxy lo make sure it is working. After confirming the browser is correctly pointed at the proxy, you try to browse a web site. The browser indicates it is "loading" but never displays any part the page. Checking the proxy, you see a valid request in the proxy from your browser. Checking the response to the proxy, you see the results displayed in the accompanying screenshot. Which of the following answers is the most likely reason the browser hasn't displayed the page yet?

A. The proxy is likely hung and must be restarted.

B. The proxy is configured to trap responses.

C. The proxy is configured to trap requests.

D. The site you are trying to reach is currently down.

ANSWER: C

Explanation:

The proxy is configured to trap requests. An intercepting, non-transparent web proxy sits between the browser and the destination server and can pause HTTP requests for review or modification before forwarding them. When request trapping is enabled, the browser successfully sends its request to the proxy, so the proxy will show a valid browser request; however, the proxy does not transmit that request onward until the operator explicitly forwards it or disables interception. The browser therefore remains in a loading state because it is still waiting for the transaction to complete and has not yet received page content. This behavior is normal during manual proxy testing and is useful in penetration testing because it allows the tester to inspect headers, parameters, cookies, and request bodies before they reach the application. Forwarding the trapped request, or turning request interception off, allows the proxy to continue the transaction and enables the browser to render the returned page. PortSwigger documents that intercepted requests are held until they are forwarded, dropped, or interception is disabled: Burp Suite Proxy: intercepting HTTP messages. The broader role of an intercepting proxy in examining web traffic is also described in Burp Suite Proxy documentation.

QUESTION NO: 24

A client has asked for a vulnerability scan on an internal network that does not have internet access. The rules of engagement prohibits any outside connection for the Nessus scanning machine. The customer has asked you to scan for a new critical vulnerability, which was released after the testing started, winch of the following methods of updating the Nessus plugins does not violate the rules of engagement?

A. Connect the scanning machine via wireless bridge and download the updated directly

B. Change the routing and connect through an alternative gateway

C. Proceed with the test and note the limitation of updating the plugins

D. Download the updates on an alternative machine and manually load on scanning machine

ANSWER: D

Explanation:

Download the updates on an alternative machine and manually load on scanning machine is correct because it preserves the explicit engagement restriction: the Nessus scanner itself never establishes an external connection. Nessus supports offline plugin updating, allowing the required plugin package to be obtained on a separate, Internet-connected system and then transferred to the isolated scanner through an approved mechanism, such as controlled removable media or an authorized internal file-transfer process. The tester should maintain the integrity of the update by obtaining it from Tenable, verifying any provided checksum or signature where applicable, documenting the package version and transfer method, and following the customer's media-handling procedures. Once loaded, the scanner can evaluate the newly disclosed vulnerability using current detection logic while remaining within the network boundary defined by the rules of engagement. This approach also provides an auditable record showing that no prohibited outbound connectivity occurred from the testing appliance. Tenable documents the offline-update workflow and associated plugin-package handling in its Nessus Offline Updates documentation. More generally, obtaining plugins and keeping them current is part of maintaining effective Nessus coverage, as described in Tenable's plugin documentation.

QUESTION NO: 25

Which of the following tools can be used as a Linux vulnerability scanner that is capable of identifying operating systems and network services?

Each correct answer represents a complete solution. Choose all that apply.

A. Cheops

B. Fport

C. Elsave

D. Cheops-ng

ANSWER: A D

Explanation:

Cheops and **Cheops-ng** are appropriate selections because both are Linux-oriented network-discovery and management tools that can identify reachable systems, infer operating-system characteristics, and enumerate network services. Cheops was an early graphical network-management application for Unix-like platforms. Its host-discovery and scanning functions use network probing to build information about devices and the services they expose, making it useful during reconnaissance and vulnerability-assessment work. Cheops-ng is the successor project and similarly provides graphical network discovery, mapping, and host/service information gathering. These capabilities support a penetration tester's need to identify the systems present on a target network and understand their exposed network-service footprint before conducting further assessment. Service enumeration and operating-system detection are foundational reconnaissance activities because they help establish the attack surface and guide subsequent validation of vulnerabilities. The tools' use of network scanning and fingerprinting is conceptually aligned with the host and service discovery techniques documented by the Nmap project, a widely used reference for this type of assessment activity. See the Nmap OS detection documentation and the Nmap service and version detection documentation for background on these reconnaissance functions.

QUESTION NO: 26

You run the following PHP script:

$password = mysql_real_escape_string($_POST["password"]);?>

What is the use of the mysql_real_escape_string() function in the above script.

Each correct answer represents a complete solution. Choose all that apply

A. It escapes all special characters from strings $_POST["name"] and $_POST["password"].

B. It escapes all special characters from strings $_POST["name"] and $_POST["password"] except ' and ".

C. It can be used to mitigate a cross site scripting attack.

D. It can be used as a countermeasure against a SQL injection attack.

ANSWER: A D

Explanation:

`mysql_real_escape_string()` escapes characters with special meaning in a SQL string literal, including quote characters and backslashes, before the supplied values are incorporated into a query. Its escaping behavior is tied to the active MySQL connection and its character set, which is important because SQL parsing depends on that connection context. Therefore, applying it to `$_POST["name"]` and `$_POST["password"]` is intended to transform potentially dangerous user-controlled input into escaped string content suitable for inclusion in a properly quoted SQL statement.

Escaping SQL metacharacters is a historical countermeasure against SQL injection because it prevents attacker-supplied quote and escape characters from prematurely terminating a string literal or changing the intended query syntax. The PHP documentation specifically describes this function as escaping special characters in a string for use in an SQL statement: PHP manual: mysql_real_escape_string. In modern PHP applications, prepared statements with parameterized queries are the preferred defense, since query structure and data are handled separately. OWASP similarly identifies parameterized queries as the primary protection against injection: OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 27 - (SIMULATION)

Fill in the blank with the appropriate tool.

____scans IP networks for NetBIOS name information and works in the same manner as nbtstat, but it operates on a range of addresses instead of just one.

ANSWER: See the explanation for the answer

Explanation:

Answer: `nbtscan`

`nbtscan` scans IP address ranges for NetBIOS name information. It performs a function similar to `nbtstat`, but unlike `nbtstat`, it is designed to enumerate multiple hosts across a network range.

```
nbtscan 192.168.1.0/24
```

QUESTION NO: 28

Which of the following tools allow you to perform HTTP tunneling?

Each correct answer represents a complete solution. Choose all that apply.

A. BackStealth

B. Tunneled

C. Nikto

D. HTTPort

ANSWER: A B D

Explanation:

BackStealth, Tunneled, and HTTPort are tools intended to tunnel communications through HTTP or HTTPS-style web traffic. HTTP tunneling encapsulates another protocol or an interactive connection within HTTP requests and responses, allowing a client and server component to carry traffic through environments where web access is permitted but direct outbound connections are restricted. HTTPort is a well-known example: it provides a local proxy-like endpoint and relays supported traffic through an HTTP-based tunnel to a remote server. BackStealth is similarly associated with concealing or relaying remote communications through web traffic, while Tunneled is designed for the same general HTTP-tunneling use case. In a penetration-testing context, recognizing these tools is useful for assessing whether egress controls, web proxies, and traffic inspection can detect unauthorized tunneling rather than merely allowing outbound HTTP traffic. Effective defenses commonly include authenticated proxies, destination allowlisting, TLS inspection where appropriate and authorized, and behavioral monitoring for unusual long-lived or high-volume HTTP sessions. The HTTPort project is documented at SourceForge: HTTPort; broader testing guidance for assessing network controls and tunneling exposure is available in the OWASP Web Security Testing Guide.

QUESTION NO: 29

You have compromised a Windows XP system and Injected the Meterpreter payload into the lsass process. While looking over the system you notice that there is a popular password management program on the system. When you attempt to access the file that contains the password you find it is locked. Further investigation reveals that it is locked by the passmgr process. How can you use the Meterpreter to get access to this file?

A. Use the getuid command to determine the user context the process is runningunder, then use the imp command to impersonate that user.

B. use the getpid command to determine the user context the process is runningunder, then use the Imp command to impersonate that user.

C. Use the execute command to the passmgr executable. That will give you access to the file.

D. Use the migrate command to jump to the passmgr process. That will give you accessto the file.

ANSWER: D

Explanation:

Use the migrate command to jump to the passmgr process. That will give you accessto the file. Meterpreter's `migrate` command moves the active Meterpreter session into a specified running process. In this situation, migrating into the password manager's process places the session in the same process context that opened and currently holds the password file. This lets the tester interact through the process that already has the relevant file access and handle state, rather than attempting to open a file that is locked from the original Meterpreter process. Migration is also a standard Meterpreter post-exploitation technique for changing the session's process context when a target application process is more useful for a specific task. The target process must be selected by its process identifier, typically identified through Meterpreter process-listing functionality, and the session must have sufficient rights to inject into it. Rapid7 documents Meterpreter's process migration capability in its Meterpreter Basics guide. The related Meterpreter command reference is available in the Metasploit Documentation.

QUESTION NO: 30

Which of the following statements about SSID is NOT true?

A. Default settings of SSIDs are secure.

B. All wireless devices on a wireless network must have the same SSID in order to communicate with each other.

C. It acts as a password for network access.

D. It is used to identify a wireless network.

ANSWER: A

Explanation:

“Default settings of SSIDs are secure.” is the statement that is not true. An SSID is the service set identifier: the network name advertised or configured for an IEEE 802.11 wireless LAN. It is an identifier, not a security control, and changing or hiding it does not provide meaningful protection against an attacker who can observe wireless-management traffic. Default SSID configurations are especially unsuitable as an assurance of security because they may disclose the access-point vendor or model and are commonly known or easily discovered. Wireless-network security should instead be based on properly configured authentication and encryption, such as WPA2 or WPA3 with strong credentials, along with sound access-point administration. The National Institute of Standards and Technology notes that SSIDs are not secret and that WLAN security depends on appropriate security mechanisms rather than obscuring network identifiers. See NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks. Cisco likewise describes the SSID as a name that identifies a WLAN, while access protection is provided through configured security policies and authentication. See Cisco WLAN Overview documentation.

QUESTION NO: 31

You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure. com network. Now, when you have finished your penetration testing, you find that the weare- secure.com server is highly vulnerable to SNMP enumeration. You advise the we-are-secure Inc. to turn off SNMP; however, this is not possible as the company is using various SNMP services on its remote nodes. What other step can you suggest to remove SNMP vulnerability?

Each correct answer represents a complete solution. Choose two.

A. Close port TCP 53.

B. Change the default community string names.

C. Upgrade SNMP Version 1 with the latest version.

D. Install antivirus.

ANSWER: B C

Explanation:

Changing the default community string names is an essential SNMP hardening measure when SNMPv1 or SNMPv2c must remain in use. Community strings function as shared credentials in these versions, and default or easily guessed values such as *public* and *private* allow unauthorized parties to query management information or, where write access is enabled, alter device configuration. They should be replaced with unique, strong values and assigned the minimum necessary read-only or read-write access. NIST guidance recognizes that SNMPv1 and SNMPv2c community strings are sent without cryptographic protection and therefore should not be used where stronger protection is available.

Upgrading SNMP Version 1 with the latest version means migrating to SNMPv3. SNMPv3 supports user-based authentication and privacy protections, allowing management traffic to be authenticated and, when configured, encrypted. This prevents the cleartext credential exposure and unauthenticated enumeration risks inherent in earlier SNMP versions. SNMPv3 should be configured with strong authentication and privacy settings, distinct user credentials, and least-privilege authorization. See NIST SP 800-53 Rev. 5 for secure management protocol expectations and RFC 3414 for the SNMPv3 User-based Security Model.

QUESTION NO: 32

Joseph works as a Network Administrator for WebTech Inc. He has to set up a centralized area on the network so that each employee can share resources and documents with one another. Which of the following will he configure to accomplish the task?

A. WEP

B. VPN

C. Intranet

D. Extranet

ANSWER: C

Explanation:

Intranet is correct because it is a private network environment designed for an organization's internal users. It provides a centralized, access-controlled location where employees can publish, locate, and share documents, internal applications, collaboration tools, policies, and other organizational resources. Intranet services commonly use standard web technologies, such as web servers, browsers, authentication, and permissions, while restricting access to authorized personnel on the company network or connected through approved remote-access mechanisms.

For WebTech's requirement, an intranet creates the internal collaboration space needed for employees to exchange information and resources without making those materials publicly available. The network administrator can further apply role-based access controls, secure authentication, shared storage permissions, and auditing to ensure that users access only the resources appropriate to their jobs. This use aligns with the general definition of an intranet as a private network for sharing information within an organization. The U.S. National Institute of Standards and Technology discusses enterprise security architectures and access controls that support protected internal services in NIST SP 800-207. Microsoft also documents internal collaboration and document-sharing capabilities in SharePoint documentation, a common platform used to implement intranet-style services.

QUESTION NO: 33

Which of the following federal laws are related to hacking activities?

Each correct answer represents a complete solution. Choose three.

A. 18 U.S.C. 1030

B. 18 U.S.C. 1028

C. 18 U.S.2510

D. 18 U.S.C. 1029

ANSWER: A C D

Explanation:

18 U.S.C. 1030 is the Computer Fraud and Abuse Act, the principal U.S. federal statute addressing unauthorized access to protected computers. Its prohibited conduct includes intentionally accessing a computer without authorization or exceeding authorized access, obtaining information, causing damage, trafficking in passwords, and certain extortion involving computers. These are core activities encountered in hacking investigations and penetration-testing legal discussions. The statutory text is available through the U.S. House Office of the Law Revision Counsel.

18 U.S.2510 is part of the federal Wiretap Act framework. Although this section primarily defines terms used throughout the chapter, those definitions govern the related restrictions on intercepting wire, oral, and electronic communications. Capturing network communications, intercepting data in transit, and using interception tools can therefore implicate this legal framework. The chapter's definitions and related provisions are published at 18 U.S.C. Chapter 119.

18 U.S.C. 1029 addresses fraud and related activity involving access devices, including unauthorized access-device use, trafficking, and possession of device-making equipment in specified circumstances. Because compromises may involve payment-card numbers, account credentials, authentication tokens, or tools used to create or misuse access devices, this statute is directly relevant to many computer-enabled intrusion and fraud cases.

QUESTION NO: 35

You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement?

Each correct answer represents a complete solution. Choose two.

A. MAC filtering the router

B. Using WPA encryption

C. Using WEP encryption

D. Not broadcasting SSID

ANSWER: A B

Explanation:

Using WPA encryption is a sound baseline security measure because modern WPA-family protections authenticate access to the wireless network and encrypt traffic sent over the radio link. In a current deployment, WPA3-Personal is preferred where client support permits it; WPA2 with AES/CCMP remains the practical compatibility baseline for many guest environments. A coffee shop should also isolate guests from internal business systems through a separate guest network or VLAN, but wireless encryption remains an important control for the access layer. The Wi-Fi Alliance describes WPA3's strengthened wireless protections at https://www.wi-fi.org/discover-wi-fi/security.

MAC filtering the router can provide an additional access-control measure by permitting only configured wireless client hardware addresses. It is most useful in a small, managed environment where staff can maintain an allowlist and where it supplements stronger controls such as WPA encryption and network segmentation. NIST identifies MAC-address filtering as one of the access-control techniques that may be used for WLANs, while emphasizing that wireless security should use layered safeguards. See NIST's guidance in SP 800-153, Guidelines for Securing Wireless Local Area Networks.

QUESTION NO: 36

Which of the following is a web ripping tool?

A. Netcat

B. NetBus

C. SuperScan

D. Black Widow

ANSWER: D

Explanation:

Black Widow is a web ripping tool: it crawls a target website, follows links, and downloads or mirrors site content for offline inspection. In penetration-testing and web-assessment contexts, this kind of tool is useful for mapping a site's reachable content, identifying linked files and directories, collecting pages for review, and understanding the application's exposed structure. "Ripping" refers to recursively retrieving web resources rather than simply making an individual HTTP request or performing a port scan. BlackWidow's documentation describes the product as a website scanner and site-mapping utility, with capabilities to scan sites and gather site content and links. This aligns with the web-ripping classification used in common security-tool taxonomies. For further product details, see the BlackWidow Website Scanner page. More broadly, OWASP recognizes application mapping and discovery as important activities during web security testing; see the OWASP Web Security Testing Guide: Information Gathering.