PassQueen
a.k.a dumpsqueen.com

Certified Professional Ethical Hacker (CPEH)

GAQM CPEH-001

Version Demo

Total Demo Questions: 86

Total Premium Questions: 867

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to Ethical Hacking	67
Topic 2, Footprinting and Reconnaissance	60
Topic 3, Scanning Networks	107
Topic 4, Enumeration	29
Topic 5, System Hacking	79
Topic 6, Malware Threats	31
Topic 7, Sniffing	55
Topic 8, Social Engineering	27
Topic 9, Denial of Service	10
Topic 10, Session Hijacking	10
Topic 11, Hacking Web Servers	21
Topic 12, Hacking Web Applications	51
Topic 13, SQL Injection	18
Topic 14, Hacking Wireless Networks	32
Topic 15, Evading IDS, Firewalls, and Honeypots	70
Topic 16, Cloud Computing	4
Topic 17, Cryptography	120
Topic 18, Penetration Testing	54
Topic 19, Mix Questions	22
Total	867

QUESTION NO: 1

What is the minimum number of network connections in a multi homed firewall?

A. 3

B. 5

C. 4

D. 2

ANSWER: D

Explanation:

The correct answer is **2**. A multihomed firewall must connect to at least two distinct network segments so that it can inspect, control, and enforce policy on traffic passing between them. In the minimum deployment, one interface is connected to a less-trusted network, such as the Internet or another external network, and the other is connected to a more-trusted internal network. The firewall acts as the controlled boundary between these networks and applies its rules to traffic that attempts to traverse that boundary.

“Multihomed” describes a host or security device with more than one network interface or network attachment. This differs from the number of hosts, routes, or security zones that may exist in a particular enterprise design. A production firewall can have additional interfaces for a DMZ, management network, guest network, partner connection, or separate security zones, but those are extensions of the basic architecture rather than a minimum requirement. NIST describes firewalls as devices or systems that control traffic between networks with differing trust levels, while the Internet standards recognize multihomed hosts as systems using multiple interfaces. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and RFC 1122.

QUESTION NO: 2

The following are types of Bluetooth attack EXCEPT_____?

A. Bluejacking

B. Bluesmacking

C. Bluesnarfing

D. Bluedriving

ANSWER: D

Explanation:

Bluedriving is the correct exception because it refers to discovering and cataloging Bluetooth-enabled devices while moving through an area, much like wireless wardriving. It is principally a reconnaissance or device-discovery activity: an assessor uses Bluetooth scanning to identify devices that are visible, determine their Bluetooth addresses and advertised information, and map where devices can be found. By itself, this process does not exploit a Bluetooth vulnerability, alter a device, access protected data, or disrupt Bluetooth communications. It may be used during the information-gathering phase of an ethical hacking engagement to identify potential targets and assess Bluetooth exposure, but it is not itself categorized as a direct Bluetooth attack. Bluetooth security guidance emphasizes that device discovery and visibility settings affect what information can be exposed to nearby scanners; organizations should disable discoverability when it is not required and use appropriate pairing and authentication controls. See the Bluetooth discovery and security discussion in NIST SP 800-121 Rev. 2, Guide to Bluetooth Security and the Bluetooth security recommendations from the UK National Cyber Security Centre.

QUESTION NO: 3

A security administrator is reviewing a packet capture and observes a TCP connection beginning with SYN, SYN/ACK, and ACK packets.

What does this sequence represent?

A. The TCP three-way handshake

B. A UDP session establishment

C. A TCP connection teardown

D. An ICMP echo exchange

ANSWER: A

Explanation:

The TCP three-way handshake is correct because it is the normal process used to establish a TCP connection. The client sends a SYN packet to request a connection, the server replies with SYN/ACK to acknowledge the request and synchronize its own sequence number, and the client sends an ACK to complete the setup. After this exchange, both endpoints can transmit application data.

Observing this sequence during an authorized assessment or incident investigation confirms that a TCP service accepted the connection attempt. It does not, by itself, identify the application protocol; the destination port and subsequent payload must be examined for that purpose. TCP connection establishment is specified in RFC 9293: Transmission Control Protocol.

QUESTION NO: 4

Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?

A. Service Oriented Architecture

B. Object Oriented Architecture

C. Lean Coding

D. Agile Process

ANSWER: A

Explanation:

Service Oriented Architecture is correct because it is an architectural design approach in which discrete, self-contained software services expose business or application capabilities for use by other applications. A service has a defined interface and can be invoked through a communication mechanism, commonly across a network. This separation enables systems to use capabilities such as authentication, customer lookup, payment processing, or reporting without needing to embed the implementation of each capability directly in every consuming application.

The key idea in Service Oriented Architecture is that functionality is organized and delivered as interoperable services. Consumers depend on a service contract—what the service does, the inputs it accepts, and the outputs it returns—rather than on its internal implementation. This supports reuse, integration between heterogeneous systems, independent evolution of components, and clearer boundaries between application responsibilities. These characteristics directly match the question's description of distinct software pieces providing functionality to other applications as services. The OASIS SOA Reference Model describes SOA as a paradigm for organizing and using distributed capabilities that may be under different ownership domains. See the OASIS SOA Reference Model and the NIST glossary definition of service-oriented architecture.

QUESTION NO: 5

What are two things that are possible when scanning UDP ports? (Choose two.)

A. A reset will be returned

B. An ICMP message will be returned

C. The four-way handshake will not be completed

D. An RFC 1294 message will be returned

E. Nothing

ANSWER: B E

Explanation:

When a UDP probe is sent to a closed UDP port, the target host can return an ICMP Destination Unreachable message, specifically the Port Unreachable condition. This is the principal definitive response used by UDP scanners to identify a port as closed. UDP is connectionless, so there is no transport-layer connection setup or teardown before the scanner sends its probe; the result depends on whether the UDP service or the network stack generates a response.

Nothing is also a valid and common result of a UDP-port scan. An open UDP service often silently drops an unexpected or empty probe rather than replying. Firewalls and packet filters may also discard UDP probes or their responses without informing the scanner. Consequently, a scanner commonly classifies a port with no response as *open|filtered*, because silence alone cannot distinguish an open service that did not reply from filtering that prevented the probe or response from being observed. Nmap documents both ICMP port-unreachable responses for closed UDP ports and the open|filtered classification resulting from no response. See the Nmap UDP Scan documentation and RFC 1122 ICMP error-message requirements.

QUESTION NO: 6

Which Metasploit Framework tool can help penetration tester for evading Anti-virus

Systems?

A. msfpayload

B. msfcli

C. msfencode

D. msfd

ANSWER: C

Explanation:

msfencode is the correct answer in the context of the older Metasploit Framework toolset covered by this question. It was a command-line utility for applying Metasploit encoders to payload shellcode. Encoders transform the payload's byte representation and include a decoder stub so that the intended payload can execute after decoding in memory. During an authorized penetration test, this capability could be used to assess whether an endpoint security product detects a payload only through a simple static signature or can identify the payload through behavioral and memory-based detection techniques. Thus, msfencode was associated with payload encoding and historical antivirus-evasion testing workflows.

Encoding should be understood as a controlled testing technique, not as a guarantee of bypassing modern antivirus or endpoint detection and response products. Current security tools commonly use behavioral analysis, emulation, reputation, memory inspection, and other detection layers in addition to static signatures. Metasploit later consolidated legacy payload-generation and encoding functions into `msfvenom`; however, the historical tool name expected by this question is msfencode. Rapid7's documentation describes Metasploit payload handling at Working with Payloads, and the Metasploit documentation provides current usage guidance at Metasploit Documentation.

QUESTION NO: 7

A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database.

In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

A. Semicolon

B. Single quote

C. Exclamation mark

D. Double quote

ANSWER: B

Explanation:

Single quote is correct because it is commonly used as an initial, low-impact probe when assessing a parameter for SQL injection during an authorized web-application test. SQL string literals are frequently delimited with single quotation marks. If an application incorporates user-controlled input into a SQL statement without correct parameterization or escaping, supplying a single quote can terminate the expected string context and cause a database syntax error, altered application behavior, or another observable indication that the input may reach a SQL query. This makes it a useful first diagnostic character for determining whether further, carefully controlled validation is warranted.

The test should be performed only within the agreed scope and with attention to application stability, logging, and the possibility that errors are intentionally suppressed. A quote alone does not prove exploitability; the tester should correlate any response with the input point and then use safe, methodical testing to establish whether the application uses parameterized queries and whether injection is actually possible. OWASP's testing guidance identifies quote characters as a standard way to test SQL query behavior, while OWASP's prevention guidance emphasizes prepared statements with parameterized queries as the primary defense. See the OWASP SQL Injection overview and the OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 8

The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the

EF = 1 (100%).

What is the closest approximate cost of this replacement and recovery operation per year?

A. $146

B. $1320

C. $440

D. $100

ANSWER: A

Explanation:

$146 is the closest available annual cost. The single loss expectancy (SLE) is the complete cost incurred for one hard-drive failure. Here, replacement hardware costs $300, while recovery labor takes 14 total hours: 10 hours to restore the operating system and software plus 4 hours to restore the database. At $10 per hour, labor is $140, making the SLE $440. Because the exposure factor is 100%, the entire stated loss is included in the SLE.

The annual rate of occurrence (ARO) is one failure every three years, or 1/3 per year (approximately 0.33). Annualized loss expectancy (ALE) is calculated as SLE multiplied by ARO: $440 × 1/3 = $146.67 per year. Since the question asks for the closest approximate yearly cost and the listed value is expressed in whole dollars, $146 is the intended answer. This calculation provides a quantitative estimate of the expected annual financial impact of this specific failure scenario, supporting cost-based decisions about backups, spare hardware, redundancy, and recovery controls. NIST's risk-

management guidance describes risk assessment as considering loss magnitude and likelihood; see NIST SP 800-30 Rev. 1. For the standard ALE terminology and formula, see the Annualized loss expectancy overview.

QUESTION NO: 9

Which regulation defines security and privacy controls for Federal information systems and organizations?

A. NIST-800-53

B. PCI-DSS

C. EU Safe Harbor

D. HIPAA

ANSWER: A

Explanation:

NIST-800-53 is correct because NIST Special Publication 800-53 is the authoritative federal control catalog titled *Security and Privacy Controls for Information Systems and Organizations*. It establishes a comprehensive set of security and privacy controls that federal agencies use to protect information systems, manage privacy risks, and support compliance with the Federal Information Security Modernization Act framework. The publication organizes controls into families such as access control, incident response, contingency planning, risk assessment, system and communications protection, and personally identifiable information processing and transparency.

Under the Risk Management Framework, federal organizations select, tailor, implement, assess, authorize, and continuously monitor controls using this catalog in accordance with system impact and organizational risk considerations. Although the question calls it a regulation, NIST Special Publication 800-53 is more precisely a NIST control standard and guidance publication used to meet federal information-security requirements. Its scope explicitly addresses both security and privacy controls for information systems and organizations, which directly matches the wording of the question. The current publication and its control catalog are available from NIST SP 800-53 Release 5, Update 1; its role within federal risk management is described by NIST's Risk Management Framework.

QUESTION NO: 10

Study the log below and identify the scan type.

```
tcpdump -vv host 192.168.1.10
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 36166)
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 33796)
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 47066)
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74 0 (ttl 48, id 35585)
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 32834)
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 26292)
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 51058)

tcpdump -vv -x host 192.168.1.10
17:35:06.731739 eth0 < 192.168.1.10 > victim: ip-proto-130 0 (ttl 59, id 42060)
4500 0014 a44c 0000 3b82 57b8 c0a8 010a c0a8 0109 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
```

A. nmap -sR 192.168.1.10

B. nmap -sS 192.168.1.10

C. nmap -sV 192.168.1.10

D. nmap -sO 192.168.1.10

ANSWER: D

Explanation:

`nmap -sO 192.168.1.10` is an IP protocol scan. Rather than testing TCP or UDP port numbers, this scan determines which IP protocols the target host supports. Nmap sends IP packets using different protocol numbers in the IP header and interprets the target's responses, including ICMP Protocol Unreachable messages, to identify protocol numbers that appear open, closed, or filtered. This produces traffic that is characteristic of IP-protocol enumeration, not an ordinary TCP SYN, service-version, or RPC scan. The corrected command omits the incomplete `-T` timing option; when used, `-T` must be followed by a timing template number such as `-T4`. Nmap documents `-sO` as its IP protocol scan option and explains that it is intended to discover supported IP protocols, such as ICMP, TCP, UDP, and others. See the Nmap IP Protocol Scan documentation and the Nmap timing and performance documentation.

QUESTION NO: 11

SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts. Which of the following features makes this possible?

(Choose two.)

A. It used TCP as the underlying protocol.

B. It uses community string that is transmitted in clear text.

C. It is susceptible to sniffing.

D. It is used by all network devices on the market.

ANSWER: B C

Explanation:

It uses community string that is transmitted in clear text. is correct because SNMPv1 and SNMPv2c use a community string as a simple shared credential. In these versions, the community value is included in SNMP messages without cryptographic protection. If a weak, default, or discovered read-only community string is accepted by an SNMP agent, an authorized query can enumerate management information from MIB objects, including interface details, routing-related data, system descriptions, process information where exposed, and other operational data. RFC 1157 specifies that the community name is carried in the SNMP message structure, and its security model does not provide modern confidentiality protection.

It is susceptible to sniffing. is also correct because unprotected SNMPv1/v2c traffic can be captured from a network segment and inspected. Packet capture can reveal community strings as well as the management requests and responses exchanged between an SNMP manager and agent. This enables an attacker who can observe the traffic to learn usable access values and identify valuable device and configuration information. Current security guidance therefore favors SNMPv3, which supports authentication and privacy features to protect management traffic. See RFC 1157: A Simple Network Management Protocol and CISA guidance on using SNMPv3 securely.

QUESTION NO: 12

Which of the following act requires employer's standard national numbers to identify them on standard transactions?

A. SOX

B. HIPAA

C. DMCA

D. PCI-DSS

ANSWER: B

Explanation:

HIPAA is correct because its Administrative Simplification provisions established national standards for electronic health-care transactions and for unique identifiers used by covered entities. Within this framework, employers participating in health-plan administration must be identified consistently in standard transactions. The employer identifier adopted for this purpose is the Employer Identification Number issued by the Internal Revenue Service. Using a standard identifier allows health plans, providers, clearinghouses, and related entities to process eligibility, enrollment, claims, and payment information with an unambiguous employer identity. This supports the interoperability and administrative-efficiency goals of HIPAA's transaction and code-set requirements while reducing errors caused by locally assigned or inconsistent employer identifiers. The statutory requirement for a unique health identifier for employers appears in HIPAA's Administrative Simplification provisions, and federal implementation materials explain that the Employer Identification Number is used as the employer identifier in standard transactions. The Centers for Medicare & Medicaid Services provides an overview of these HIPAA Administrative Simplification standards at https://www.cms.gov/regulations-and-guidance/administrative-simplification/hipaa-aca. The underlying statutory text is available through https://www.govinfo.gov/content/pkg/USCODE-2023-title42/html/USCODE-2023-title42-chap7-subchapXI-partC.htm.

QUESTION NO: 13

A newly discovered flaw in a software application would be considered which kind of security vulnerability?

A. Input validation flaw

B. HTTP header injection vulnerability

C. 0-day vulnerability

D. Time-to-check to time-to-use flaw

ANSWER: C

Explanation:

0-day vulnerability is correct because the term describes a previously unknown software flaw for which the affected vendor has had zero days to develop and distribute a fix. The key characteristic is not the technical mechanism of the flaw, such as how input is processed or whether a race condition exists, but its newly discovered and unremediated status. A zero-day may be known first to an attacker, a security researcher, or the vendor; in all cases, the organization responsible for the software has not yet had time to make a protective patch broadly available. Such vulnerabilities require prompt assessment because attackers can potentially exploit them before normal patch management can address the exposure. Defensive actions commonly include monitoring vendor advisories, applying temporary mitigations or configuration changes, increasing detection coverage, and deploying the vendor's update as soon as it is available. CISA explains that zero-day vulnerabilities are flaws that have been discovered but not yet patched, while NIST's glossary defines a zero-day attack in terms of exploiting a previously unknown vulnerability before a fix exists. See CISA's zero-day vulnerability overview and the NIST CSRC glossary entry for zero-day attack.

QUESTION NO: 14

Which of the following are common indicators that an email message may be a phishing attempt? (Choose three.)

A. An unexpected request to verify account credentials

B. A sender domain that differs from the organization being claimed

C. A hyperlink that leads to a different domain than the text displayed

D. A message delivered through an organization-approved mail gateway

E. A digitally signed message with a valid trusted certificate

ANSWER: A B C

Explanation:

An unexpected request for credentials, a mismatched sender domain, and a link whose actual destination differs from its displayed text are common phishing indicators. Phishing messages often impersonate trusted organizations and attempt to create urgency so that a recipient discloses credentials, opens a malicious attachment, or visits an attacker-controlled site.

A legitimate-looking display name or logo alone does not establish that a message is trustworthy. Recipients should inspect the complete sender address, independently verify urgent requests, and hover over links or otherwise validate destinations before interacting with them. CISA provides phishing-recognition guidance at Recognize and Report Phishing.

QUESTION NO: 15

Elliot is in the process of exploiting a web application that uses SQL as a back-end database. He's determined that the application is vulnerable to SQL injection, and has introduced conditional timing delays into injected queries to determine whether they are successful. What type of SQL injection is Elliot most likely performing?

A. Error-based SQL injection

B. Blind SQL injection

C. Union-based SQL injection

D. NoSQL injection

ANSWER: B

Explanation:

Blind SQL injection is correct because Elliot is using the application's response time as an indirect signal of whether an injected SQL condition evaluated as intended. This is specifically the time-based form of blind SQL injection. Rather than receiving database values or detailed query errors directly in the HTTP response, an attacker injects a conditional expression that causes the database to pause only when a tested condition is true. For example, the attacker can test whether a character in a database value matches a guess and observe whether the server response is delayed. Repeating these true-or-false tests enables data extraction even when the application does not visibly display query results. The defining characteristic is that the attacker infers information from observable behavior—here, timing—rather than from returned SQL output. OWASP describes blind SQL injection as an attack in which attackers ask the database true-or-false questions and infer answers from changes in application behavior, including time delays. PortSwigger likewise identifies conditional delays as a standard technique for time-based blind SQL injection. See OWASP: Blind SQL Injection and PortSwigger Web Security Academy: Blind SQL injection.

QUESTION NO: 16

Which of the following security controls help reduce the risk of unauthorized wireless-network access? (Choose three.)

A. Use WPA3-Enterprise or WPA2-Enterprise with 802.1X authentication

B. Disable WEP security

C. Place guest wireless users on a separate network

D. Rely only on a hidden SSID for access control

E. Use the same shared password permanently for all employees and guests

ANSWER: A B C

Explanation:

Using WPA3-Enterprise or WPA2-Enterprise with 802.1X authentication, disabling obsolete WEP security, and maintaining a separate guest network are effective controls. Enterprise wireless authentication can require individual user or device credentials and supports centralized access control. WEP is obsolete because its cryptographic design is vulnerable and should not be used. A separate guest network limits exposure by keeping visitor devices away from internal systems and sensitive resources.

Changing the SSID alone does not provide meaningful authentication or encryption, and hiding the SSID is not a reliable access-control measure because wireless management traffic can still reveal the network name. NIST provides wireless-security recommendations in SP 800-153, Guidelines for Securing Wireless Local Area Networks.

QUESTION NO: 17

Which of the following tools are used for enumeration? (Choose three.)

A. SolarWinds

B. USER2SID

C. SID2USER

D. DumpSec

ANSWER: B C D

Explanation:

USER2SID, **SID2USER**, and **DumpSec** are enumeration tools because they help an assessor identify accounts, identifiers, group relationships, and permissions exposed by a Windows environment. USER2SID translates a known Windows account name into its security identifier (SID), while SID2USER performs the reverse lookup from an SID to an account name. These mappings are valuable during Windows and SMB enumeration because SIDs identify security principals and may reveal domain or local-account naming information. Microsoft explains that SIDs are unique values used to identify security principals such as users and groups: Understand Security Identifiers.

DumpSec is a Windows security-reporting and enumeration utility that can collect details such as user and group membership, password-policy information, shares, and file-system permissions. Such information helps ethical hackers document the target's accessible security configuration and identify accounts or authorization relationships that warrant further authorized testing. This fits the broader reconnaissance and enumeration workflow, in which services and exposed identity information are systematically queried and recorded. For general guidance on discovering and enumerating services in an authorized assessment, see the Nmap Reference Guide.

QUESTION NO: 18

Assume a business-crucial web-site of some company that is used to sell handsets to the customers worldwide. All the developed components are reviewed by the security team on a monthly basis. In order to drive business further, the web-site developers decided to add some 3rd party marketing tools on it. The tools are written in JavaScript and can track the customer's activity on the site. These tools are located on the servers of the marketing company.

What is the main security risk associated with this scenario?

A. External script contents could be maliciously modified without the security team knowledge

B. External scripts have direct access to the company servers and can steal the data from there

C. There is no risk at all as the marketing services are trustworthy

D. External scripts increase the outbound company data traffic which leads greater financial losses

ANSWER: A

Explanation:

External script contents could be maliciously modified without the security team knowledge is correct because JavaScript loaded from a third-party marketing provider is executed by the customer's browser within the security context of the company's website. The website may have been reviewed at the time the external script tag was added, but the provider can subsequently change the content delivered from its own servers without any change to the company's application code or a new internal security review. If the provider's infrastructure, deployment process, or account is compromised, an attacker can inject code into the marketing script. That code can interact with page content available to the site, observe customer activity, alter transactions or displayed information, and potentially collect sensitive data entered into pages where the script executes. This is a supply-chain risk: trust in a third-party dependency extends to every visitor who loads it. OWASP describes third-party JavaScript as a common client-side supply-chain exposure and recommends controlling, monitoring, and applying browser protections to such dependencies. Subresource Integrity can also allow a browser to verify that a fetched script matches an expected cryptographic hash, where using a versioned, static asset is practical. See the OWASP Subresource Integrity guidance and MDN's Subresource Integrity documentation.

QUESTION NO: 19

Which of the following is a symmetric cryptographic standard?

A. DSA

B. PKI

C. RSA

D. 3DES

ANSWER: D

Explanation:

3DES is a symmetric cryptographic standard because it encrypts and decrypts data using the same shared secret key. Formally known as the Triple Data Encryption Algorithm (TDEA), it applies the underlying Data Encryption Standard operation three times, typically with either two or three independently managed keys. Symmetric encryption is designed for efficiently protecting bulk data when communicating parties can securely establish and protect the shared key. This makes it distinct from cryptographic systems used primarily for public-key operations, such as signatures, key establishment, or certificate-based trust management. Although 3DES was widely deployed in legacy financial and enterprise environments, it is now being retired for most new uses because its 64-bit block size creates practical security limitations when encrypting substantial volumes of data. The National Institute of Standards and Technology states that TDEA encryption was disallowed after December 31, 2023, except for limited legacy decryption and key-unwrapping purposes. Modern implementations should generally use AES, another symmetric encryption standard, instead. Nevertheless, 3DES remains the correct classification in this question because it is unequivocally a symmetric-key encryption algorithm. See NIST SP 800-67 Rev. 2 and NIST's TDEA retirement notice.

QUESTION NO: 20

Which of the following practices support the principle of least privilege in a cloud identity and access management environment? (Choose three.)

A. Assign narrowly scoped roles to users and workloads

B. Review and remove unused permissions regularly

C. Use separate accounts or roles for administrative tasks

D. Grant administrator access to all developers by default

E. Share one administrator account among the operations team

ANSWER: A B C

Explanation:

Assigning permissions through narrowly scoped roles limits users and workloads to only the actions and resources required for their legitimate duties. Reviewing and removing unused permissions is also essential because access often accumulates when employees change roles, projects end, or temporary accounts remain active.

Using separate accounts or roles for administrative tasks helps ensure that highly privileged permissions are used only when needed and improves accountability in audit records. Granting broad administrator rights by default or sharing administrator credentials violates least privilege and makes security investigation more difficult. NIST defines least privilege as restricting access to the minimum necessary for authorized functions in its least privilege glossary entry. Guidance for managing cloud access is also available from the CISA Cloud Security Technical Reference Architecture.

QUESTION NO: 21

Which of the following actions are appropriate during the containment phase of an incident involving a compromised workstation? (Choose two.)

A. Isolate the affected workstation from the network

B. Preserve relevant logs and volatile evidence where feasible

C. Allow the user to continue normal work while monitoring the system

D. Delete all security logs to prevent disclosure of sensitive information

E. Immediately reuse the system credentials on other workstations

ANSWER: A B

Explanation:

Isolating the affected workstation from the network and preserving relevant evidence are appropriate containment actions. Network isolation can stop command-and-control communications, reduce the opportunity for lateral movement, and limit data exfiltration. Evidence such as alerts, logs, memory data, active connections, and timestamps should be preserved so that the response team can determine the scope and cause of the compromise.

Containment is intended to limit harm while supporting subsequent eradication and recovery. Immediately rebuilding a system without collecting relevant evidence can destroy information needed to understand the incident, and continuing normal use of a suspected compromised system can increase risk. NIST describes containment, eradication, and recovery activities in SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

QUESTION NO: 22

Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

A. STARTTLS

B. FORCETLS

C. UPGRADETLS

ANSWER: A

Explanation:

STARTTLS is the SMTP extension command used to request an upgrade from an existing plaintext SMTP session to a TLS-protected session. During the SMTP exchange, a client first connects and receives the server's capabilities through the EHLO response. If the server advertises STARTTLS, the client sends the STARTTLS command. After the server confirms that it is ready, the TLS handshake occurs, establishing encryption and authentication protections for the connection. The client then issues EHLO again within the protected TLS session before continuing with mail submission or relay commands.

This mechanism is defined specifically for SMTP by RFC 3207, “SMTP Service Extension for Secure SMTP over Transport Layer Security.” It protects SMTP traffic while it is in transit over that particular client-to-server or server-to-server connection. In normal deployment, STARTTLS is often opportunistic: servers use TLS when both communicating parties support and negotiate it. Stronger delivery assurances can additionally be implemented through policies such as MTA-STS or DANE, but the SMTP command that initiates the TLS upgrade itself remains STARTTLS. See RFC 3207 and the IETF SMTP over TLS specification.

QUESTION NO: 23

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

A. 110

B. 135

C. 139

D. 161

E. 445

F. 1024

ANSWER: B C E

Explanation:

For legacy Windows NT, Windows 2000, and Windows XP environments, blocking ports 135, 139, and 445 at the network perimeter is an appropriate defense-in-depth measure to prevent exposure of the Windows networking services commonly associated with NetBIOS and file-sharing attacks. Port 139 carries NetBIOS Session Service traffic and was historically used for Windows file and printer sharing over NetBIOS. Port 445 carries Microsoft SMB directly over TCP/IP, without requiring the NetBIOS session layer; it is especially important to filter because newer Windows systems can use it for SMB-based file sharing, named pipes, and remote administration. Port 135 is used by the Microsoft RPC Endpoint Mapper, which helps clients locate RPC services and has long been relevant to exposure and enumeration of legacy Windows hosts. Filtering all three helps ensure that externally originating systems cannot reach the primary Windows service-discovery, RPC, and SMB pathways used by these operating systems. The filter should normally be applied inbound at the perimeter, while any required internal access should be controlled through segmentation and explicit allow rules. Microsoft’s port guidance identifies TCP 135 for RPC Endpoint Mapper, TCP 139 for NetBIOS Session Service, and TCP 445 for SMB: Microsoft service overview and network port requirements. Additional SMB security guidance is available from Microsoft SMB secure traffic documentation.

QUESTION NO: 24

A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it? Select the best answers.

A. Use port security on his switches.

B. Use a tool like ARPwatch to monitor for strange ARP activity.

C. Use a firewall between all LAN segments.

D. If you have a small network, use static ARP entries.

E. Use only static IP addresses on all PC's.

ANSWER: A B D

Explanation:

Using port security on switches helps limit which MAC addresses may connect to an access port. This reduces the opportunity for an unauthorized device to join the LAN and send forged ARP replies. In a production switched environment, this control is commonly combined with switch-based protections such as DHCP snooping and Dynamic ARP Inspection, which validate ARP bindings and are specifically designed to mitigate ARP spoofing. Cisco describes these related Layer 2 protections at Cisco Dynamic ARP Inspection documentation.

Using a tool like ARPwatch to monitor for strange ARP activity provides an important detection and response control. ARPwatch observes ARP traffic and records changes in IP-to-MAC mappings, enabling administrators to investigate unexpected mapping changes quickly and isolate a suspected attacker before poisoning has a wider impact. The project documentation is available at Lawrence Berkeley National Laboratory's ARPwatch page.

For a small, stable network, static ARP entries prevent hosts from dynamically accepting a malicious replacement MAC address for an important IP address, such as a default gateway or critical server. Because the mappings are manually fixed, forged ARP replies cannot simply overwrite those configured associations. This approach is operationally difficult at scale but is effective where addresses and hardware remain stable.

QUESTION NO: 25

When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is

A. OWASP is for web applications and OSSTMM does not include web applications.

B. OSSTMM is gray box testing and OWASP is black box testing.

C. OWASP addresses controls and OSSTMM does not.

D. OSSTMM addresses controls and OWASP does not.

ANSWER: D

Explanation:

OSSTMM addresses controls and OWASP does not is the intended distinction in this comparison. OSSTMM is a broad, operational security-testing methodology that evaluates security through defined test channels and explicitly considers the presence and effectiveness of security controls. Its approach is designed to produce measurable, repeatable results regarding how protections operate across a target's environment, including human, physical, wireless, telecommunications, data-network, and other relevant channels. In OSSTMM terminology, controls are a core part of assessing operational security and determining the exposure that remains after those controls are considered.

OWASP's Web Security Testing Guide is instead a focused guide for assessing the security of web applications and their supporting web technologies. It supplies a practical testing framework and test scenarios for web application risks, such as authentication, authorization, session management, input validation, and client-side behavior. Thus, the key methodological contrast expressed by this question is OSSTMM's formal, control-oriented operational model versus OWASP's web-application testing focus. See the OSSTMM 3 documentation and OWASP's Web Security Testing Guide.

QUESTION NO: 26

A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

A. Forensic attack

B. ARP spoofing attack

C. Social engineering attack

D. Scanning attack

E. Malware attack

ANSWER: E

Explanation:

Malware attack is correct because deploying antivirus controls at both the email gateway and endpoint creates defense in depth against malicious software. An email gateway can inspect inbound and outbound messages, attachments, and links before they reach users' mailboxes. This provides an early opportunity to detect or block known malicious files and suspicious content commonly used to deliver ransomware, trojans, worms, and other malware. Endpoint antivirus then provides another protective layer if a malicious file bypasses gateway inspection, arrives through another channel, or is introduced after delivery.

Using separate layers is important because malware delivery and execution occur at different points in the environment. Gateway scanning reduces exposure at the perimeter, while desktop antivirus can scan local files, monitor process behavior, and respond when malicious code attempts to execute. This layered arrangement reduces the likelihood that a single missed detection results in a compromised system. CISA describes malware as malicious software that can damage systems, steal information, or disrupt operations, and recommends protective controls including security software and email protections. See CISA's malware guidance and CISA's phishing guidance.

QUESTION NO: 27

Windows LAN Manager (LM) hashes are known to be weak.

Which of the following are known weaknesses of LM? (Choose three.)

A. Converts passwords to uppercase.

B. LM password hashes are stored without salting.

C. Makes use of only 32-bit encryption.

D. Effective length is 7 characters.

ANSWER: A B D

Explanation:

LM hashing has several design properties that make password recovery substantially easier than with modern password-verifier schemes. "Converts passwords to uppercase" is a significant weakness because it removes case sensitivity before the hash is calculated, shrinking the possible password search space. "LM password hashes are stored without salting" is also a weakness: identical passwords generate identical LM hash values, enabling attackers to use precomputed tables and efficiently identify password reuse. "Effective length is 7 characters" reflects LM's division of a password of up to 14 characters into two independent seven-character halves. Each half can be attacked separately, greatly reducing the effort required to recover a longer password; passwords of seven characters or fewer also leave a predictable second half. These legacy properties are why Microsoft recommends disabling LM hash storage and avoiding LM/NTLMv1 authentication where possible. Microsoft's documentation notes that LM hashes are weak and should not be stored, while NIST recommends using modern, resistant password-storage methods with salting and appropriate work factors. See Microsoft's guidance on preventing LM hash storage and NIST SP 800-63B.

QUESTION NO: 28

The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:

```
[ATTEMPT] target 192.168.1.106 - login "root" - pass "a" 1 of 20
[ATTEMPT] target 192.168.1.106 - login "root" - pass "123" 2 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "a" 3 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "123" 4 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "a" 5 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "123" 6 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "a" 7 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "123" 8 of 20
```

What is most likely taking place?

A. Ping sweep of the 192.168.1.106 network

B. Remote service brute force attempt

C. Port scan of 192.168.1.106

D. Denial of service attack on 192.168.1.106

ANSWER: B

Explanation:

Remote service brute force attempt is the correct interpretation of output that shows repeated authentication attempts against a network-accessible service on the target host. In an authorized penetration test, a brute-force or password-spraying tool commonly cycles through candidate usernames, passwords, or both while connecting to a particular service, such as SSH, FTP, Telnet, RDP, SMB, or a web-login endpoint. The tool's output generally identifies the target address, service or port, attempts being made, and possibly successful credentials when a valid combination is found. This activity is an authentication attack rather than simple host discovery or service enumeration because its purpose is to test whether weak, default, reused, or otherwise guessable credentials permit remote access. Credential testing should be explicitly authorized and carefully rate-limited, since repeated failed logins can trigger account lockouts, alerts, and operational impact. OWASP describes authentication testing, including testing for weak lockout controls and credential attacks, in its Web Security Testing Guide. NIST also identifies brute-force password guessing as a relevant threat addressed by strong authentication and password controls in SP 800-63B.

QUESTION NO: 29

Which of the following statements about digital signatures are correct? (Choose two.)

A. They can detect modification of signed data

B. They can support authentication of the signer

C. They automatically encrypt the signed message contents

D. They require recipients to possess the signer's private key

E. They eliminate the need to validate certificates or public-key bindings

ANSWER: A B

Explanation:

A digital signature can provide evidence of message integrity and can support authentication of the signer when the associated public key is reliably bound to that signer. The signer creates the signature using a private key, and recipients validate it with the corresponding public key. If signed content is changed after signing, signature verification fails.

Digital signatures do not normally provide confidentiality because the signed message may remain readable to anyone who receives it. Encryption is required when message contents must be kept secret. Public-key certificates are commonly used to associate a signer identity with a public key. NIST describes digital signatures in FIPS 186-5, Digital Signature Standard.

QUESTION NO: 30

What does the following command in netcat do?

nc -l -u -p55555 < /etc/passwd

A. logs the incoming connections to /etc/passwd file

B. loads the contents of /etc/passwd into a UDP listener on port 55555

C. grabs the /etc/passwd file when connected to UDP port 55555

D. deletes the /etc/passwd file when connected to the UDP port 55555

ANSWER: B

Explanation:

The command loads the contents of `/etc/passwd` into netcat's standard input and makes that input available through a UDP listener on port 55555. The shell redirection operator `<` is evaluated before netcat runs, so netcat receives the file's contents as if they had been typed into its input stream. The `-l` flag places netcat in listening mode, `-u` selects UDP rather than TCP, and `-p55555` specifies local port 55555 in traditional netcat implementations. Consequently, when a UDP peer communicates with the listener, netcat can transmit the redirected `/etc/passwd` content to that peer. This is a classic example of how command-line redirection can expose local file data over the network, particularly when a process is intentionally listening for remote interaction. The file is not modified by this command; it is used only as the input source for netcat. Netcat's listen mode and UDP support are documented in the nc.traditional manual page. The semantics of shell input redirection are described in the GNU Bash Redirections manual.

QUESTION NO: 31

Which of the following tools are used for enumeration? (Choose three.)

A. SolarWinds

B. USER2SID

C. Cheops

D. SID2USER

E. DumpSec

ANSWER: B D E

Explanation:

USER2SID, **SID2USER**, and **DumpSec** are classic Windows/SMB enumeration utilities. USER2SID is used to resolve a known account name to its Windows security identifier (SID), while SID2USER performs the reverse lookup, resolving a SID to an associated account. Such mappings help an authorized tester identify valid users, groups, and account naming information during the enumeration phase. Microsoft explains that SIDs are unique values used to identify security principals such as users and groups, making SID resolution directly relevant to Windows identity enumeration. DumpSec is designed to collect and report security-relevant information from Windows systems, including account, group, policy, share, and permission data. This makes it useful for systematically enumerating a target's accessible Windows security configuration and account information in an approved assessment. These utilities are commonly taught as legacy but foundational examples of Windows enumeration techniques; modern engagements may use supported administrative interfaces or current assessment tools to gather comparable information. See Microsoft's overview of security identifiers and Microsoft's guidance on security groups.

QUESTION NO: 32

Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

A. Restore a random file.

B. Perform a full restore.

C. Read the first 512 bytes of the tape.

D. Read the last 512 bytes of the tape.

ANSWER: B

Explanation:

Perform a full restore is correct because recovery verification must demonstrate that the complete backup set can be read, processed by the backup software, and restored into a usable state. A successful full restore exercises the entire recovery chain: the tape media, tape drive, backup catalog or metadata, backup application, data streams, and restoration process. It provides practical evidence that all protected data—not merely a small sample—is available and recoverable when needed. This is especially important for tape backups, where media degradation, drive compatibility issues, corrupted backup sets, and catalog problems might not be discovered by checking isolated portions of the tape. The restored content should also be validated for completeness and usability, ideally in a segregated test environment so that production systems are not overwritten. NIST guidance emphasizes testing recovery procedures and validating that backups can support restoration of systems and data. CISA likewise recommends regularly testing backups to confirm that restoration works as intended. See NIST SP 800-34 Rev. 1, Contingency Planning Guide and CISA StopRansomware Guide.

QUESTION NO: 33

Windows LAN Manager (LM) hashes are known to be weak.

Which of the following are known weaknesses of LM? (Choose three.)

A. Converts passwords to uppercase.

B. Hashes are sent in clear text over the network.

C. Makes use of only 32-bit encryption.

D. Effective length is 7 characters.

E. Does not use a salt, so identical passwords produce identical hashes.

ANSWER: A D E

Explanation:

LM password hashing is weak because it converts passwords to uppercase before processing them. This eliminates case sensitivity, substantially reducing the password search space and making offline guessing more practical. LM also processes a password as two independent 7-character portions: passwords are padded or truncated to 14 characters and then divided into two halves. Consequently, an attacker can crack each half separately rather than needing to search for the entire password as one value; this is the practical meaning of the effective length being 7 characters. In addition, LM hashes do not use a unique per-password salt. Identical passwords therefore produce identical LM hash values, enabling precomputation and reuse of cracking work across accounts and systems. These design properties are why modern Windows environments should avoid storing or accepting LM authentication material. Microsoft's NTLM protocol documentation describes the legacy LM one-way-function behavior and its password handling: MS-NLMP: NT LAN Manager Protocol. For broader password-storage guidance on the importance of salts and resistant password hashing, see the OWASP Password Storage Cheat Sheet.

QUESTION NO: 34

Which of the following protocols is commonly used to securely administer network devices and Linux or UNIX servers over an untrusted network?

A. Telnet

B. SSH

C. TFTP

D. SNMPv1

ANSWER: B

Explanation:

Secure Shell (SSH) is correct because it provides encrypted remote login, command execution, and file-transfer capabilities between a client and a server. SSH protects the confidentiality and integrity of the session and supports server authentication, helping administrators avoid exposing credentials and commands in clear text.

Telnet provides remote terminal access but does not provide comparable encryption for ordinary sessions. SSH normally uses TCP port 22, although administrators may configure an alternative port. The SSH transport protocol is specified in RFC 4253.

QUESTION NO: 35

What are two security benefits of using a unique salt for each stored password hash? (Choose two.)

A. It causes identical passwords to produce different stored hashes

B. It reduces the effectiveness of precomputed hash tables

C. It encrypts the password before transmission

D. It allows passwords to be stored in plain text safely

E. It eliminates the need for a password-hashing algorithm

ANSWER: A B

Explanation:

A unique salt ensures that two users who choose the same password will have different stored password hashes. This prevents an attacker from immediately identifying password reuse merely by comparing stored hash values.

Salts also make precomputed attacks, such as rainbow-table attacks, substantially less useful because an attacker would need to generate separate precomputed values for each salt. A salt does not make a weak password strong and does not replace the need for a slow, password-specific hashing algorithm with an appropriate work factor. NIST recommends storing passwords using salted, iterated password-hashing schemes in NIST SP 800-63B.

QUESTION NO: 36

Which of the following techniques will identify if computer files have been changed?

A. Network sniffing

B. Permission sets

C. Integrity checking hashes

D. Firewall alerts

ANSWER: C

Explanation:

Integrity checking hashes is correct because a cryptographic hash function produces a fixed-length digest that represents the contents of a file at a particular point in time. An assessor or security-monitoring system first records a trusted baseline hash for each file. It can later recalculate the hash and compare the result with that baseline. If even a very small change is made to the file's contents, such as modifying a character, adding data, or removing data, the newly calculated digest will differ, indicating that the file has changed. This process is a core function of file-integrity monitoring and is particularly valuable for detecting unauthorized modification of operating-system files, application binaries, configurations, logs, and other sensitive assets. For reliable monitoring, baseline hashes must be securely protected; otherwise, an attacker who can alter both a file and its stored reference hash could conceal the change. Modern cryptographic hashes such as SHA-256 are appropriate for integrity verification because they are designed to make undetected content changes computationally impractical. NIST describes cryptographic hash functions and their integrity role in FIPS 180-4, Secure Hash Standard. File-integrity monitoring is also recognized as a security-control practice in NIST SP 800-53 Rev. 5.

QUESTION NO: 37

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.

What is the most likely cause?

A. The network devices are not all synchronized.

B. Proper chain of custody was not observed while collecting the logs.

C. The attacker altered or erased events from the logs.

D. The security breach was a false positive.

ANSWER: A

Explanation:

The network devices are not all synchronized. is correct because meaningful cross-device log correlation depends on every logging system using a consistent, accurate time source. Firewalls, proxy servers, and IDS sensors independently timestamp events. If their system clocks drift or they use different time zones, timestamps for the same connection or attack sequence can appear in an incorrect order when logs are combined. This creates apparent inconsistencies even where each individual device recorded its own events accurately.

During incident response, synchronized timestamps allow an investigator to reconstruct an activity timeline: for example, associating a proxy request with the corresponding firewall connection and IDS alert. Network Time Protocol (NTP) is commonly used to synchronize infrastructure clocks to approved time servers. Time settings should include a common time source, appropriate time zone configuration, and monitoring for clock drift. The resulting consistent timestamps improve the reliability of event correlation, incident scoping, and forensic timeline analysis. NIST identifies synchronized clocks as important to log management and recommends using time synchronization protocols such as NTP; see NIST SP 800-92, Guide to Computer Security Log Management. Guidance for operating and securing NTP is also available from NIST Network Time Protocol Best Practices.

QUESTION NO: 38

Which of the following practices help preserve the usefulness and integrity of security logs? (Choose three.)

A. Synchronize systems with a reliable time source

B. Restrict write access to log files

C. Forward logs to a centralized logging system

D. Allow all users to clear local event logs

E. Disable logging to improve system performance

ANSWER: A B C

Explanation:

Synchronizing clocks with a reliable time source is important because event timestamps must be accurate for analysts to reconstruct an incident timeline across endpoints, servers, and network devices. NTP or another approved time-synchronization service is commonly used for this purpose.

Restricting write access to logs helps prevent an attacker or unauthorized user from deleting or altering evidence. Forwarding logs to a centralized logging system provides additional protection because records can be retained outside the affected host and correlated with other telemetry. These measures support detection, investigation, and accountability. NIST recommends centralized logging, time synchronization, and protection of log data in SP 800-92: Guide to Computer Security Log Management.

QUESTION NO: 39

A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

A. white box

B. grey box

C. red box

D. black box

ANSWER: D

Explanation:

black box is correct because the tester begins from the perspective of an unknown external party, using an external IP address and having no advance knowledge of the organization's internal systems, network design, applications, credentials, or defensive controls. This approach simulates a realistic outside attacker who must first perform reconnaissance and discovery to identify the exposed DMZ attack surface. The assessment would ordinarily include identifying public-facing hosts, enumerating available services, assessing application and infrastructure weaknesses, and determining whether an externally reachable weakness could permit further access.

The defining characteristic is the absence of pre-supplied environment knowledge. Consequently, the tester's findings demonstrate risk as it appears to an unauthenticated or minimally informed Internet-based adversary, including the effectiveness of perimeter segmentation and the security posture of systems intentionally exposed in the DMZ. This scenario aligns with penetration-testing guidance that begins with target discovery and information gathering when limited target information is provided. NIST describes penetration testing as an exercise that can include discovery, enumeration, vulnerability analysis, and exploitation activities; see NIST SP 800-115. The reconnaissance and information-gathering activities used for this external viewpoint are also covered in the OWASP Web Security Testing Guide.

QUESTION NO: 40

Which of the following are recommended controls for protecting privileged administrator accounts? (Choose three.)

A. Require multifactor authentication for privileged access

B. Use separate administrative and standard user accounts

C. Log and review privileged-account activity

D. Allow all administrators to share one common account

E. Store administrator passwords in an unencrypted shared spreadsheet

ANSWER: A B C

Explanation:

Requiring multifactor authentication, using separate accounts for administrative and routine work, and reviewing privileged-account activity are recommended controls. Multifactor authentication reduces the risk that a stolen password alone will permit privileged access. Separate administrative accounts reduce exposure because administrators do not need to use elevated privileges for email, web browsing, and other ordinary tasks. Logging and reviewing privileged actions supports accountability and can reveal misuse or compromise.

Shared administrator credentials reduce accountability and make it difficult to determine which person performed an action. Privileged passwords should not be stored in unprotected documents or distributed through informal channels. NIST guidance for privileged accounts and least privilege is available in NIST SP 800-53 AC-6, Least Privilege.

QUESTION NO: 41

Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?

A. Sarbanes-Oxley Act (SOX)

B. Gramm-Leach-Bliley Act (GLBA)

C. Fair and Accurate Credit Transactions Act (FACTA)

D. Federal Information Security Management Act (FISMA)

ANSWER: A

Explanation:

The Sarbanes-Oxley Act (SOX) is correct. Enacted in 2002, SOX strengthened corporate-accountability and financial-reporting requirements for U.S. public companies following major accounting scandals. In particular, Section 302 requires an issuer's principal executive officer and principal financial officer—normally the CEO and CFO—to personally certify each quarterly and annual report. Their certification addresses the accuracy of the report, the absence of untrue material statements or material omissions, and their responsibility for establishing and maintaining disclosure controls and procedures. Section 906 also requires a written certification accompanying periodic reports that the report fully complies with applicable Securities Exchange Act requirements and that the information fairly presents, in all material respects, the issuer's financial condition and results of operations. These personal certifications make senior leadership directly accountable for the completeness and reliability of financial disclosures. The statutory text is available through Public Law 107-204 (Sarbanes-Oxley Act), and the U.S. Securities and Exchange Commission summarizes the related officer-certification requirements in its certification and disclosure rules.

QUESTION NO: 42

Under what conditions does a secondary name server request a zone transfer from a primary name server?

A. When a primary SOA is higher than a secondary SOA

B. When a secondary SOA is higher than a primary SOA

C. When a primary name server has had its service restarted

D. When a secondary name server has had its service restarted

E. When the TTL falls to zero

ANSWER: A

Explanation:

When a primary SOA is higher than a secondary SOA is correct because DNS secondary-server synchronization is governed by the serial number in the zone's Start of Authority (SOA) record. At the interval specified by the SOA refresh field, a secondary server queries the primary (also called the master) server for the zone's SOA record and compares the advertised serial number with the serial number of its locally stored zone copy. If the primary's serial number is greater, the secondary recognizes that the primary holds a newer version of the zone and requests a zone transfer. Depending on server support and the change history retained by the primary, this can be an incremental zone transfer (IXFR) or a full zone transfer (AXFR). Administrators must therefore increment the SOA serial whenever they publish DNS zone changes; otherwise, secondary servers have no serial-based indication that their copies need updating. The DNS zone-maintenance model, including SOA serial comparison and refresh processing, is specified in RFC 1034, section 4.3.5. The SOA record fields and zone-transfer notification behavior are further described in RFC 1996.

QUESTION NO: 43

What is the main difference between a "Normal" SQL Injection and a "Blind" SQL Injection vulnerability?

A. The request to the web server is not visible to the administrator of the vulnerable application.

B. The attack is called "Blind" because, although the application properly filters user input, it is still vulnerable to code injection.

C. The successful attack does not show an error message to the administrator of the affected application.

D. The vulnerable application does not display errors with information about the injection results to the attacker.

ANSWER: D

Explanation:

The vulnerable application does not display errors with information about the injection results to the attacker. This is the defining characteristic of blind SQL injection: the application may still execute attacker-controlled SQL, but it does not directly return useful database error messages, query output, or other verbose feedback in the HTTP response. The tester must therefore infer whether an injected condition was true or false from indirect observable behavior, such as a changed page response, a different status code, a response-time delay, or an out-of-band interaction. For example, a conditionally true predicate can cause normal content to be returned, while a false predicate may change the page or suppress results; time-based techniques deliberately introduce a measurable delay when a condition is true. This distinction concerns the visibility of results to the attacker, rather than whether a server administrator can see requests or whether input filtering is present. OWASP describes blind SQL injection as a situation where application responses do not reveal query results or errors, requiring inference-based methods. See the OWASP Blind SQL Injection guidance and the OWASP SQL Injection Prevention Cheat Sheet for technical context and defensive practices.

QUESTION NO: 44

Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

A. Metasploit scripting engine

B. Nessus scripting engine

C. NMAP scripting engine

D. SAINT scripting engine

ANSWER: C

Explanation:

NMAP scripting engine is correct because Nmap's vulnerability-assessment capability is extended through the Nmap Scripting Engine (NSE). NSE executes Lua scripts against discovered services and exposes checks that go beyond ordinary port and version scanning. Its script library includes service-specific capabilities for common vectors such as SMB, HTTP,

and FTP, enabling tasks such as enumerating configurations, identifying known vulnerable service behavior, checking authentication exposure, and gathering protocol-level information relevant to vulnerability analysis.

In a practical ethical-hacking workflow, Nmap first identifies reachable hosts, open ports, and detected service versions; NSE scripts can then be selected by name or category to perform targeted follow-up checks. The `vuln` script category is specifically intended for scripts that test for known vulnerabilities, while other categories and protocol-focused scripts support deeper discovery and validation. This makes NSE the resource that turns Nmap from a network and service scanner into a basic, extensible vulnerability-scanning tool. Nmap documentation describes NSE and its usage at Nmap Scripting Engine documentation, and provides the available script categories, including vulnerability scripts, at NSE usage and script categories.

QUESTION NO: 45

In Trojan terminology, what is a covert channel?

A. A channel that transfers information within a computer system or network in a way that violates the security policy

B. A legitimate communication path within a computer system or network for transfer of data

C. It is a kernel operation that hides boot processes and services to mask detection

D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections

ANSWER: A

Explanation:

A channel that transfers information within a computer system or network in a way that violates the security policy is the correct definition of a covert channel. A covert channel uses a mechanism not intended or authorized for communication to convey information across a security boundary. In the context of Trojan activity, malware may use such a channel to pass commands, leak collected data, or signal another process while bypassing the system's normal access-control and information-flow rules. The defining issue is not merely that data is transmitted secretly; it is that the communication path enables information flow that the applicable security policy does not permit.

Covert channels may exploit shared system resources or observable characteristics, such as file-lock state, process timing, resource utilization, or other conditions that can be manipulated by one security domain and observed by another. Security evaluation guidance distinguishes covert channels from normal communication interfaces precisely because their use can circumvent mandatory controls. The National Institute of Standards and Technology describes covert channels as communication paths not intended for information transfer and notes their relevance to enforcing information-flow policy. This concept is also reflected in the NIST Computer Security Resource Center definition of a covert channel and NIST's SP 800-53 security-control guidance concerning information-flow enforcement.

QUESTION NO: 46

The network administrator at Spears Technology, Inc has configured the default gateway

Cisco router's access-list as below:

You are hired to conduct security testing on their network.

You successfully brute-force the SNMP community string using a SNMP crack tool.

The access-list configured at the router prevents you from establishing a successful connection.

You want to retrieve the Cisco configuration from the router. How would you proceed?

A. Use the Cisco's TFTP default password to connect and download the configuration file

B. Run a network sniffer and capture the returned traffic with the configuration file from the router

C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address

D. Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0

ANSWER: B D

Explanation:

In an authorized assessment, the workable technique is to use an SNMP SET operation with a source address that matches the address range permitted by the router's SNMP access list. Cisco devices can expose configuration-copy functionality through the CISCO-CONFIG-COPY-MIB. A properly constructed SET request can instruct the device to copy its running or startup configuration to a specified TFTP server. Because the access list evaluates the apparent packet source, spoofing an allowed source address can cause the device to accept the request when source-address validation is absent or ineffective.

The corresponding return path is essential: replies and the TFTP configuration transfer are sent to the spoofed, permitted address rather than directly to the testing host. Therefore, capturing traffic on the network segment associated with that spoofed address allows the assessor to obtain the configuration data carried in the resulting transfer. This pairing of a spoofed-source SNMP SET request and packet capture is why both actions are required. SNMP SET request semantics are defined in RFC 3416, and Cisco documents configuration copying through SNMP in its SNMP Configuration Guide.

QUESTION NO: 47

Which of the following tools can be used to perform a zone transfer?

A. NSLookup

B. Finger

C. Dig

D. Sam Spade

E. Host

F. Netcat

G. Neotrace

ANSWER: A C D E

Explanation:

A DNS zone transfer retrieves the records in a DNS zone from an authoritative name server when that server permits the request. The standard full-zone transfer mechanism is AXFR, normally carried over TCP port 53. *NSLookup* can request a zone listing through its interactive `ls` functionality, where supported by the installed version and the target server. *Dig* directly supports AXFR queries, for example with an `AXFR` query type directed at an authoritative server. *Host* can perform a zone transfer using its zone-listing capability, such as `host -l`. *Sam Spade*, a legacy network-reconnaissance utility, also includes DNS interrogation functionality that can request zone transfers. In every case, a successful transfer depends on the DNS server's transfer-access policy; properly configured servers restrict transfers to authorized secondary name servers. AXFR is defined in the DNS protocol specification, and the commonly used command-line tools document the relevant zone-transfer query features. See RFC 5936: DNS Zone Transfer Protocol and the dig manual page.

QUESTION NO: 48

Which of the following are well known password-cracking programs?

A. L0phtcrack

B. NetCat

C. Jack the Ripper

D. Netbus

E. John the Ripper

ANSWER: A E

Explanation:

L0phtcrack and **John the Ripper** are well-known password-cracking and password-auditing programs. L0phtcrack is designed primarily for auditing Windows password security. It obtains password-hash data where authorized, performs dictionary, hybrid, and brute-force-style recovery attempts, and reports password-strength findings so administrators can remediate weak credentials. Its long-standing use in Windows security assessments makes it a commonly recognized password-cracking tool. The vendor describes its product as a password-auditing and recovery application at L0phtCrack.

John the Ripper is an established open-source password-security auditing tool with broad platform and hash-format support. It can test password hashes against wordlists, mangling rules, incremental modes, and other cracking techniques; this makes it useful to ethical hackers and defenders conducting authorized credential-strength assessments. The project documentation describes its password-cracking capabilities, supported formats, and operating modes at Openwall: John the Ripper password cracker. In an ethical-hacking context, both tools must be used only with explicit authorization and within the defined scope of an engagement.

QUESTION NO: 49

While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model. Which type of firewall is the tester trying to traverse?

A. Packet filtering firewall

B. Application-level firewall

C. Circuit-level gateway firewall

D. Stateful multilayer inspection firewall

ANSWER: C

Explanation:

Circuit-level gateway firewall is correct because this firewall category operates at the OSI session layer and evaluates whether a connection is legitimately established, principally by monitoring the TCP handshake and session setup. Rather than examining the detailed contents of individual packets or understanding application commands, it validates connection state and relays permitted sessions between endpoints. This approach can conceal internal network addressing while allowing the gateway to enforce rules governing which sessions may be created.

For a penetration tester, identifying this behavior matters because connectivity depends on successfully establishing an approved session through the gateway. The observed focus on TCP handshaking is the key technical indicator: the three-way handshake establishes the connection state that a circuit-level gateway uses to determine whether traffic belongs to a valid circuit. NIST describes firewalls as controls that mediate network traffic based on policy, while firewall architectures may apply controls at different layers. Cisco's networking reference also identifies circuit-level gateways as session-layer devices that monitor TCP handshakes. See NIST SP 800-41 Rev. 1 and Cisco: What Is a Firewall?.

QUESTION NO: 50

When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

A. Network tap

B. Layer 3 switch

C. Network bridge

D. Application firewall

ANSWER: A

Explanation:

Network tap is correct because it is a purpose-built hardware device that passively copies traffic traversing a physical network link to one or more monitoring ports. A capture system running Wireshark can connect to the tap's monitor output and receive the packets in both directions without becoming an active endpoint in the communication path. This makes a tap particularly appropriate when the objective is comprehensive packet acquisition from the wire, including traffic that would ordinarily remain confined to the link between the two connected devices.

In addition to visibility, passive operation is important in an investigation or monitoring context: a properly deployed tap does not require the capture host to transmit traffic onto the production link, and it avoids changing normal switching behavior. Wireshark's capture documentation notes that packet capture depends on the interface and network setup providing the packets to the capture system; a tap supplies that visibility directly. Cisco likewise describes network taps as passive devices used to provide a copy of network traffic to monitoring and analysis tools. See the Wireshark User's Guide: Capturing Live Network Data and Cisco's network TAP overview.

QUESTION NO: 51

Which of the following controls are effective primary defenses against SQL injection attacks? (Choose two.)

A. Parameterized queries

B. Allow-list input validation

C. Client-side JavaScript validation only

D. Displaying detailed database errors to users

E. Using a shared database administrator account

ANSWER: A B

Explanation:

Parameterized queries are a primary defense against SQL injection because they separate SQL code from untrusted input. The database driver sends the query structure and parameter values separately, preventing supplied data from being interpreted as part of the SQL command.

Allow-list input validation is also an important defense because it restricts input to the expected format, type, length, and permitted values. For example, an application expecting an integer identifier should reject input that contains SQL metacharacters or other unexpected characters. Escaping alone can be error-prone, and client-side validation can be bypassed; therefore, controls must be enforced server-side. OWASP recommends parameterized queries and allow-list validation in its SQL Injection Prevention Cheat Sheet.

QUESTION NO: 52

Which of the following LM hashes represent a password of less than 8 characters?

(Choose two.)

A. BA810DBA98995F1817306D272A9441BB

B. 44EFCE164AB921CQAAD3B435B51404EE

C. 0182BD0BD4444BF836077A718CCDF409

D. CEC52EB9C8E3455DC2265B23734E0DAC

E. B757BF5C0D87772FAAD3B435B51404EE

F. E52CAC67419A9A224A3B108F3FA6CB6D

ANSWER: B E

Explanation:

LM hashing processes a password by converting it to uppercase, padding it with null bytes to 14 bytes, and splitting that value into two independent seven-byte blocks. Each block is used to produce a 16-hex-character DES-derived component, so an LM hash normally consists of two 16-character halves. When the original password is fewer than eight characters, the second seven-byte block contains only padding. Its resulting LM component is the well-known constant `AAD3B435B51404EE`. Therefore, an LM value whose second half is that constant indicates that no password characters occupied the second block and that the password length was at most seven characters. Both `44EFCE164AB921CQAAD3B435B51404EE` and `B757BF5C0D87772FAAD3B435B51404EE` contain this identifying second-half value. The former appears to contain a non-hexadecimal transcription character in its first half, but its displayed `AAD3B435B51404EE` suffix is the relevant indicator intended by the question. LM hashes are obsolete and insecure; modern systems should use stronger password-verifier mechanisms. See Hashcat's LM hash example reference and NIST's Digital Identity Guidelines.

QUESTION NO: 53

What is the purpose of DNS AAAA record?

A. Authorization, Authentication and Auditing record

B. Address prefix record

C. Address database record

D. IPv6 address resolution record

ANSWER: D

Explanation:

The purpose of an **IPv6 address resolution record** is to associate a DNS host name with its 128-bit IPv6 address. When a client needs to connect to a service over IPv6, it queries DNS for an AAAA resource record, and DNS returns the IPv6 address configured for that name. For example, an AAAA record can map `www.example.com` to an address such as `2001:db8::10`. This is the IPv6 counterpart to an A record, which maps a name to a 32-bit IPv4 address. AAAA records are essential for dual-stack deployments, where a host may publish both A and AAAA records so that clients can select IPv4 or IPv6 connectivity as appropriate. The record type is standardized by the IETF in RFC 3596, which defines the AAAA format and specifies that it stores an IPv6 address for a domain name. DNS terminology describes this process as name-to-address mapping rather than protocol-level address resolution such as ARP or Neighbor Discovery. See RFC 3596: DNS Extensions to Support IP Version 6 and the IANA DNS Parameters registry.

QUESTION NO: 54

The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.

An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is:

nmap 192.168.1.64/28.

Why he cannot see the servers?

A. The network must be down and the nmap command and IP address are ok.

B. He needs to add the command ' ' ' ' ip address ' ' ' ' just before the IP address.

C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range.

D. He needs to change the address to 192.168.1.0 with the same mask.

ANSWER: C

Explanation:

He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range. A `/28` prefix corresponds to the mask `255.255.255.240`, which creates blocks of 16 addresses. Therefore, the target `192.168.1.64/28` identifies the address block from `192.168.1.64` through `192.168.1.79`. Within that block, `192.168.1.64` is the network address and `192.168.1.79` is the broadcast address; the ordinary usable host range is `192.168.1.65` through `192.168.1.78`. None of the listed servers—`192.168.1.122`, `192.168.1.123`, and `192.168.1.124`—falls inside this scan target, so Nmap has no reason to probe them. The company's stated `255.255.255.192` mask is `/26`, under which the `192.168.1.64` subnet spans `192.168.1.64` to `192.168.1.127`; thus the servers are part of the actual subnet but are omitted because the attacker supplied the narrower prefix. See Nmap target specification documentation and RFC 4632 for CIDR addressing details.

QUESTION NO: 55

Which of the following is an example of two factor authentication?

A. PIN Number and Birth Date

B. Username and Password

C. Digital Certificate and Hardware Token

D. Fingerprint and Smartcard ID

ANSWER: D

Explanation:

Fingerprint and Smartcard ID is an example of two-factor authentication because it combines credentials from two independent authentication-factor categories. A fingerprint is an inherence factor: it verifies something the user is, based on a physical or behavioral characteristic. A smartcard ID is a possession factor: it verifies something the user has, namely the issued physical card or token. Authentication is considered multifactor only when it requires evidence from distinct factor types, rather than multiple pieces of information from the same type. This combination therefore provides stronger assurance that the person requesting access is both the authorized card holder and the individual associated with the enrolled biometric template. In an ethical-hacking or security assessment context, recognizing the factor categories is important when reviewing login controls, determining whether a system truly implements MFA, and evaluating the impact of credential theft. NIST identifies something you know, something you have, and something you are as authenticator-factor categories and discusses the use of multiple factors in digital identity systems. See NIST SP 800-63B: Digital Identity Guidelines—Authentication and Lifecycle Management and NIST's definition of multifactor authentication.

QUESTION NO: 56

Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer is accomplished with the DNS

B. A zone transfer is accomplished with the nslookup service

C. A zone transfer passes all zone information that a DNS server maintains

D. A zone transfer passes all zone information that a nslookup server maintains

E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections

F. Zone transfers cannot occur on the Internet

ANSWER: A C E

Explanation:

“A zone transfer is accomplished with the DNS” is correct in the intended sense because zone transfers are a DNS protocol function performed between authoritative DNS servers. A primary server supplies zone data to an authorized secondary server so that the secondary can maintain a synchronized copy of the zone. The DNS zone-transfer specification defines both full transfers and incremental transfers, including the request and response behavior used by DNS servers. See RFC 5936: DNS Zone Transfer Protocol.

“A zone transfer passes all zone information that a DNS server maintains” correctly describes a full zone transfer. A full transfer provides the receiving secondary server with the resource records comprising the zone, enabling it to serve authoritative responses for that replicated zone. This replication model is part of the DNS architecture described in RFC 1034.

“A zone transfer can be prevented by blocking all inbound TCP port 53 connections” is also correct for network-based transfers because DNS zone transfers use TCP port 53. Denying inbound TCP connections to that service prevents remote secondary servers or unauthorized remote clients from establishing the TCP session required to request and receive a transfer. In practice, administrators commonly permit TCP port 53 only from explicitly authorized secondary DNS servers while retaining appropriate DNS service for legitimate clients.

QUESTION NO: 57

Name two software tools used for OS guessing? (Choose two.)

A. Nmap

B. Snadboy

C. Queso

D. UserInfo

E. NetBus

ANSWER: A C

Explanation:

Nmap and Queso are both tools used for operating-system guessing, more commonly called operating-system fingerprinting. Nmap performs active OS detection by sending a set of specially crafted TCP, UDP, and ICMP probes to a target and comparing the target’s responses with its fingerprint database. These network-stack characteristics can reveal likely operating-system families, versions, and device types. Nmap’s OS-detection capability is invoked with the `-O` option, and it is a standard feature used during authorized reconnaissance and security assessments.

Queso is also an active TCP/IP stack fingerprinting utility. It probes a host with selected packet patterns and evaluates response behavior, such as TCP flag handling, window sizes, and other implementation-specific details, to infer the target operating system. Queso is historically significant in ethical-hacking and network-security training because it demonstrates how differences in protocol-stack implementation can disclose platform information before direct access is obtained. In practice, fingerprinting results should be treated as informed estimates and validated with additional authorized enumeration evidence. Nmap documents its OS-detection method at Nmap Network OS Detection; Queso is documented in the Kali Linux tools repository at Kali Linux: Queso.

QUESTION NO: 58

What does a type 3 code 13 represent? (Choose two.)

A. Echo request

B. Destination unreachable

C. Network unreachable

D. Administratively prohibited

E. Port unreachable

F. Time exceeded

ANSWER: B D

Explanation:

In IPv4 ICMP, the type field identifies the broad message category, while the code field supplies the specific condition within that category. Type 3 is the ICMP *Destination Unreachable* message class. Therefore, “Destination unreachable” correctly identifies the overall meaning of a type 3 message. Code 13 further specifies the reason for that unreachable condition: *Communication Administratively Prohibited*, commonly expressed as “Administratively prohibited.” This response is generated when a router, firewall, or other policy-enforcing device denies traffic because of an administrative filtering rule rather than because a route or target service is unavailable.

The Internet Assigned Numbers Authority’s ICMP parameter registry lists type 3 as Destination Unreachable and assigns code 13 to Communication Administratively Prohibited. RFC 1812 also specifies that routers may use ICMP Destination Unreachable code 13 when forwarding is prohibited by administrative filtering. These two descriptions are complementary: one names the ICMP message type and the other names the particular code-defined cause. See the IANA ICMP Parameters registry and RFC 1812, section 5.2.7.1.

QUESTION NO: 59

Which security properties can DNS Security Extensions (DNSSEC) provide for DNS data? (Choose two.)

A. Data-origin authentication

B. Data integrity

C. Confidentiality of DNS queries

D. Encryption of all DNS zone files

E. Anonymity for DNS clients

ANSWER: A B

Explanation:

DNSSEC provides data-origin authentication by allowing a validating resolver to verify that DNS records were signed by the authoritative zone or an authorized signer in the chain of trust. This helps a resolver determine whether a response originated from the legitimate DNS authority.

DNSSEC also provides data integrity by enabling detection of modification to signed DNS data. If an attacker changes a signed record in transit, signature validation fails. DNSSEC does not encrypt DNS queries or responses and therefore does not provide confidentiality. Encrypted DNS transports, such as DNS over TLS or DNS over HTTPS, address confidentiality separately. DNSSEC is specified in RFC 4033, and CISA provides deployment guidance in its DNSSEC guide.

QUESTION NO: 60

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network.

Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

A. SNMPUtil

B. SNScan

C. SNMPScan

D. Solarwinds IP Network Browser

E. NMap

ANSWER: A B D

Explanation:

SNMPUtil, SNScan, and Solarwinds IP Network Browser are appropriate tools for performing SNMP-focused discovery and enumeration. SNMPUtil is a command-line utility for communicating with SNMP agents and issuing requests such as reads of management information. This enables an administrator or authorized assessor to query exposed SNMP services and retrieve relevant managed-object data. Microsoft documents SNMP utilities and the SNMP management model at Microsoft Learn: SNMP.

SNScan is designed specifically to locate and query SNMP-enabled hosts, making it suitable for identifying responding devices and gathering information exposed through SNMP. Solarwinds IP Network Browser likewise supports network discovery and browsing of device information, including information obtained from SNMP-capable network equipment. These capabilities are directly relevant to SNMP enumeration because they help identify reachable SNMP agents and inspect the management data those agents make available under authorized conditions. SolarWinds describes SNMP as a standard mechanism used to monitor and manage network devices in its SNMP overview.

QUESTION NO: 61

Which of the following is an extremely common IDS evasion technique in the web world?

A. unicode characters

B. spyware

C. port knocking

D. subnetting

ANSWER: A

Explanation:

Unicode characters is correct because web applications, servers, proxies, and intrusion-detection systems must decode text and URLs before interpreting a request. An attacker can use Unicode/UTF-8 encoding variations to make a malicious path, parameter, or payload appear different to an IDS than it does to the target application. This is particularly significant when components normalize or decode input differently, creating a discrepancy between the security device's inspection and the application's eventual interpretation. Historically, overlong UTF-8 sequences and alternate encodings have been used to obscure characters such as path separators or traversal sequences. Properly implemented systems should reject invalid UTF-8, apply canonical normalization, and ensure that filtering and application processing use consistent decoding rules. RFC 3629 specifies UTF-8 validity requirements, including restrictions that prevent overlong encodings, while OWASP emphasizes canonicalization and validating input after decoding as important defenses against encoding-based attacks. These encoding and normalization inconsistencies make Unicode-based evasions a well-known web-focused IDS evasion technique. See RFC 3629: UTF-8, a transformation format of ISO 10646 and the OWASP Canonicalize Data guidance.

QUESTION NO: 62

Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

A. It is a network fault and the originating machine is in a network loop

B. It is a worm that is malfunctioning or hardcoded to scan on port 500

C. The attacker is trying to detect machines on the network which have SSL enabled

D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

ANSWER: D

Explanation:

The attacker is trying to determine the type of VPN implementation and checking for IPSec

is correct because port 500 is the well-known UDP port assigned to the Internet Key Exchange (IKE) protocol. IKE is the key-management and security-association negotiation protocol commonly used with IPsec VPNs. By sending probes to UDP port 500 across multiple hosts, an attacker can identify systems that appear to expose IKE services and may therefore be configured as IPsec VPN gateways or endpoints. Responses, timing behavior, and IKE negotiation details can assist with later fingerprinting of the VPN implementation and its configuration. The observation that the traffic is sourced from port 500 and directed to port 500 is consistent with IKE communication and scanning activity aimed at that service; it is not merely a generic TCP/UDP port sweep. The IANA service-name registry lists UDP port 500 for ISAKMP, the protocol family and port convention used by IKE, while the IKEv2 standard specifies that IKE uses UDP port 500 by default. See the IANA Service Name and Port Number Registry and RFC 7296: Internet Key Exchange Protocol Version 2.

QUESTION NO: 63

For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender's public key

B. Receiver's private key

C. Receiver's public key

D. Sender's private key

ANSWER: D

Explanation:

A digital signature is generated using the sender's private key. The sender first computes a cryptographic hash, also called a message digest, from the message. That digest is then signed using the sender’s private key—more precisely, modern signature schemes apply a private-key signing operation to a suitably encoded hash rather than simply “encrypting” it in the general confidentiality sense. The recipient obtains the sender’s public key, often through a validated digital certificate, and uses it to verify the signature against a newly calculated digest of the received message. A successful verification provides evidence that the signature was created by the holder of the corresponding private key and that the signed message has not been altered since signing. This provides authentication, integrity, and nonrepudiation support; it does not by itself keep the message confidential. NIST describes digital signatures as mechanisms generated with a private key and verified with the associated public key. See NIST FIPS 186-5, Digital Signature Standard and RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

QUESTION NO: 64

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

A. Reverse Social Engineering

B. Tailgating

C. Piggybacking

D. Announced

ANSWER: B

Explanation:

Tailgating is correct because the unauthorized person obtains physical access by closely following an authorized employee through a controlled entrance. The scenario describes access occurring after a lunch rush, when employees may be less likely to notice someone entering behind them and when a door may be opened frequently. This is a physical-security and social-engineering concern: the attacker exploits ordinary employee behavior rather than defeating the lock, badge reader, or other entry-control technology.

In security usage, tailgating commonly describes an unapproved person entering a secured area immediately behind an authorized person without being explicitly permitted or checked. Preventive controls include training personnel to challenge or report unknown entrants, requiring each person to badge individually, using turnstiles or mantraps, and monitoring entry points. NIST's glossary identifies tailgating as gaining unauthorized access by following an authorized person through a secure entry, which directly matches the described event. See the NIST Computer Security Resource Center definition of tailgating and CISA guidance on physical security.

QUESTION NO: 65

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

A. USER, NICK

B. LOGIN, NICK

C. USER, PASS

D. LOGIN, USER

ANSWER: A

Explanation:

USER, NICK represents the core identity-registration commands an IRC client uses when connecting to an IRC server. The `NICK` command supplies the nickname that will identify the client on the network, while `USER` provides the required user information used by the server to complete registration. After the server has accepted these registration details, it sends the appropriate welcome numerics and the client is considered connected to the IRC network; it can then issue commands such as `JOIN` to enter a channel.

In practical IRC protocol exchanges, the precise ordering of the nickname and user-information commands can vary by client or server implementation, and a `PASS` command may precede them when the server requires a password. However, the fundamental pair for ordinary IRC client registration is the nickname command together with the user-information command. This distinction is useful in ethical-hacking work involving IRC traffic analysis or botnet command-and-control investigations: recognizing registration commands helps identify a new IRC client session before channel activity begins. RFC 2812 documents the IRC client protocol and its registration process, including the `NICK` and `USER` commands: RFC 2812, Client Registration. The IRCv3 specification also describes the modern client registration sequence: IRCv3 Capability Negotiation.

QUESTION NO: 66

Which of the following guidelines or standards is associated with the credit card industry?

A. Control Objectives for Information and Related Technology (COBIT)

B. Sarbanes-Oxley Act (SOX)

C. Health Insurance Portability and Accountability Act (HIPAA)

D. Payment Card Industry Data Security Standards (PCI DSS)

ANSWER: D

Explanation:

Payment Card Industry Data Security Standards (PCI DSS) is the security standard specifically associated with the payment-card industry. It establishes a baseline of technical and operational safeguards for entities that store, process, or transmit cardholder data, as well as organizations that can affect the security of the cardholder-data environment. The standard is administered by the PCI Security Standards Council and is intended to promote consistent protection of payment account data throughout the payment ecosystem.

PCI DSS requirements address core security practices such as maintaining secure networks and systems, protecting stored account data, encrypting cardholder data sent across open or public networks, managing vulnerabilities, enforcing strong access controls, monitoring and testing security controls, and maintaining an information-security policy. For an ethical hacker or security professional, PCI DSS is especially relevant because penetration testing, vulnerability management, segmentation validation, and evidence of security-control operation may be necessary parts of an organization's compliance program. The PCI Security Standards Council provides the authoritative standard and supporting materials at PCI DSS. Its overview of the standard's purpose and applicability is also available at PCI SSC merchant resources.

QUESTION NO: 67

Which method of password cracking takes the most time and effort?

A. Brute force

B. Rainbow tables

C. Dictionary attack

D. Shoulder surfing

ANSWER: A

Explanation:

Brute force is correct because it is an exhaustive guessing method: it systematically tests password candidates until it finds one that produces the required authentication result or matches a captured password hash. In the general case, it may need to examine every possible combination in the defined character set and password length range. The number of candidates grows exponentially as length and character variety increase. For example, adding one position to a password multiplies the search space by the number of permitted characters, so even a modest increase in length can substantially increase the computing time required.

The actual duration depends on whether guessing is performed online or offline, the permitted candidate space, the hardware available, and the password-hashing algorithm. Offline attacks against hashes can be particularly costly when a password storage system uses a modern, deliberately slow, salted password-hashing function. NIST requires password verifiers to use salted hashing and recommends an additional cost factor to make each guess more expensive, which directly increases the work involved in exhaustive cracking. See NIST SP 800-63B and the OWASP guidance on blocking brute-force attacks.

QUESTION NO: 68

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

A. Use the same machines for DNS and other applications

B. Harden DNS servers

C. Use split-horizon operation for DNS servers

D. Restrict Zone transfers

E. Have subnet diversity between DNS servers

ANSWER: B C D E

Explanation:

DNS is foundational infrastructure, so its security should combine server hardening, controlled disclosure of DNS data, and resilient service design. “Harden DNS servers” is correct because authoritative and recursive DNS hosts should be dedicated, patched, minimally exposed, monitored, and configured so that recursion, administrative access, and unnecessary services are limited. “Use split-horizon operation for DNS servers” is also appropriate where an organization needs different internal and external DNS answers; it helps avoid unnecessarily publishing internal names, addressing details, or services to the public Internet. “Restrict Zone transfers” is essential because zone data can reveal a detailed inventory of hosts and services. Transfers should be permitted only to authorized secondary servers, typically enforced with source restrictions and authenticated mechanisms such as TSIG. “Have subnet diversity between DNS servers” improves availability and resistance to network failures or attacks: authoritative servers placed on separate networks are less likely to become unreachable through one routing, subnet, or provider incident. These measures align with CISA guidance to secure DNS infrastructure and with DNS operational guidance covering authenticated zone transfers and resilient authoritative service deployment. See CISA: Securing DNS and RFC 2845: Secret Key Transaction Authentication for DNS (TSIG).

QUESTION NO: 69

You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place.

Your peer, Peter Smith who works at the same department disagrees with you.

He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.

What is Peter Smith talking about?

A. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain

B. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks

C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks

D. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to bypass the filters in your gateway

ANSWER: A

Explanation:

Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain is correct because security controls depend on people to use, maintain, and respond to them appropriately. Even a well-designed environment with hardened devices, filtering, malware protection, and detection capabilities can be undermined when an

employee is deceived by social engineering, discloses credentials, approves a fraudulent request, mishandles sensitive information, or fails to report suspicious activity promptly. Attackers frequently target people because human trust, urgency, and routine business processes can provide a path around otherwise robust technical safeguards.

Effective security therefore requires a defense-in-depth program that includes recurring awareness education, role-specific training, phishing-reporting procedures, clear access-control practices, and exercises that help personnel recognize and escalate suspicious events. This does not place blame on users; rather, it recognizes that organizational processes and usable security design must support people in making safe decisions. NIST identifies awareness and training as essential elements of an information-security program and describes the need to ensure users understand their security responsibilities. CISA likewise emphasizes that social-engineering resistance and a security-aware workforce are important protections against compromise. See NIST SP 800-50 and CISA Phishing Guidance.

QUESTION NO: 70

Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.

Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.

In this context, what can you say?

A. Bob can be right since DMZ does not make sense when combined with stateless firewalls

B. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one

C. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations

D. Bob is partially right. DMZ does not make sense when a stateless firewall is available

ANSWER: C

Explanation:

Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations is the correct answer because a demilitarized zone is a network-segmentation design that places public-facing systems in a separate, controlled network from the internal workstation network. Its security value is not dependent on whether the firewall performs stateful inspection. A stateless packet-filtering firewall can still enforce the fundamental DMZ policy: permit only specifically required inbound traffic from the Internet to designated public servers, tightly control traffic between the DMZ and internal networks, and prevent direct Internet-originated access to workstations.

Segregating Internet-exposed servers reduces the chance that compromise of a web, mail, DNS, or similar public service becomes immediate access to internal user endpoints and business systems. The firewall rules protecting a DMZ should follow least privilege, allowing only necessary protocols, source and destination addresses, and ports. Stateful firewalls can provide additional connection-awareness and are often preferable, but they are not a prerequisite for the architectural separation supplied by a DMZ. NIST describes firewalls as mechanisms for controlling traffic between networks with differing security requirements and discusses DMZ-style perimeter architectures in its Guidelines on Firewalls and Firewall Policy (SP 800-41 Rev. 1). See also the NCSC network security guidance on network segregation and controlling access between network zones.