PassQueen
a.k.a dumpsqueen.com

EC-Council Certified Security Analyst (ECSA)

ECCouncil 412-79

Version Demo

Total Demo Questions: 42

Total Premium Questions: 423

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Penetration Testing Essential Concepts	103
Topic 2, Penetration Testing Scoping and Engagement Methodology	35
Topic 3, Open Source Intelligence (OSINT)	23
Topic 4, Social Engineering Penetration Testing	12
Topic 5, Network Penetration Testing	139
Topic 6, Web Application Penetration Testing	31
Topic 7, Wireless Penetration Testing	14
Topic 8, Password Cracking	17
Topic 9, SQL Injection	14
Topic 10, Cloud Penetration Testing	1
Topic 11, Report Writing and Post Testing Actions	29
Topic 12, Mix Questions	5
Total	423

QUESTION NO: 1

An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.

A. logical

B. anti-magnetic

C. magnetic

D. optical

ANSWER: D

Explanation:

optical is correct because CDs and DVDs store information as physical patterns—such as pits and lands or changes in reflectivity—on a disc surface. An optical drive reads those patterns using a laser and converts the reflected light into digital data. Unlike a hard disk drive, magnetic tape, or floppy disk, this storage mechanism does not depend on magnetic domains to represent the recorded information. Therefore, exposing a conventional CD or DVD to a large magnet does not reliably erase its contents. Secure disposal of optical discs instead requires methods that physically destroy or render the optical layer unreadable, such as shredding with equipment designed for optical media, pulverizing, or otherwise destroying the data-bearing layer according to the organization's media-sanitization policy. NIST's media-sanitization guidance distinguishes sanitization approaches according to the storage medium and emphasizes selecting a technique that is appropriate for the medium's recording technology and the required level of protection. The basic structure and laser-based reading method of optical discs are described by the Encyclopaedia Britannica overview of compact discs. For practical sanitization planning, consult NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization.

QUESTION NO: 2

Diskcopy is:

A. a utility byAccessData

B. a standard MS-DOS command

C. Digital Intelligence utility

D. dd copying tool

ANSWER: B

Explanation:

The correct answer is **a standard MS-DOS command**. DISKCOPY is a legacy MS-DOS command designed to duplicate the complete contents of one floppy disk onto another floppy disk. Unlike copying individual files, it performs a disk-level copy: it reads the source disk and writes its contents to a destination disk, making it useful where the goal is to reproduce the disk rather than selectively transfer files. The command is commonly associated with DOS-era removable media and can prompt the operator to insert the source and target disks when only one floppy drive is available. In an ECSA or forensic context, this distinction matters because DISKCOPY represents an operating-system command for making a duplicate of traditional floppy media, rather than a specialized modern forensic-imaging product. Microsoft's historical command documentation describes DISKCOPY as copying the contents of one floppy disk to another, and notes its command syntax and operational behavior. The command's purpose is therefore accurately characterized as a standard MS-DOS command. See Microsoft's DISKCOPY command reference and the Windows command reference overview for background on legacy command-line utilities.

QUESTION NO: 3

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame. What ports should you open for SNMP to work through Firewalls (Select 2)

A. 162

B. 160

C. 161

D. 163

ANSWER: A C

Explanation:

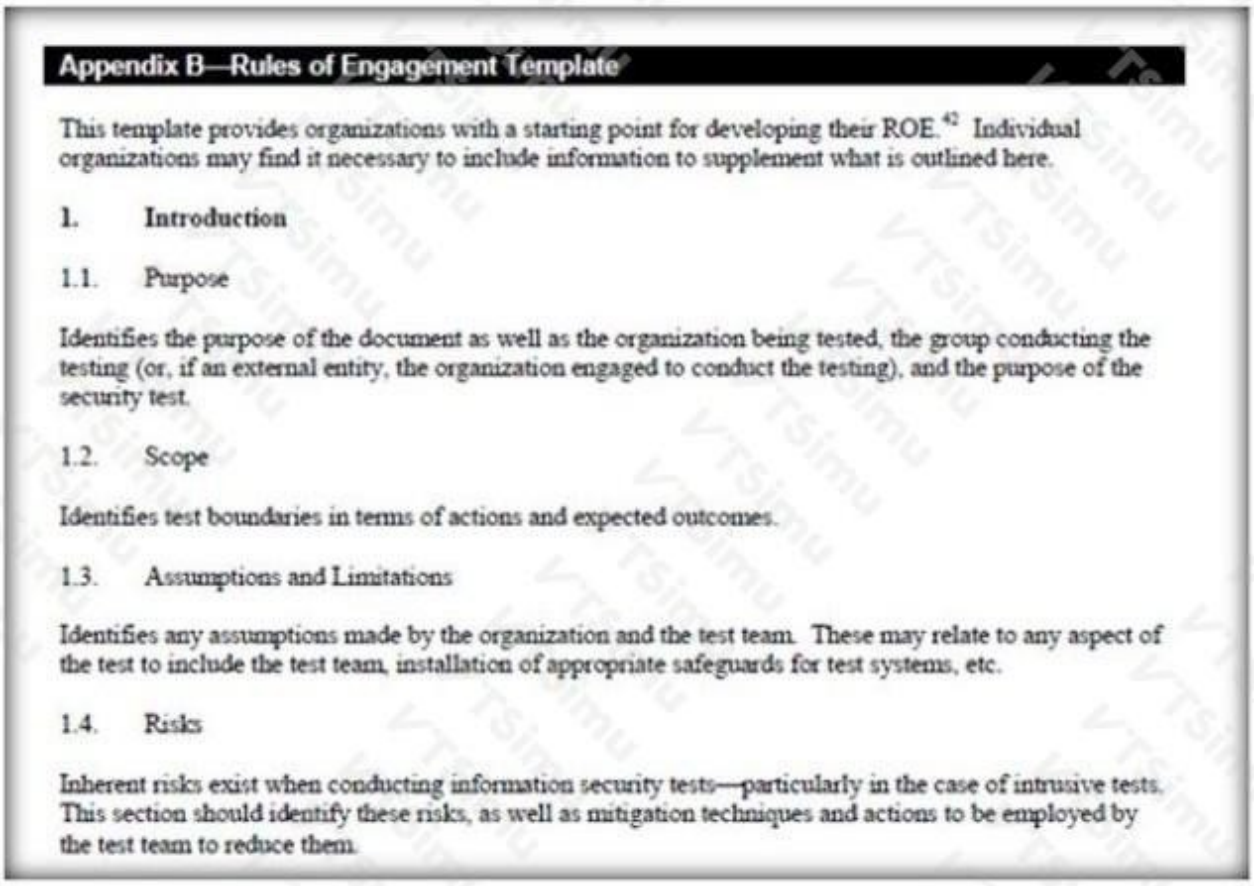
161 and **162** are the standard SNMP ports and should be permitted as required by the organization's monitoring design. SNMP agents normally listen on UDP port 161 for requests from an SNMP manager, including polling requests such as GET, GETNEXT, GETBULK, and SET operations. Therefore, a firewall between the manager and remote-office devices must allow the manager to reach the agents on UDP 161, with return traffic allowed by the firewall's stateful rules or corresponding access-control rules.

UDP port 162 is used by the SNMP manager or notification receiver to receive unsolicited SNMP notifications, traditionally called traps, as well as informs. If remote-office agents send traps or informs to the central monitoring system, the firewall must permit the agents' traffic to the manager's UDP 162 listener. In practice, firewall rules should be limited to the known manager and agent IP addresses rather than broadly opening these ports. The IANA service-name registry assigns *snmp* to port 161 and *snmptrap* to port 162, and the SNMP transport mappings specify these well-known UDP ports. See the IANA Service Name and Port Number Registry and RFC 3417.

QUESTION NO: 4

Rule of Engagement (ROE) is the formal permission to conduct a pen-test. It provides top-level guidance for conducting the penetration testing.

Various factors are considered while preparing the scope of ROE which clearly explain the limits associated with the security test.



Appendix B—Rules of Engagement Template

This template provides organizations with a starting point for developing their ROE.[42] Individual organizations may find it necessary to include information to supplement what is outlined here.

1. Introduction

1.1. Purpose

Identifies the purpose of the document as well as the organization being tested, the group conducting the testing (or, if an external entity, the organization engaged to conduct the testing), and the purpose of the security test.

1.2. Scope

Identifies test boundaries in terms of actions and expected outcomes.

1.3. Assumptions and Limitations

Identifies any assumptions made by the organization and the test team. These may relate to any aspect of the test to include the test team, installation of appropriate safeguards for test systems, etc.

1.4. Risks

Inherent risks exist when conducting information security tests—particularly in the case of intrusive tests. This section should identify these risks, as well as mitigation techniques and actions to be employed by the test team to reduce them.

Which of the following factors is NOT considered while preparing the scope of the Rules of Engagment (ROE)?

A. A list of employees in the client organization

B. A list of acceptable testing techniques

C. Specific IP addresses/ranges to be tested

D. Points of contact for the penetration testing team

ANSWER: A

Explanation:

A list of employees in the client organization is not ordinarily a scope-setting factor in a penetration-testing Rules of Engagement document. Scope defines the authorized boundaries of the engagement: the systems and network ranges that may be assessed, the permitted methods, operational constraints, timing, escalation procedures, and the responsible contacts who can authorize decisions or respond to an incident. An organization-wide employee list does not itself establish a technical boundary, testing authorization, or an approved activity. Although specific named personnel may be relevant to a narrowly authorized social-engineering assessment, that would be documented as part of a defined target population and an explicitly approved test scenario—not as a general list of employees used to prepare the engagement scope. Properly defining scope protects both the client and the assessment team by making clear which assets and actions have consent, while ensuring that communication can be handled through designated points of contact. NIST's penetration-testing guidance describes establishing rules of engagement and identifying targets, contacts, and testing constraints before testing begins. The Penetration Testing Execution Standard likewise treats Rules of Engagement as the agreement governing authorization, scope, and operational procedures. See NIST SP 800-115 and PTES Rules of Engagement.

QUESTION NO: 5

E-mail logs contain which of the following information to help you in your investigation? (Select up to 4)

A. user account that was used to send the email

B. attachments sent with the e-mail message

C. unique message identifier

D. contents of the e-mail message

E. date and time the message was sent

ANSWER: A C E

Explanation:

Email-server and mail-transfer-agent logs are valuable forensic sources because they record message-processing events and metadata needed to establish a timeline and trace a message's path. The *user account that was used to send the email* identifies the authenticated sender or submitting account associated with the transmission event. This can help correlate the email activity with account logons, IP addresses, and other audit records. A *unique message identifier*, such as a Message-ID header value or a server-assigned queue ID, provides a durable correlation value for following the same message across gateway, relay, delivery, and archival records. The *date and time the message was sent* supplies the chronological evidence required to reconstruct events; investigators should retain the logged time zone and account for clock synchronization when correlating systems. These details are commonly retained as message metadata in mail logs, while the message body and attachments ordinarily require message journaling, mailbox access, or a separate content archive rather than routine transport logging. NIST's incident-handling guidance emphasizes preserving and correlating relevant log evidence, and Microsoft documents message tracing as a way to locate and report email-processing events: NIST SP 800-61 Rev. 2; Microsoft message trace documentation.

QUESTION NO: 6

Which of the following is developed to address security concerns on time and reduce the misuse or threat of attacks in an organization?

A. Vulnerabilities checklists

B. Configuration checklists

C. Action Plan

D. Testing Plan

ANSWER: A

Explanation:

Vulnerabilities checklists are correct because they provide a structured, repeatable way to identify known weaknesses, insecure conditions, missing patches, and exposures that could be exploited in an organization. By documenting the items that must be reviewed and validating them routinely, a security team can prioritize remediation before a weakness is abused. This supports timely risk reduction: findings can be assigned severity, tracked to closure, and reassessed after corrective actions are implemented. Checklists also promote consistency across systems and assessments, reducing the chance that common security issues are overlooked because of an ad hoc or incomplete review process.

In practical vulnerability-management work, a checklist can cover operating-system updates, application versions, unnecessary services, weak authentication settings, exposed ports, default credentials, and known configuration weaknesses. It is therefore an effective operational aid for reducing the attack surface and addressing recurring security concerns systematically. NIST describes security configuration checklists as documents that provide instructions for securely configuring information technology products, while its vulnerability-management guidance emphasizes identifying and remediating vulnerabilities as a continuous process. See NIST SP 800-70 Rev. 4 and CISA Vulnerabilities and Exposures.

QUESTION NO: 7

Windows identifies which application to open a file with by examining which of the following?

A. The File extension

B. The file attributes

C. The file Signature at the end of the file

D. The file signature at the beginning of the file

ANSWER: A

Explanation:

Windows normally determines the application used when a user opens a file through its file-association mechanism, which is primarily based on **the File extension**. For example, when a user opens a file named `report.pdf`, Windows uses the `.pdf` extension to look up the registered association and launches the configured PDF-handling application. These associations are represented in the Windows Registry and may be set system-wide or per user. Users can also change the default application associated with a particular extension through Windows Default Apps settings or the file Properties dialog. This behavior is important in security assessments because an extension is metadata in a filename rather than proof of the file's true internal format; a file can be renamed with a misleading extension. Therefore, security tools and content-validation processes may additionally inspect file contents or signatures, but that is not the normal Windows shell mechanism for selecting the application to open a file. Microsoft documents file-extension associations and default-app configuration at File Types and Change default apps in Windows.

QUESTION NO: 8

Which of the following will not handle routing protocols properly?

A. "Internet-router-firewall-net architecture"

B. "Internet-firewall-router-net architecture"

C. "Internet-firewall -net architecture"

D. "Internet-firewall/router(edge device)-net architecture"

ANSWER: B

Explanation:

"Internet-firewall-router-net architecture" will not handle routing protocols properly because the firewall is positioned between the Internet-facing routing domain and the router that must exchange routing information with external peers. Dynamic routing protocols require the router to send and receive specific protocol traffic, and some protocols depend on multicast communication or use IP protocol numbers rather than TCP or UDP ports. A conventional firewall policy may not inspect, forward, or correctly support this traffic unless it is explicitly designed and configured to do so. Consequently, placing a firewall before the router can interfere with route advertisements, neighbor formation, and routing-table convergence. Network designs normally put the edge router at the Internet boundary so it can perform its routing role, while the firewall controls traffic moving from that routed edge toward protected internal networks. Cisco's routing documentation describes how routing protocols establish neighbor relationships and exchange routing information, while Cisco's firewall guidance notes that protocol-specific inspection and policy handling may be required for traffic crossing a firewall. See Cisco OSPF configuration documentation and Cisco ASA inspection documentation.

QUESTION NO: 9

You are working in the security Department of law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?

A. 10

B. 25

C. 110

D. 135

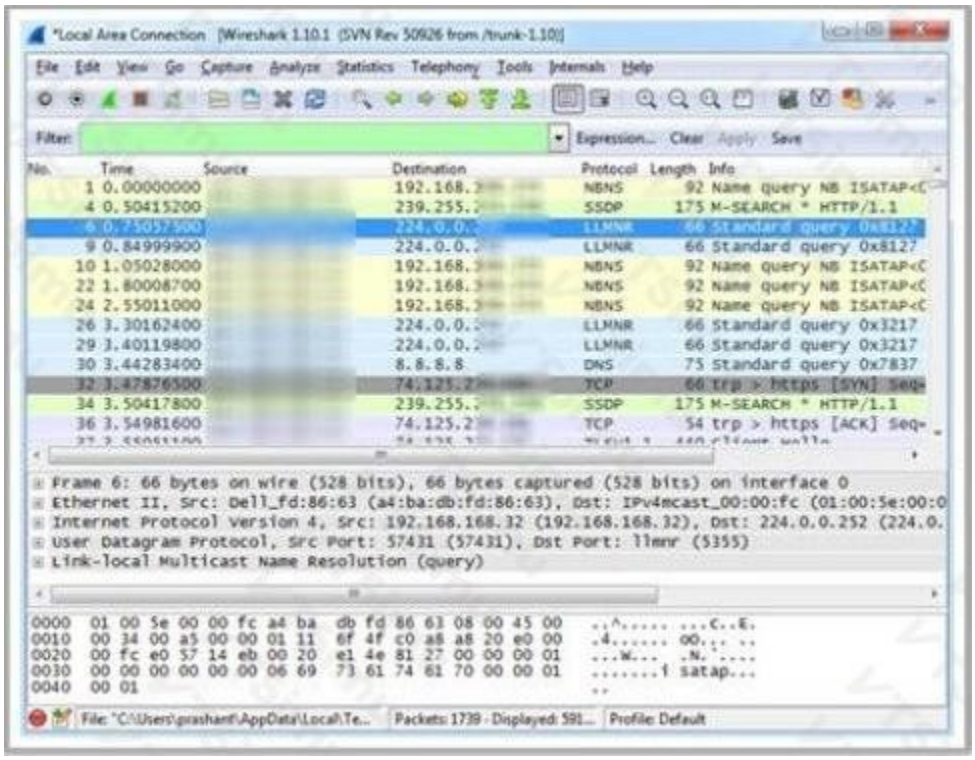
ANSWER: B

Explanation:

25 is correct because the Simple Mail Transfer Protocol (SMTP) traditionally uses TCP port 25 for server-to-server email relay and for SMTP service listening on mail servers. SMTP is the protocol responsible for submitting and transferring email messages; its protocol design permits message-envelope fields, including the sender address, to be supplied by the connecting client. This is why a message can be made to appear to originate from a particular address when a server permits unauthenticated or insufficiently restricted SMTP submission or relay. Modern mail systems commonly apply authentication, sender-policy controls, and other anti-spoofing measures, but these protections do not change SMTP's well-known port assignment. The Internet Assigned Numbers Authority lists SMTP as assigned to TCP port 25. RFC 5321 also defines SMTP's standard TCP service endpoint as port 25. In a legitimate security-testing context, this port would be relevant when communicating with an organization's SMTP relay service, provided the test is explicitly authorized and performed within the established scope. See the IANA Service Name and Port Number Registry and RFC 5321, section 3.1.

QUESTION NO: 10

Which Wireshark filter displays all the packets where the IP address of the source host is 10.0.0.7?



A. ip.dst==10.0.0.7

B. ip.port==10.0.0.7

C. ip.src==10.0.0.7

D. ip.dstport==10.0.0.7

ANSWER: C

Explanation:

`ip.src==10.0.0.7` is the appropriate Wireshark display filter because `ip.src` identifies the source-address field of an IPv4 packet. Applying this expression instructs Wireshark to show packets whose IPv4 source address exactly matches `10.0.0.7`, regardless of the destination address, upper-layer protocol, or port number. This is useful when analyzing activity initiated by a particular host, such as reviewing connections, requests, scans, or possible data exfiltration originating from that system. Wireshark display filters use protocol fields and comparison operators; the double-equals operator performs an equality comparison against the supplied IPv4 address. The filter is entered in Wireshark's display-filter bar after packets have been captured, allowing the analyst to narrow the displayed packet set without altering the underlying capture file. Wireshark's display-filter reference documents `ip.src` as the IPv4 source-address field, and its User's Guide describes the syntax and operation of display filters. See the Wireshark IPv4 display-filter reference and the Wireshark User's Guide on display filters.

QUESTION NO: 11

During the course of a corporate investigation, you find that an Employee is committing a crime. Can the Employer file a criminal complain with Police?

A. Yes, and all evidence can be turned over to the police

B. Yes, but only if you turn the evidence over to a federal law enforcement agency

C. No, because the investigation was conducted without following standard police procedures

D. No, because the investigation was conducted without warrant

ANSWER: A

Explanation:

Yes, and all evidence can be turned over to the police is correct. A corporate investigation is a private-sector inquiry conducted on behalf of the employer, and an employer that discovers suspected criminal conduct may make a report or criminal complaint to the appropriate police agency. The employer may also voluntarily preserve and provide relevant evidence obtained during its investigation, such as records, device images, access logs, witness statements, emails, or other materials that may assist law enforcement. The employer should maintain the integrity of that material by documenting collection, handling, dates, responsible personnel, and any transfers to law enforcement. This supports authenticity and continuity if the matter later proceeds to a criminal investigation or prosecution. A private employer is not required to obtain a police warrant before reporting suspected crime or voluntarily providing its own lawfully held business records and investigative evidence. After receiving the report, police and prosecutors independently decide whether to investigate, seek warrants or other legal process where required, and pursue charges. In practice, the organization should coordinate disclosure with legal counsel, especially where personal data, privileged material, regulated information, or cross-border data is involved. The U.S. Department of Justice explains law-enforcement reporting and investigative responsibilities at https://www.justice.gov/criminal/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime. Evidence-handling principles are also described by NIST in NIST SP 800-86.

QUESTION NO: 12

John, a penetration tester from a pen test firm, was asked to collect information about the host file in a Windows system directory. Which of the following is the location of the host file in Window system directory?

A. C:\Windows\System32\Boot

B. C:\WINNT\system32\drivers\etc\hosts

C. C:\WINDOWS\system32\cmd.exe

D. C:\Windows\System32\restore

ANSWER: B

Explanation:

`C:\WINNT\system32\drivers\etc\hosts` is the appropriate answer for a Windows installation whose system root is `C:\WINNT`, as commonly seen on legacy Windows NT-family systems. The Hosts file is a plain-text, local hostname-resolution file. Before querying DNS, Windows can use entries in this file to map host names to IP addresses; consequently, it is a useful artifact during penetration-testing reconnaissance and configuration review. The relevant directory is the `system32\drivers\etc` directory beneath the operating system's configured system root, and the actual file name is `hosts`, with no file extension. Modern Windows installations generally use `C:\Windows` as the system root, producing the analogous default path `C:\Windows\System32\drivers\etc\hosts`. The question's stated `C:\WINNT` system root therefore makes the listed legacy path the correct location. Microsoft documents the Hosts file as a local file that maps host names to IP addresses and is used in name resolution; see Microsoft Learn: Hosts file. Additional background on Windows name resolution and the Hosts file is available from Microsoft Support: Configure TCP/IP to use DNS.

QUESTION NO: 13

You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Use attack as a launching point to penetrate deeper into the network

B. Demonstrate that no system can be protected against DoS attacks

C. List weak points on their network

D. Show outdated equipment so it can be replaced

ANSWER: C

Explanation:

List weak points on their network is correct because a denial-of-service test evaluates the availability component of security and can reveal weaknesses in how a target environment handles excessive, malformed, or resource-intensive traffic. When explicitly authorized and tightly scoped in the rules of engagement, the test can identify capacity bottlenecks, unprotected network paths, single points of failure, inadequate rate limiting, weak resilience controls, and insufficient monitoring or incident-response procedures. The useful result is documented evidence of where service availability may fail, together with the observed impact and recommendations for remediation. This enables the organization to prioritize safeguards such as traffic filtering, redundancy, upstream mitigation, service hardening, alerting, and tested recovery procedures. Because DoS testing can disrupt production services, a professional engagement should define permitted techniques, targets, timing, stop conditions, notification contacts, and rollback procedures before execution. NIST's security testing guidance emphasizes that assessment activities should be planned, authorized, and used to identify vulnerabilities and improve the security posture. See NIST SP 800-115, Technical Guide to Information Security Testing and Assessment and the CISA guidance on denial-of-service attacks.

QUESTION NO: 14

The offset in a hexadecimal code is:

A. The last byte after the colon

B. The 0x at the beginning of the code

C. The 0x at the end of the code

D. The first byte after the colon

E. The hexadecimal address shown at the beginning of a hex-dump line, before the colon

ANSWER: E

Explanation:

An offset is the position of a byte or sequence of bytes relative to the beginning of the data source (or, in some contexts, relative to a specified base address). In a conventional hex dump, it is normally the numeric value printed at the far left of each row, before the colon; for example, in `00000010: 48 65 6C 6C 6F`, `00000010` identifies the location at which that row's bytes begin. It is commonly displayed in hexadecimal, which makes it easier to correlate byte locations with addresses, file structures, and forensic findings. The `0x` prefix is merely a notation used in many programming languages and tools to indicate that a number is written in base 16; it is not itself an offset. A byte shown after the colon is data at the indicated location, rather than the location identifier. The GNU `hexdump` documentation describes output formats that include an address/offset field, and the Linux manual page shows address values being printed before data output. See the GNU Coreutils documentation for hexadecimal output and the hexdump manual page.

QUESTION NO: 15

Attackers create secret accounts and gain illegal access to resources using backdoor while bypassing the authentication procedures. Creating a backdoor is a where an attacker obtains remote access to a computer on a network.



Which of the following techniques do attackers use to create backdoors to covertly gather critical information about a target machine?

A. Internal network mapping to map the internal network of the target machine

B. Port scanning to determine what ports are open or in use on the target machine

C. Sniffing to monitor all the incoming and outgoing network traffic

D. Social engineering and spear phishing attacks to install malicious programs on the target machine

ANSWER: D

Explanation:

Social engineering and spear phishing attacks to install malicious programs on the target machine is correct because it describes a common initial-access and delivery method for establishing a persistent covert foothold. An attacker can craft a

convincing, target-specific email or message that induces a user to open a malicious attachment, follow a malicious link, or execute a disguised program. Once the payload runs, it can install a remote-access trojan, web shell, or other backdoor that enables the attacker to communicate with the compromised host, maintain access, and collect sensitive system or user information without normal user authentication. Spear phishing is especially effective for this purpose because the attacker tailors the lure to a particular individual, role, or organization, increasing the chance that the malicious program is executed. MITRE ATT&CK identifies spearphishing attachments and links as phishing techniques used to gain access, while its software and persistence tactics document how malware can retain remote access after execution. See MITRE ATT&CK: Phishing and MITRE ATT&CK: Persistence.

QUESTION NO: 16

You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printer out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the _____ in order to track the emails back to the suspect.

A. Routing Table

B. Firewall log

C. Configuration files

D. Email Header

ANSWER: D

Explanation:

Email Header is correct because complete email headers preserve the technical delivery metadata needed to trace a message's route. Although a printed email may show the visible sender, recipient, date, and subject, it often omits the full headers. Examining the original message on the complainant's computer or in the mail account allows the investigator to acquire the header data in its native context and preserve it as evidence. Of particular forensic value are the ordered `Received:` fields, which document the mail servers that processed the message and can identify the originating server or source IP address, subject to factors such as relays, spoofing, or anonymization services. Headers may also contain Message-ID values, authentication results, return-path information, and timestamps that help correlate messages with provider records and logs. The investigator should preserve the original emails and associated metadata using sound evidence-handling procedures, then work through the appropriate legal process to request supporting records from the relevant email or network provider. The Internet Engineering Task Force specifies the standard format for Internet message header fields in RFC 5322. Google's guidance also explains how to view full message headers and analyze delivery information in an email message: View message headers in Gmail.

QUESTION NO: 17

An automated electronic mail message from a mail system which indicates that the user does not exist on that server is called as?

A. SMTP Queue Bouncing

B. SMTP Message Bouncing

C. SMTP Server Bouncing

D. SMTP Mail Bouncing

ANSWER: D

Explanation:

SMTP Mail Bouncing is the intended answer. In standard email terminology, this is commonly called a *bounce message* or a non-delivery report (NDR). A receiving SMTP server generates this type of automated delivery-status notification when it

cannot deliver a message to the addressed mailbox, including when the local part of the recipient address does not identify an existing user. The original sender or the sender's return-path address receives the notification, allowing the sender or a mail administrator to identify and correct an invalid recipient address.

SMTP defines permanent delivery failures using the 5xx response class. In particular, a recipient mailbox that cannot be found is commonly represented by the enhanced status code `5.1.1`, meaning "Bad destination mailbox address." After accepting a message and subsequently determining delivery cannot be completed, a mail system reports that outcome through a delivery-status notification, which is the formal mechanism behind a bounced email. This behavior is relevant in security testing because mail-server responses and bounce handling can reveal whether recipient accounts or addresses are valid. See RFC 5321: Simple Mail Transfer Protocol and RFC 3464: Delivery Status Notifications.

QUESTION NO: 18

What threat categories should you use to prioritize vulnerabilities detected in the pen testing report?

A. 1, 2, 3, 4, 5

B. Low, medium, high, serious, critical

C. Urgent, dispute, action, zero, low

D. A, b, c, d, e

ANSWER: B

Explanation:

Low, medium, high, serious, critical is the appropriate ordered set of threat categories for prioritizing findings in this penetration-testing report context. A useful report must translate technical evidence into a clear remediation sequence for management and system owners. These labels provide a graduated scale that distinguishes issues with limited business or technical consequence from those that require immediate attention because they could enable substantial compromise, service disruption, or loss of sensitive data. Applying the categories consistently requires considering exploitability, the affected asset's importance, exposure, existing controls, and the realistic impact of successful exploitation. The resulting severity should be recorded with the finding, supporting evidence, affected systems, and a practical remediation recommendation, so that critical and serious issues can be assigned, tracked, and remediated first. This approach is consistent with risk-based vulnerability management: technical weaknesses are prioritized according to the likelihood and impact relevant to the organization rather than merely listed in discovery order. NIST describes risk assessment as identifying and estimating risk to support risk-management decisions, while the CVSS framework provides a standardized way to communicate vulnerability severity characteristics. See NIST SP 800-30 Rev. 1 and FIRST CVSS.

QUESTION NO: 19

During the process of fingerprinting a web application environment, what do you need to do in order to analyze HTTP and HTTPS request headers and the HTML source code?

A. Examine Source of the Available Pages

B. Perform Web Spidering

C. Perform Banner Grabbing

D. Check the HTTP and HTML Processing by the Browser

ANSWER: D

Explanation:

Checking the HTTP and HTML processing by the browser is the appropriate activity because browser developer tools expose both the client-side document and the network exchanges used to obtain it. During web-application fingerprinting, an assessor can inspect the page's rendered DOM and original HTML, then use the browser Network panel to review HTTP or

HTTPS requests and responses. This reveals request methods, URLs, parameters, cookies, response headers, redirects, content types, caching directives, security headers, and technology-related indicators. The information is useful for identifying how the application communicates, which resources and endpoints it exposes, and clues about its hosting or application stack.

Modern browser developer tools are designed for exactly this type of inspection. For example, the Network panel records resource requests and provides their headers, while the Elements/Inspector view enables examination of the HTML and DOM associated with a page. HTTPS does not prevent this analysis when it is performed in the browser that established the secure session; the browser can display the decrypted request and response details to its user. See the Chrome DevTools Network reference and MDN's browser developer tools overview.

QUESTION NO: 20

Identify the policy that defines the standards for the organizational network connectivity and security standards for computers that are connected in the organizational network.

A. Information-Protection Policy

B. Special-Access Policy

C. Remote-Access Policy

D. Acceptable-Use Policy

E. Network-Connection Policy

ANSWER: E

Explanation:

Network-Connection Policy is correct because it establishes the organization's required conditions for devices that connect to its internal network. Its scope includes network-connectivity requirements and the security baseline that connected computers must meet, such as approved configuration, authentication, endpoint protection, patch status, and compliance with network-access controls. In other words, it governs whether and how a computer may attach to the organizational network and defines the security standards applicable to that connection.

This type of policy supports the principle that devices should not receive network access merely because they are physically or logically able to connect. Instead, access should be controlled and tied to defined technical safeguards. NIST's access-control guidance describes the need to control system and network access, including the enforcement of organizationally defined access requirements. CISA likewise emphasizes securing network infrastructure and managing devices connected to enterprise networks. These practices make a Network-Connection Policy the policy category that directly addresses security and connectivity standards for computers attached to the organizational network. See NIST SP 800-53, Access Control and CISA guidance on securing network infrastructure devices.

QUESTION NO: 21

If a suspect computer is located in an area that may have toxic chemicals, you must:

A. coordinate with the HAZMAT team

B. determine a way to obtain the suspect computer

C. assume the suspect machine is contaminated

D. do not enter alone

ANSWER: A

Explanation:

coordinate with the HAZMAT team is correct because a potentially toxic environment is first a personnel-safety incident, not solely a digital-evidence collection issue. Hazardous-materials specialists are trained and equipped to identify chemical hazards, establish safe entry procedures and protective-equipment requirements, control contamination, and determine whether the area can safely be entered and items removed. A forensic examiner should not independently assess chemical exposure risks or attempt to retrieve a device before the scene has been evaluated and managed by qualified responders. Coordination also helps preserve evidentiary integrity: the HAZMAT team can advise on decontamination, packaging, handling restrictions, and chain-of-custody considerations for equipment that may have been exposed to hazardous substances. U.S. OSHA guidance emphasizes that hazardous-waste operations require a site-specific safety and health plan and appropriate hazard controls, while FEMA describes hazardous-materials response as involving trained personnel who assess and mitigate chemical threats. These practices align with sound incident-response and digital-forensics procedures, where life safety and scene safety take priority before evidence acquisition begins. See OSHA 29 CFR 1910.120, Hazardous Waste Operations and Emergency Response and FEMA National Response Framework.

QUESTION NO: 22

In the context of file deletion process, which of the following statement holds true?

A. When files are deleted, the data is overwritten and the cluster marked as available

B. The longer a disk is inuse, the less likely it is that deleted files will be overwritten

C. While booting, the machine may create temporary files that can delete evidence

D. Secure delete programs work by completely overwriting the file in one go

ANSWER: C D

Explanation:

While booting, the machine may create temporary files that can delete evidence because ordinary deletion generally changes filesystem metadata rather than immediately erasing the underlying file content. The blocks or clusters previously used by a deleted file can remain available for later allocation. During startup, the operating system and applications may write logs, paging data, caches, temporary files, updates, and other operational data. Such writes can reuse those available locations and overwrite remnants that could otherwise be recovered during forensic examination. This is why incident-response and forensic practice emphasizes avoiding unnecessary booting or use of a system that may contain evidence, and instead acquiring storage through controlled forensic procedures.

Secure delete programs work by completely overwriting the file in one go in the traditional hard-disk context: they write replacement data to the file's allocated storage before removing its filesystem reference. A full overwrite pass is intended to prevent recovery of the former content from the reused sectors; NIST recognizes overwrite as a media-sanitization technique for applicable storage media. In practice, the effectiveness of any overwrite-based method depends on the storage technology and its handling of physical locations, so validated sanitization procedures are important. See NIST SP 800-88 Rev. 1 and the NIST data-protection guidance.

QUESTION NO: 23

Assessing a network from a hacker's point of view to discover the exploits and vulnerabilities that are accessible to the outside world is which sort of vulnerability assessment?

A. Network Assessments

B. Application Assessments

C. Wireless Network Assessments

D. External Assessment

ANSWER: D

Explanation:

External Assessment is correct because it evaluates an organization's externally exposed attack surface from the perspective of an unauthenticated Internet-based attacker. The assessment identifies public-facing systems and services—such as web applications, VPN gateways, mail servers, DNS infrastructure, and remote-access portals—and determines whether vulnerabilities or configuration weaknesses can be discovered and exploited from outside the organization's network perimeter. This perspective is essential because an external threat actor generally begins with only publicly available information and access to Internet-reachable assets. The assessment therefore focuses on reconnaissance, service enumeration, vulnerability identification, and validation of exposure without assuming internal network access or trusted credentials. This directly matches the question's emphasis on exploits and vulnerabilities accessible "to the outside world." NIST describes external testing as testing performed from outside the target organization's network boundary, while PCI DSS guidance similarly distinguishes external vulnerability scanning as scanning systems exposed to untrusted networks. These practices help organizations prioritize remediation of weaknesses that could enable an initial compromise from the Internet. See NIST SP 800-115, Technical Guide to Information Security Testing and Assessment and PCI DSS Document Library.

QUESTION NO: 24

What information can be collected by dumpster diving?

A. Sensitive documents

B. Email messages

C. Customer contact information

D. All the above

ANSWER: D

Explanation:

All the above is correct because dumpster diving is a social-engineering and physical-information-gathering technique in which an attacker searches an organization's discarded materials for useful intelligence. Waste can contain sensitive documents, including internal reports, network diagrams, passwords, financial records, and printed communications. It may also include customer contact information from discarded forms, mailing lists, account paperwork, or reports. Printed email messages, email headers, message extracts, and other communications can similarly be recovered when they have been disposed of without appropriate destruction. Even partial records can help an assessor or attacker profile personnel, identify systems and business processes, create convincing phishing pretexts, or discover information that supports further access attempts. Secure disposal must therefore cover both paper and electronic media; organizations should use controls such as cross-cut shredding, locked disposal bins, retention procedures, and media sanitization. CISA's guidance on protecting sensitive information emphasizes securely destroying information when it is no longer needed, while NIST provides detailed sanitization guidance for media that may contain organizational data. See CISA: Protecting Sensitive Information and NIST SP 800-88 Rev. 1: Guidelines for Media Sanitization.