DUMPSBOSS.

EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

ECCouncil ECSAv10

Version Demo

Total Demo Questions: 20

Total Premium Questions: 383

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Penetration Testing Essential Concepts	45
Topic 2, Penetration Testing Scoping and Engagement Methodology	34
Topic 3, Open Source Intelligence (OSINT)	20
Topic 4, Social Engineering Penetration Testing	16
Topic 5, Network Penetration Testing	155
Topic 6, Web Application Penetration Testing	63
Topic 7, Wireless Penetration Testing	24
Topic 8, IoT Penetration Testing	5
Topic 9, Cloud Penetration Testing	9
Topic 10, Report Writing and Post Testing Actions	12
Total	383

QUESTION NO: 1

Vulnerability assessment is an examination of the ability of a system or application, including current security procedures and controls, to withstand assault. It recognizes, measures, and classifies security vulnerabilities in a computer system, network, and communication channels.

A vulnerability assessment is used to identify weaknesses that could be exploited and predict the effectiveness of additional security measures in protecting information resources from attack.

Which of the following vulnerability assessment technique is used to test the web server infrastructure for any misconfiguration and outdated content?

A. Passive Assessment

B. Host-based Assessment

C. External Assessment

D. Application Assessment

ANSWER: D

Explanation:

Application Assessment is correct because this assessment approach evaluates the security of a web application and the web-server environment that supports it. Its scope commonly includes reviewing server and application configuration, exposed functionality, HTTP methods, directory and file handling, default content, error handling, installed components, and software versions. These checks identify insecure settings and obsolete content or components that may expose known vulnerabilities or unnecessary attack surface.

In a web context, application assessment is not limited to testing the application's custom code or input fields. It also examines the deployment stack and configuration choices that affect how the application is delivered and protected. A tester can therefore identify web-server misconfigurations such as unsafe defaults, enabled administrative interfaces, unnecessary services, weak TLS settings, directory listing, and outdated server-side frameworks or libraries. This makes it the appropriate technique for assessing both the web-facing application and infrastructure conditions described in the question.

The OWASP Web Security Testing Guide identifies configuration and deployment management testing as a core part of web-application security testing: OWASP Web Security Testing Guide. OWASP also documents risks associated with vulnerable and outdated components: OWASP Top 10: Vulnerable and Outdated Components.

QUESTION NO: 2

The Finger service displays information such as currently logged-on users, email address, full name, etc. Which among the following ports would you scan to identify this service during a penetration test?

A. Port 89

B. Port 99

C. Port 69

D. Port 79

ANSWER: D

Explanation:

The correct answer is **Port 79**. The Finger protocol is a legacy TCP/IP application-layer service used to retrieve user-related information from a remote system. Depending on server configuration, responses may disclose details such as account names, users currently logged in, full names, home directories, login shells, idle times, and other information useful during reconnaissance. Finger is assigned the well-known TCP port 79 by the Internet Assigned Numbers Authority (IANA). During a penetration test, scanning TCP/79 can identify whether a Finger daemon is listening. If the service is exposed, an assessor may query it carefully to determine whether it reveals information that could support account enumeration or social-engineering scenarios. Because Finger commonly transmits responses in clear text and can expose unnecessary user metadata, modern systems generally disable it unless there is a specific operational requirement. The IANA Service Name and Transport Protocol Port Number Registry lists *finger* as using TCP port 79, and RFC 1288 defines the Finger User Information Protocol and its intended user-information queries. See the IANA service-name registry entry for Finger and RFC 1288.

QUESTION NO: 3

Identify the type of testing that is carried out without giving any information to the employees or administrative head of the organization.

A. Unannounced Testing

B. Double Blind Testing

C. Announced Testing

D. Blind Testing

ANSWER: B

Explanation:

Double Blind Testing is correct because it is designed to simulate a highly realistic attack scenario in which both the penetration tester and the organization's defensive personnel operate with minimal prior knowledge. In this model, employees and the administrative or security leadership are not informed in advance that the assessment is occurring. That lack of notification allows the engagement to evaluate whether normal monitoring, escalation, incident-response, and decision-making processes identify and handle the simulated intrusion as they would a genuine attack.

The defining value of double-blind testing is that it measures the organization's practical defensive readiness rather than merely validating technical controls in a coordinated exercise. The tester must perform reconnaissance and discovery with limited target knowledge, while the organization's personnel must detect and respond without being primed to expect testing activity. Such exercises require formal authorization and carefully defined rules of engagement before testing begins, even though operational staff are not told about the assessment. NIST describes penetration testing as a process that simulates attacks to identify and validate security weaknesses; see NIST SP 800-115. EC-Council's penetration-testing certification context is available at EC-Council ECSA.

QUESTION NO: 4

Which of the following attributes has a LM and NTLMv1 value as 64bit + 64bit + 64bit and NTLMv2 value as 128 bits?

A. Hash Key Length

B. C/R Value Length

C. C/R Key Length

D. Hash Value Length

ANSWER: B

Explanation:

C/R Value Length is correct because it describes the length of the challenge/response value produced by the authentication protocol. In LM and NTLMv1 authentication, the response is 24 bytes long, commonly expressed as three 64-bit blocks (64 bits + 64 bits + 64 bits). This structure results from using DES-based operations to generate three encrypted blocks from the server challenge. NTLMv2 uses a stronger response construction based on HMAC-MD5. Its NT proof string is 16 bytes, or 128 bits, and is the fixed-length cryptographic proof associated with the NTLMv2 response. Therefore, the stated 192-bit LM/NTLMv1 value and 128-bit NTLMv2 value identify the challenge/response value-length attribute rather than the hash-key or hash-value length. Microsoft's NTLM protocol specification defines the 16-byte NTProofStr in an NTLMv2 response and documents the response message structures: MS-NLMP: NT LAN Manager Protocol. The historical NTLM response construction, including its 24-byte response field, is also specified in RFC 2759.

QUESTION NO: 5

You are working on a pen testing assignment. Your client has asked for a document that shows them the detailed progress of the pen testing. Which document is the client asking for?

A. Scope of work (SOW) document

B. Rule of engagement with signatures of both the parties

C. Project plan with work breakdown structure

D. Engagement log

ANSWER: D

Explanation:

An engagement log is the document used to record the detailed, ongoing progress of a penetration-testing engagement. It serves as a chronological operational record of testing activity, such as dates and times of work, systems assessed, actions performed, evidence collected, communications, encountered issues, and significant decisions or changes made during the engagement. This level of documentation allows the client and the testing team to track what has been completed, understand the current status, and maintain an auditable record that supports later reporting and review.

Maintaining detailed records throughout a security assessment is an established testing practice. NIST describes the importance of documenting assessment activities and results so that the assessment can be managed, reproduced where necessary, and reported accurately. In a penetration test, an engagement log provides that day-to-day traceability while the work is in progress, rather than merely defining the authorized work or presenting a final summary. See NIST SP 800-115: Technical Guide to Information Security Testing and Assessment and the Penetration Testing Execution Standard reporting guidance.

QUESTION NO: 6

Allen and Greg, after investing in their startup company called Zamtac Ltd., developed a new web application for their company. Before hosting the application, they want to test the robustness and immunity of the developed web application against attacks like buffer overflow, DOS, XSS, and SQL injection.

What is the type of the web application security test Allen and Greg should perform?

A. Web fuzzing

B. Web crawling

C. Web spidering

D. Web mirroring

ANSWER: A

Explanation:

Web fuzzing is the appropriate security test because it evaluates how a web application handles unexpected, malformed, excessive, or deliberately invalid input. A fuzzer can repeatedly submit altered values through request parameters, form fields, headers, cookies, APIs, and file-upload interfaces while monitoring the application for crashes, unhandled exceptions, abnormal resource consumption, and unsafe responses. This makes fuzzing particularly useful for identifying robustness weaknesses that can contribute to buffer-overflow conditions and denial-of-service exposure.

For a web application, fuzzing may also use payloads and input mutations intended to expose insecure input handling associated with cross-site scripting and SQL injection. The test should be conducted in an authorized pre-production environment with suitable logging and monitoring so that the team can reproduce discovered failures, identify the affected input path, and fix validation, encoding, query construction, or error-handling weaknesses before deployment. OWASP describes fuzzing as submitting large amounts of random or malformed data to discover flaws and unexpected behavior, while NIST defines fuzz testing as testing software with invalid or unexpected inputs. See the OWASP Fuzzing guidance and the NIST definition of fuzz testing.

QUESTION NO: 7

Jacob is a penetration tester at TechSoft Inc. based at Singapore. The company assigned him the task of conducting penetration test on the IoT devices connected to the corporate network. As part of this process, he captured the network traffic of the devices, their mobile applications, and cloud connections to check whether any critical data are transmitted in plain text. Also, he tried to check whether SSL/TLS protocols are properly updated and implemented.

Which of the following IoT security issues Jacob is dealing with?

A. Poor authentication/authorization

B. Lack of transport encryption

C. Privacy concerns

D. Insecure software/firmware

ANSWER: B

Explanation:

Lack of transport encryption is the issue being assessed. Jacob captures traffic between IoT devices, their companion mobile applications, and cloud services to determine whether sensitive or critical data travels in plaintext. This is a direct test of whether data is protected while in transit across a network. He also evaluates whether SSL/TLS is current and correctly implemented, which is essential because TLS provides confidentiality and integrity protections for application traffic when properly configured and validated.

IoT ecosystems commonly exchange credentials, telemetry, commands, identifiers, and other sensitive information among devices, apps, APIs, and cloud platforms. If these communications do not use secure transport protocols, or use obsolete TLS versions or weak configurations, an attacker able to observe or intercept network traffic may be able to read or manipulate that data. Testing packet captures for unencrypted protocols and reviewing TLS deployment therefore identifies transport-layer protection gaps. OWASP specifically identifies insecure data transfer and storage as an IoT risk area, including the exposure of sensitive information during communications. The OWASP IoT Security Testing Guide also includes testing controls for secure communications and transport encryption. See the OWASP Internet of Things Project and NIST SP 800-52 TLS Guidelines.

QUESTION NO: 8

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:

SNMP communication normally requires UDP ports 161 and 162 to be permitted through intervening firewalls. UDP port 161 is the well-known SNMP service port used when an SNMP manager polls an agent for operational information, such as interface status, device health, counters, and configuration-related values. In a multi-office deployment, a firewall must therefore allow the manager to send UDP requests to the remote SNMP agents on port 161 and allow the corresponding traffic back to the manager. UDP port 162 is used for SNMP notifications, including traps and informs, sent asynchronously by an SNMP agent to the SNMP manager or other configured notification receiver. This traffic is especially important when the manager must receive alerts without waiting for its next polling interval. Firewall policy should be scoped as tightly as possible: restrict sources and destinations to the known SNMP managers and agents, use UDP for standard SNMP transport, and apply SNMPv3 authentication and privacy where supported. The Internet Assigned Numbers Authority registers SNMP at port 161 and SNMPTRAP at port 162: IANA Service Name and Port Number Registry. SNMP transport and notification behavior are also specified in RFC 3417.

QUESTION NO: 9

ABC Technologies, a large financial company, hired a penetration tester to do physical penetration testing. On the first day of his assignment, the penetration tester goes to the company posing as a repairman and starts checking trash bins to collect the sensitive information. What is the penetration tester trying to do?

A. Trying to attempt social Engineering using phishing

B. Trying to attempt social engineering by shoulder surfing

C. Trying to attempt social engineering by eavesdropping

D. Trying to attempt social engineering by dumpster diving

ANSWER: D

Explanation:

Trying to attempt social engineering by dumpster diving is correct. Dumpster diving is a physical information-gathering technique in which an assessor searches discarded material—such as waste bins, recycling containers, or improperly disposed documents and media—for sensitive information. In an authorized physical penetration test, this can reveal items that support later assessment activities, including employee names, phone lists, organizational charts, internal documentation, network diagrams, discarded credentials, or documents containing customer and financial data. Posing as a repairman may help the tester blend into the environment, but the specific activity described is examining trash bins for sensitive information, which is dumpster diving. This scenario evaluates whether the organization has effective disposal controls, such as locked disposal bins, shredding procedures, clean-desk practices, secure media destruction, and staff awareness of information-handling requirements. For a financial company in particular, secure disposal helps reduce the risk that confidential client or business information can be recovered after it is discarded. NIST identifies disposal as part of

media sanitization and describes methods for rendering data on media inaccessible or unrecoverable. See NIST SP 800-88 Rev. 1, Guidelines for Media Sanitization and the CISA guidance on securing data.

QUESTION NO: 10

What is the purpose of the Traceroute command?

A. For extracting information about the network topology, trusted routers, and firewall locations

B. For extracting information about closed ports

C. For extracting information about the server functioning

D. For extracting information about opened ports

ANSWER: A

Explanation:

The purpose of the Traceroute command is to identify the path that packets take from a source host to a destination host. It does this by sending probes with progressively increased time-to-live (TTL) values, causing intermediate routers to return messages when the TTL expires. The resulting output lists the network hops along the route and typically reports round-trip timing for each hop. During authorized reconnaissance or troubleshooting, this information can help an analyst infer aspects of network topology, identify routing devices and path changes, and recognize where packet filtering or firewall behavior may affect traffic. Traceroute does not directly enumerate service ports; rather, it focuses on the Layer 3 path between systems. Implementations vary by platform: the Unix/Linux `traceroute` utility commonly uses UDP probes by default, while Windows `tracert` commonly uses ICMP Echo Requests. The underlying TTL mechanism is standardized in IP, and the command is a useful early-stage network discovery tool when used within the scope of authorization. See the RFC 1812 router requirements for TTL processing requirements and the Microsoft tracert documentation for command behavior and usage.

QUESTION NO: 11

A pen tester has extracted a database name by using a blind SQL injection. Now he begins to test the table inside the database using the below query and finds the table:

IF (LEN(SELECT TOP 1 NAME from sysobjects where xtype='U')=3) WAITFOR DELAY '00:00:10'--

spx?id=1; IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),1,1)))=101) WAITFOR DELAY '00:00:10'--

IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),2,1)))=109) WAITFOR DELAY '00:00:10'--

IF (ASCII(lower(substring((SELECT TOP 1 NAME from sysobjects where xtype=char(85)),3,1)))=112) WAITFOR DELAY '00:00:10'—

What is the table name?

A. CTS

B. QRT

C. EMP

D. ABC

ANSWER: C

Explanation:

EMP is the table name. This is a time-based blind SQL injection extraction sequence: the initial condition establishes that the selected user table name has a length of three characters. The subsequent predicates test each character individually by taking a one-character `SUBSTRING`, normalizing it with `LOWER`, and comparing its `ASCII` value to a guessed numeric value. A true comparison triggers `WAITFOR DELAY`, giving the tester an observable timing signal despite the application not directly returning query output.

The observed values map directly to the lowercase characters in the table name: ASCII decimal 101 is `e`, 109 is `m`, and 112 is `p`. Because the first, second, and third character tests correspond to those values, the recovered three-character identifier is `emp`; SQL Server object names are commonly displayed in uppercase in such answer choices, yielding `EMP`. The query identifies user-defined tables through the `sysobjects` object type value `U`. Microsoft documents SQL Server's object catalog metadata in sys.objects documentation, and documents the character-to-integer conversion used here in its ASCII function reference.

QUESTION NO: 12

Arnold is trying to gain access to a database by inserting exploited query statements with a WHERE clause. He wants to retrieve all the entries from a particular table (e. g. StudName) using the WHERE clause. What query does Arnold need to write to retrieve the information?

A. EXTRACT * FROM StudName WHERE roll_number = 1 order by 1000

B. DUMP * FROM StudName WHERE roll_number = 1 AND 1=1—

C. SELECT * FROM StudName WHERE roll_number = '' or '1' = '1'

D. RETRIVE * FROM StudName WHERE roll_number = 1'#

E. SELECT * FROM StudName WHERE roll_number = 1 OR 1=1 --

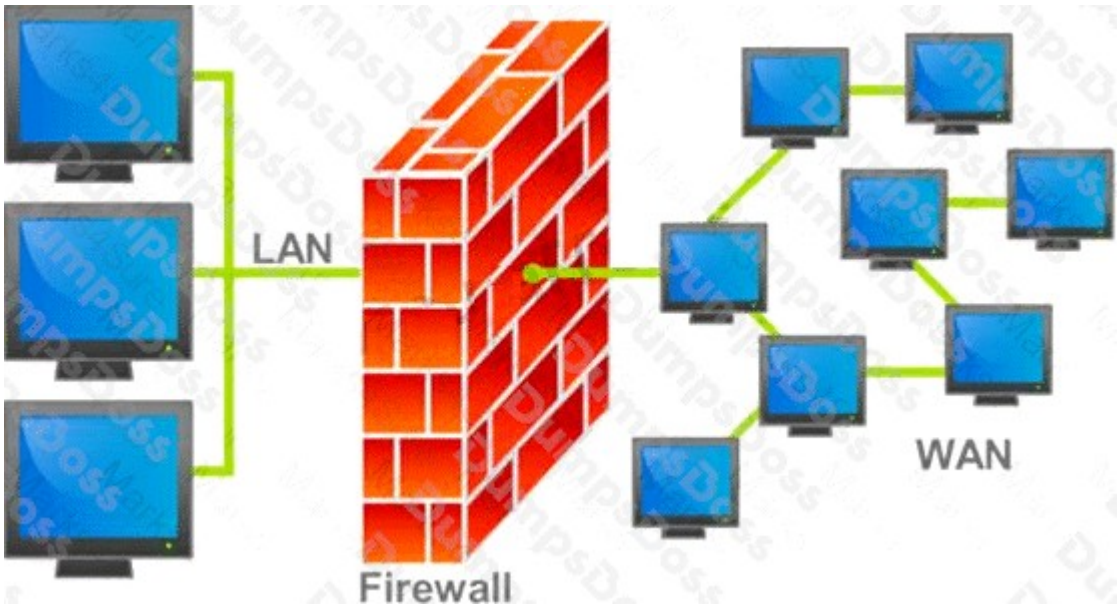
ANSWER: E

Explanation:

`SELECT * FROM StudName WHERE roll_number = 1 OR 1=1 --` is the correct query because the `OR 1=1` predicate is a tautology: it evaluates to true for every row. In a vulnerable application that concatenates untrusted input directly into an SQL statement, adding this predicate can cause the `WHERE` clause to match every record in `StudName`, rather than only a specific roll number. The trailing SQL comment marker prevents any remaining text appended by the application—such as a closing quote or additional condition—from changing the intended query structure. This illustrates the classic SQL-injection pattern in which attacker-controlled input changes query logic. In practice, developers should prevent this class of flaw by using parameterized queries (prepared statements), which keep data values separate from SQL syntax, along with least-privilege database accounts and appropriate input handling. OWASP describes SQL injection and its prevention in its SQL Injection Prevention Cheat Sheet; SQL comment syntax is also documented in the PostgreSQL SQL lexical structure documentation.

QUESTION NO: 13

A firewall protects networked computers from intentional hostile intrusion that could compromise confidentiality or result in data corruption or denial of service. It examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped.



Why is an appliance-based firewall is more secure than those implemented on top of the commercial operating system (Software based)?

A. Appliance based firewalls cannot be upgraded

B. Firewalls implemented on a hardware firewall are highly scalable

C. Hardware firewall appliances reduce exposure to security vulnerabilities associated with a general-purpose underlying operating system

D. Operating system firewalls are highly configured

ANSWER: C

Explanation:

Hardware firewall appliances reduce exposure to security vulnerabilities associated with a general-purpose underlying operating system is correct because an appliance-based firewall is purpose-built for its security function and is normally deployed with a hardened, tightly controlled operating environment. Its software image, enabled services, administrative interfaces, and installed applications are limited to what is needed to inspect and enforce network traffic. This reduced attack surface gives an attacker fewer potential paths to compromise the device than a firewall installed on a general-purpose commercial operating system, which commonly includes broader functionality and supporting components.

Appliance firewalls also provide a more controlled platform for secure configuration, patch management, authenticated administration, and segregation of the firewall function from ordinary server or workstation workloads. The security benefit is not that appliances are invulnerable: they still require vendor updates, secure administration, and monitoring. Rather, their dedicated and hardened design reduces the exposure created by an underlying general-purpose operating system and unnecessary services. NIST's firewall guidance emphasizes using secure, hardened configurations and minimizing exposed services as key firewall protections. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and CISA guidance on securing network infrastructure devices.

QUESTION NO: 14

James, a research scholar, received an email informing that someone is trying to access his Google account from an unknown device. When he opened his email message, it looked like a standard Google notification instructing him to click the link below to take further steps. This link was redirected to a malicious webpage where he was tricked to provide Google account credentials. James observed that the URL began with www.translate.google.com giving a legitimate appearance.

In the above scenario, identify the type of attack being performed on James' email account?

A. SMiShing

B. Dumpster diving

C. Phishing

D. Vishing

ANSWER: C

Explanation:

Phishing is the correct classification because the attacker uses a deceptive email that impersonates a trusted service, Google, and creates urgency by claiming that an unknown device is accessing James's account. The message directs James to follow a link for purported account-protection steps, but the destination is an attacker-controlled page designed to capture his Google credentials. This is the defining objective of phishing: persuading a target to disclose sensitive information, such as usernames, passwords, or authentication data, by presenting a fraudulent communication or website as legitimate.

The use of a URL beginning with `www.translate.google.com` is a credibility tactic intended to make the link appear associated with Google. Attackers can abuse URL structures, redirection mechanisms, or trusted services to obscure the real destination and reduce a recipient's suspicion. The security-relevant behavior is therefore the fraudulent email and credential-harvesting webpage, not merely the visual appearance of the URL. Users should independently navigate to their account settings rather than use unsolicited email links, and should inspect the final destination and domain before entering credentials. Guidance on recognizing and reporting these attacks is available from Google Account Help and the CISA phishing-awareness guidance.

QUESTION NO: 15

Which vulnerability assessment phase describes the scope of the assessment, identifies and ranks the critical assets, and creates proper information protection procedures such as effective planning, scheduling, coordination, and logistics?

A. Threat-Assessment Phase

B. Pre-Assessment Phase

C. Assessment Phase

D. Post-Assessment Phase

ANSWER: B

Explanation:

The **Pre-Assessment Phase** is correct because it establishes the engagement's foundation before vulnerability testing activities begin. During this phase, the assessment team and stakeholders define the authorized scope, including the systems, networks, applications, locations, time windows, and testing constraints involved. They identify business-critical assets and prioritize them according to their value, sensitivity, operational importance, and potential impact if compromised. This preparation enables the team to focus assessment resources on the areas that present the greatest organizational risk.

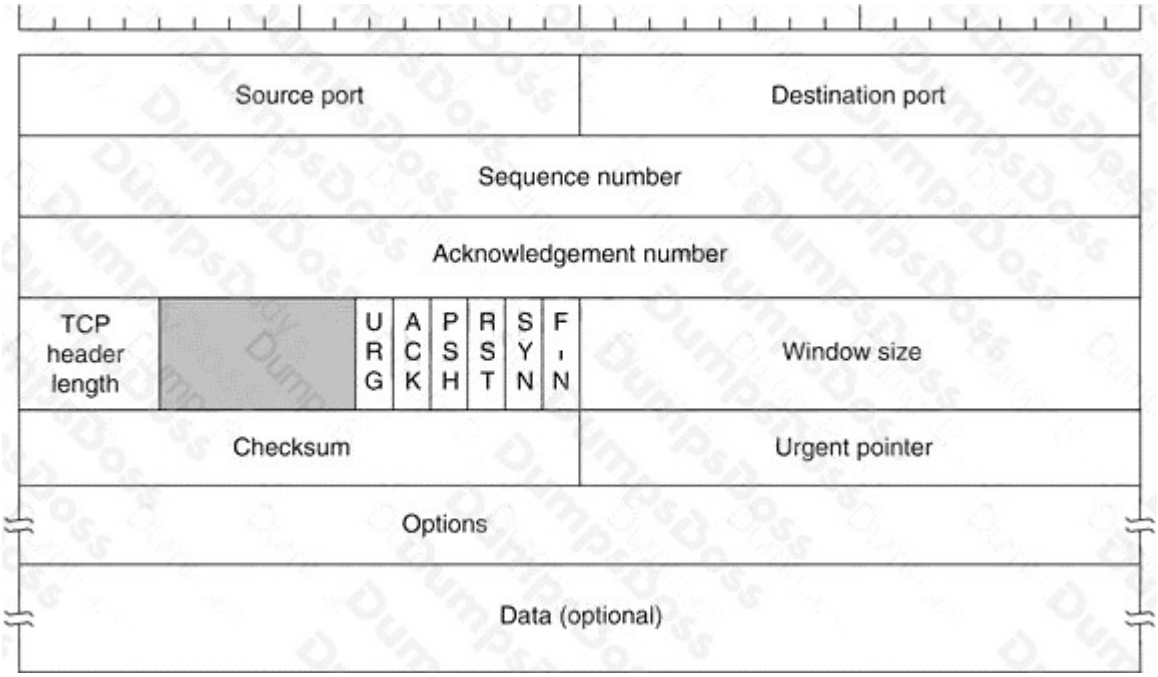
Pre-assessment work also addresses the operational safeguards needed to perform testing safely and efficiently. These include planning the work, scheduling activities to minimize business disruption, coordinating with system owners and relevant operational teams, defining communications and escalation contacts, and arranging the logistics and handling requirements for assessment information. Clearly documenting these elements ensures that the vulnerability assessment is authorized, controlled, and aligned with organizational objectives. This approach is consistent with the planning phase described in NIST SP 800-115, Technical Guide to Information Security Testing and Assessment, which calls for defining assessment scope, rules, logistics, and communication requirements before testing. EC-Council's ECSA program likewise emphasizes structured penetration-testing and assessment methodology: ECSA certification overview.

QUESTION NO: 16

Transmission control protocol accepts data from a data stream, divides it into chunks, and adds a TCP header creating a TCP segment. The TCP header is the first 24 bytes of a TCP segment that contains the parameters and state of an end-to-end TCP socket. It is used to track the state of communication between two TCP endpoints.

For a connection to be established or initialized, the two hosts must synchronize. The synchronization requires each side to send its own initial sequence number and to receive a confirmation of exchange in an acknowledgment (ACK) from the other side

The below diagram shows the TCP Header format:



A. 16 bits

B. 32 bits

C. 8 bits

D. 24 bits

ANSWER: B

Explanation:

32 bits is correct because TCP uses a 32-bit Sequence Number field and a 32-bit Acknowledgment Number field in its fixed header. During the TCP three-way handshake, each endpoint selects and transmits an Initial Sequence Number (ISN). The peer acknowledges that value by placing the next expected sequence number in its Acknowledgment Number field, allowing both endpoints to synchronize the byte sequence spaces used for reliable, ordered delivery.

The 32-bit sequence space is fundamental to TCP operation: sequence numbers identify the position of data bytes in a connection's stream, and acknowledgments report the next byte expected. Because the field is 32 bits wide, sequence values range across a wrapping 32-bit space, with TCP's sequence-number rules handling progression and wraparound during a connection. This is why a TCP header diagram depicts both the Sequence Number and Acknowledgment Number as fields spanning an entire 32-bit row. The current TCP specification defines these fields explicitly as 32-bit values and describes their role in connection synchronization and acknowledgment processing. See RFC 9293: Transmission Control Protocol and the TCP header format definition in RFC 9293.

QUESTION NO: 17

Firewall is an IP packet filter that enforces the filtering and security policies to the flowing network traffic. Using firewalls in IPv6 is still the best way of protection from low level attacks at the network and transport layers.

Which one of the following cannot handle routing protocols properly?

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

B. “Internet-firewall-router-net architecture”

C. “Internet-firewall/router(edge device)-net architecture”

D. “Internet-firewall -net architecture”

ANSWER: B

Explanation:

“Internet-firewall-router-net architecture” is correct because placing the firewall between the Internet and the routing device makes the firewall responsible for passing traffic required by dynamic routing protocols before it reaches the router that must process it. Routing protocols can use IP protocol numbers rather than TCP or UDP ports, multicast or link-local addresses, and protocol-specific packet formats. A conventional packet-filtering firewall may not correctly inspect, authenticate, or safely permit the routing exchanges required for the router to establish and maintain external routing adjacencies. This placement can therefore interfere with route updates and routing convergence, particularly when policy rules are restrictive or lack protocol-aware support.

A design that puts the Internet-facing router ahead of the firewall allows the router to participate directly in the necessary routing exchanges while the firewall protects the internal network behind it. IPv6 deployments also require filtering policies that account for essential control-plane traffic, including ICMPv6, without indiscriminately allowing untrusted traffic. The IETF’s guidance on IPv6 firewalling discusses the filtering considerations for IPv6 control and transport traffic in RFC 4890. For broader router-security and routing-protocol protection guidance, see CISA’s BGP security guidance.

QUESTION NO: 18

Traffic on which port is unusual for both the TCP and UDP ports?

A. Port 81

B. Port 443

C. Port 0

D. Port 21

ANSWER: C

Explanation:

Port 0 is the correct answer because it is reserved rather than assigned to an ordinary network service. In normal TCP and UDP communications, endpoints use valid nonzero port numbers to identify the application or service associated with a connection or datagram. Consequently, packets observed with port 0—particularly as a destination port—are anomalous and should be investigated during traffic analysis or a penetration test. Such traffic can result from malformed packets, scanning activity, packet crafting, implementation errors, or attempts to evade simplistic monitoring rules. The Internet Assigned Numbers Authority lists port 0 as reserved in both the TCP and UDP service-name and port-number registries, confirming that it is not a standard application-service port. TCP also defines port values in the range 0 through 65535, while reserving port 0; operationally, normal services bind to nonzero ports. Although UDP permits a zero source-port field to indicate that a sender does not expect replies, port 0 remains highly unusual in ordinary observed service traffic and is especially suspicious when used as a destination. See the IANA Service Name and Transport Protocol Port Number Registry and RFC 768.

QUESTION NO: 19

James is a security consultant at Big Frog Software Pvt Ltd. He is an expert in Footprinting and Social engineering tasks. His team lead tasked him to find details about the target through passive reconnaissance. James used websites to check the link popularity of the client’s domain name. What information does the link popularity provide?

A. Information about the network resources

B. Information about visitors, their geolocations, etc.

C. Information about the server and its infrastructure

D. Information about the partner of the organization

ANSWER: D

Explanation:

Information about the partner of the organization is correct because link-popularity analysis examines external websites that link to a target domain. Those inbound links can reveal business relationships that are useful during passive reconnaissance, including partners, affiliates, suppliers, customers, resellers, sponsoring organizations, and organizations sharing services or projects with the target. For a penetration tester, these relationships help build an accurate external profile of the organization without directly probing its systems. A linked partner site may also expose public contact details, technology references, trust relationships, or other contextual information relevant to later, authorized assessment activities. Search-engine link analysis and backlink-analysis services are commonly used to identify referring domains and evaluate the relationship signals represented by links. Google describes links as a key way its systems discover and understand pages: Google Search Central: How Search Works. The concept of analyzing inbound links and referring domains is also documented by Ahrefs: Ahrefs: What Are Backlinks?. Thus, the principal reconnaissance value of link popularity in this context is identifying organizations connected to the target.

QUESTION NO: 20

Which of the following equipment could a pen tester use to perform shoulder surfing?

A. Binoculars

B. Painted ultraviolet material

C. Microphone

D. All the above

ANSWER: A

Explanation:

Binoculars are appropriate equipment for performing shoulder surfing because they allow an observer to view a target's screen, keyboard, documents, badge details, or PIN-entry activity from farther away than would be possible with the naked eye. In an authorized physical-security assessment, a penetration tester may use binoculars to evaluate whether workstation placement, exposed windows, monitor positioning, screen privacy controls, or employee behavior allows sensitive information to be observed from public or otherwise accessible locations. The objective is to demonstrate the realistic exposure created when confidential information can be visually captured without directly accessing a system or handling the information. Shoulder surfing is a form of visual eavesdropping and is particularly relevant where users enter credentials, access confidential records, or work in spaces visible to visitors or people outside the building. Findings from such testing can support recommendations such as repositioning displays, applying privacy filters, limiting lines of sight, and improving user awareness. NIST recognizes observation attacks as a concern during authentication, including the risk of an attacker observing a claimant entering authentication information; see NIST SP 800-63B. Additional physical-security guidance is available from CISA Physical Security.