DUMPSBOSS.

EC-Council Certified Security Analyst (ECSA)

ECCouncil EC0-479

Version Demo

Total Demo Questions: 26

Total Premium Questions: 261

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	93
Topic 2, Penetration Testing Scoping and Engagement Methodology	6
Topic 3, Open Source Intelligence (OSINT)	16
Topic 4, Social Engineering Penetration Testing	8
Topic 5, Network Penetration Testing	67
Topic 6, Web Application Penetration Testing	17
Topic 7, Wireless Penetration Testing	4
Topic 8, Report Writing and Post Testing Actions	27
Topic 9, Mix Questions	23
Total	261

QUESTION NO: 1

A web application security analyst is reviewing HTTP response headers for an Internet-facing customer portal. Which headers can provide protection against protocol downgrade attacks and clickjacking attacks? (Select 2)

A. Strict-Transport-Security

B. X-Frame-Options

C. Server

D. Content-Length

E. Accept-Ranges

ANSWER: A B

Explanation:

Strict-Transport-Security and **X-Frame-Options** are correct. The HTTP Strict Transport Security header instructs supporting browsers to access the site only over HTTPS for the specified duration. This reduces the opportunity for an attacker to downgrade a user from HTTPS to an unencrypted HTTP connection after the browser has received the policy.

The X-Frame-Options header helps protect against clickjacking by controlling whether the browser may render the page inside a frame or iframe. A value such as `DENY` prevents framing entirely, while `SAMEORIGIN` permits framing only by pages from the same origin. Modern applications can also use the Content-Security-Policy `frame-ancestors` directive for more flexible framing restrictions. See MDN Strict-Transport-Security documentation and MDN X-Frame-Options documentation.

QUESTION NO: 2

You are reviewing Windows Security event logs following a suspected brute-force attempt against a file server. Which Event IDs are relevant for identifying failed and successful interactive or network logon attempts? (Select 2)

A. 4624

B. 4625

C. 4634

D. 1102

ANSWER: A B

Explanation:

Event ID **4625** records a failed logon attempt, while Event ID **4624** records a successful logon. These events can provide details such as the account name, logon type, source workstation or network address where available, authentication package, and failure reason. Reviewing them together can identify repeated failures followed by a successful authentication event, which may indicate password guessing, credential stuffing, or use of a compromised account.

Investigators should correlate these records with account-management events, VPN logs, firewall records, endpoint telemetry, and the expected logon behavior of the account. Microsoft documents successful logon auditing in Event 4624 and failed logon auditing in Event 4625.

QUESTION NO: 3

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Circuit-level proxy firewall

B. Packet filtering firewall

C. Application-level proxy firewall

D. Stateful firewall

ANSWER: D

Explanation:

Stateful firewall is correct because it maintains a state table containing active network sessions and the details needed to associate packets with those sessions, such as source and destination addresses, ports, protocol, and TCP connection state. When an internal host initiates an outbound connection, the firewall records that flow as established. It can then permit only the return traffic that matches the tracked session, while continuing to block unsolicited inbound connection attempts that do not correspond to an internally initiated flow. This directly implements the stated policy: inbound traffic is allowed only when it is a valid response within an existing connection created from inside the protected network. Stateful inspection is therefore a core control for enforcing outbound-initiated connectivity and limiting exposure to externally initiated sessions. NIST describes stateful inspection firewalls as examining traffic in the context of established connections and using state information to make filtering decisions. See NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy and Cisco's overview of firewall technologies.

QUESTION NO: 4

Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

A. Fuzzing

B. Tailgating

C. Man trap attack

D. Backtrapping

ANSWER: B

Explanation:

Tailgating is correct because the technician obtains entry to a restricted area by closely following authorized employees through an access-controlled entrance without using his own authorized credential. This is a common physical penetration-testing technique and physical social-engineering scenario: an attacker takes advantage of an employee's legitimate access and willingness to permit someone who appears to belong in the environment to enter behind them. Dressing as an electrician reinforces a credible pretext, helping the technician appear legitimate once inside, but the defining access-bypass action is following authorized personnel through the restricted entrance.

Effective physical security controls require personnel to prevent uncredentialed individuals from entering on their access event, even where the individual presents a plausible work-related reason for access. Organizations should reinforce this through awareness training, visitor identity verification and escort procedures, badge checks, and access-control designs that allow only one individual per authorization cycle. NIST identifies physical access authorization and enforcement as key elements of facility security controls in NIST SP 800-53 Rev. 5. Guidance on recognizing social-engineering techniques and validating unexpected personnel is also available from CISA.

QUESTION NO: 5

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” is correct because starting an operating system causes normal background activity, including creation of logs, caches, swap/page files, temporary files, and metadata updates. Those writes can reuse disk space that formerly held deleted data, thereby overwriting or altering forensic artefacts. This is why forensic best practice is to avoid booting or otherwise using a suspect system’s original storage media and instead acquire a forensic image using controlled procedures.

“Secure delete programs work by completely overwriting the file in one go” reflects the central purpose of secure deletion: rather than merely removing a filesystem reference, the tool writes data over the file’s allocated storage so that the prior contents cannot be recovered through ordinary undelete methods. The appropriate sanitization technique depends on the storage technology and threat model; modern guidance particularly distinguishes conventional magnetic media from SSDs and other flash devices. NIST describes overwrite as a media-sanitization technique and provides detailed criteria for selecting and verifying sanitization methods in NIST SP 800-88 Rev. 1. Guidance on preserving digital evidence during incident handling is also available from CISA.

QUESTION NO: 6

Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

A. Only an HTTPS session can be hijacked

B. Only DNS traffic can be hijacked

C. Only FTP traffic can be hijacked

D. HTTP protocol does not maintain session

ANSWER: D

Explanation:

HTTP protocol does not maintain session

HTTP is fundamentally a stateless request-response protocol: each request is handled independently, and the protocol itself does not create or retain a persistent user session that can be taken over. Therefore, when the question refers specifically to an HTTP-protocol session, there is no native protocol-level session for Ettercap to hijack. This aligns with HTTP’s defined stateless semantics in RFC 9110, which explains that requests are self-contained and that HTTP does not inherently retain application state between requests.

In real web applications, developers commonly add state above HTTP through mechanisms such as cookies carrying session identifiers, URL parameters, or authorization tokens. If such an application-managed token were transmitted insecurely and an attacker were positioned to intercept or modify traffic, session-token theft could become possible. That is distinct from HTTP itself maintaining a session. The question’s intended distinction is between the stateless HTTP transport semantics and a stateful application session implemented on top of HTTP. See RFC 9110: HTTP Semantics and OWASP’s Session Management Cheat Sheet.

QUESTION NO: 7

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 communications normally use UDP port 161 and UDP port 162. UDP 161 is the standard SNMP agent port: an SNMP manager sends polling requests, such as GET, GETNEXT, GETBULK, and SET requests, to the managed device's SNMP agent on this port. Opening UDP 161 along the appropriate interoffice firewall path allows the central manager to query routers, switches, servers, and other monitored devices at remote sites. UDP 162 is the standard notification-receiver port. It is used by the SNMP manager, trap receiver, or monitoring platform to accept unsolicited SNMP Trap and Inform notifications sent by agents. Therefore, a deployment that needs both routine polling and event-driven alerting must permit UDP 161 to the remote agents and UDP 162 to the management system or designated trap receiver. Firewall rules should be restricted to the known manager, agent, and trap-receiver IP addresses rather than exposed broadly. SNMPv3 should also be used where available because it supports authentication and privacy protections for management traffic. The Internet Assigned Numbers Authority lists snmp on UDP 161 and snmptrap on UDP 162 in its service-name registry. Cisco's SNMP configuration documentation likewise identifies UDP 161 for SNMP requests and UDP 162 for traps and informs. See IANA Service Name and Port Number Registry and Cisco SNMP Configuration Guide.

QUESTION NO: 8

A development team is remediating a SQL injection flaw in a web application. Which of the following controls are appropriate? (Select 3)

A. Use prepared statements with parameterized queries

B. Validate input against an allow-list of expected values

C. Run the application database account with administrative privileges

D. Grant the database account only required permissions

E. Rely only on client-side JavaScript validation

ANSWER: A B D

Explanation:

Prepared statements with parameterized queries, allow-list input validation, and a database account with only required privileges are correct. Parameterized queries keep SQL code separate from data values, preventing user input from changing the intended query structure. Allow-list validation restricts input to expected formats, such as numeric identifiers or approved values, and provides an additional layer of protection.

The database account used by the application should have only the permissions necessary for its legitimate functions. Least privilege limits the impact if an application flaw, stolen credential, or database compromise occurs. Escaping input alone is not a reliable primary defense because correct escaping depends on the database engine and the context in which the value is used. OWASP recommends prepared statements as a primary SQL injection defense in its SQL Injection Prevention Cheat Sheet. MITRE also classifies improper neutralization of SQL commands as CWE-89.

QUESTION NO: 9

http://www.thetargetsite.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

A. Execute a buffer flow in the C: drive of the web server

B. Insert a Trojan horse into the C: drive of the web server

C. Directory listing of the C:\windows\system32 folder on the web server

D. Directory listing of C: drive on the web server

ANSWER: D

Explanation:

Directory listing of C: drive on the web server is correct. This question refers to the historical IIS Unicode directory-traversal vulnerability, commonly exploited with specially encoded path separators such as the overlong Unicode form of "/". On vulnerable IIS versions, canonicalization can occur incorrectly: IIS fails to normalize the encoded traversal sequence before applying access restrictions. A crafted request can therefore move outside the published web root and reach executable utilities such as `cmd.exe`. When the URL invokes the command interpreter with a command equivalent to `dir c:\`, the server executes that command in the security context of the web service and returns its output in the HTTP response. The resulting content is a directory listing of the system's C: drive, subject to the permissions of the IIS process account. This vulnerability was especially serious because directory traversal could be combined with command execution to disclose files and potentially run arbitrary commands remotely. Microsoft documented the issue as the IIS "Web Server File Request Parsing" vulnerability and provided patches to correct the path-parsing behavior. See Microsoft Security Bulletin MS00-078 and the associated CVE-2000-0884 record.

QUESTION NO: 10

One technique for hiding information is to change the file extension from the correct one to one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

A. the File Allocation Table

B. the file header

C. the file footer

D. the sector map

ANSWER: B

Explanation:

The file header is the correct item to examine because it typically contains a file signature, commonly called a "magic number," that identifies the file's actual format independently of its filename extension. An extension is only a naming convention used by operating systems and applications to associate a file with a program; changing `.jpg` to `.doc` does not ordinarily alter the underlying bytes that define the content format. For example, a JPEG image conventionally begins with the byte sequence `FF D8 FF`, while legacy Microsoft Compound File Binary Format documents commonly begin with `D0 CF 11 E0 A1 B1 1A E1`. A forensic investigator can inspect the first bytes of a suspicious file with a hex editor or use file-identification tooling to compare its header signature with known format signatures. This validation helps identify disguised files, detect mismatches between claimed and actual types, and guide the appropriate parser or further forensic examination. The National Institute of Standards and Technology's file-signature guidance discusses using binary signatures for format identification, and the JPEG specification defines the JPEG start-of-image marker. See NIST File Signatures and ITU-T JPEG specification.

QUESTION NO: 11

You are collecting disk evidence from a suspected compromised server. Which of the following practices help preserve the integrity and admissibility of the evidence? (Select 2)

A. Use a hardware or software write blocker during acquisition

B. Boot the suspect system from its normal operating system

C. Calculate and record a cryptographic hash of the acquired image

D. Store the original drive in a shared work area for review

ANSWER: A C

Explanation:

Creating a forensic image using a write blocker and calculating a cryptographic hash value are correct. A write blocker helps prevent the evidence-acquisition workstation from modifying the original storage media during collection. This is important because even minor writes can alter timestamps, metadata, unallocated space, or recoverable content.

A cryptographic hash calculated before and after acquisition provides a means to demonstrate that the forensic image has remained unchanged. Investigators should document the hash algorithm and values, the date and time of acquisition, the person performing the collection, the source device, and each transfer of custody. Together, controlled acquisition, hashing, and a complete chain of custody support evidence integrity. NIST discusses media acquisition and cryptographic hashing in NIST SP 800-86, and its guidance for integrating forensic techniques is available in NIST SP 800-101 Rev. 1.

QUESTION NO: 12

Which of the following should a computer forensics lab used for investigations have?

A. isolation

B. restricted access

C. open access

D. an entry log

ANSWER: B

Explanation:

restricted access is correct because a forensic laboratory must protect the integrity, confidentiality, and evidentiary value of the devices and data being examined. Access should be limited to authorized personnel who have a legitimate investigative role and understand the lab's handling procedures. This physical control helps prevent accidental alteration, intentional tampering, unauthorized disclosure of sensitive information, and disputes about who could have interacted with evidence. Restricting access also supports a defensible chain of custody: the organization can demonstrate that evidence remained under controlled conditions from acquisition through examination, storage, and reporting. In practice, restricted access is implemented through measures such as locked rooms, access-control systems, designated authorized staff, and documented procedures for visitors or maintenance personnel. These safeguards complement technical forensic practices, including use of write blockers, forensic imaging, hashing, and secure evidence storage. NIST explains that sound forensic processes must preserve data integrity and support documentation of handling activities throughout an investigation. See NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. Guidance on maintaining evidence integrity and secure handling environments is also available from the Scientific Working Group on Digital Evidence (SWGDE).

QUESTION NO: 13

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 or more passes

ANSWER: C D

Explanation:

“While booting, the machine may create temporary files that can delete evidence” is correct because ordinary deletion usually removes the file-system reference to data and makes its storage space eligible for reuse. Starting an operating system can cause routine writes such as logs, paging or swap activity, temporary files, indexing data, updates, and application startup artifacts. If these writes are allocated to formerly unallocated clusters, they can overwrite portions of deleted-file content and reduce the amount of evidence that can be recovered. Consequently, forensic best practice is to avoid booting or otherwise writing to the suspect drive and instead acquire a forensic image using controlled procedures.

“Secure delete programs work by completely overwriting the file in one or more passes” is also correct. Secure-deletion tools are intended to overwrite accessible file content before or while removing its directory entry, reducing the chance that conventional recovery tools can reconstruct the original data. The precise effectiveness depends on the file system, storage medium, snapshots, journaling, and device behavior; modern SSDs in particular require media-appropriate sanitization methods because logical overwrites may not reach every physical location. NIST describes overwrite and other sanitization techniques in NIST SP 800-88 Rev. 1, while the importance of preserving evidence through controlled acquisition is addressed in the NIST digital forensics resources.

QUESTION NO: 14

A company uses public key infrastructure to issue certificates to employees and servers. Which of the following mechanisms can be used by a relying party to determine whether a certificate has been revoked before its expiration date? (Select 2)

A. Certificate Revocation List (CRL)

B. Online Certificate Status Protocol (OCSP)

C. Domain Name System zone transfer

D. Certificate expiration date

ANSWER: A B

Explanation:

A **Certificate Revocation List (CRL)** and the **Online Certificate Status Protocol (OCSP)** are correct. A CRL is a signed list published by a certification authority that identifies certificates that have been revoked. A relying party can retrieve the list and determine whether the serial number of a presented certificate appears on it.

OCSP provides a status-query mechanism through which a relying party asks an OCSP responder whether a specific certificate is good, revoked, or unknown. Both mechanisms support revocation checking when a private key is compromised, a certificate was issued in error, or the certificate holder is no longer authorized. A certificate's expiration date alone does not provide current revocation status. CRLs are defined in RFC 5280, and OCSP is specified in RFC 6960.

QUESTION NO: 15

You are preparing the final report for an authorized penetration test. Which information should be included to enable management and technical staff to understand and remediate the identified risks? (Select 3)

A. An executive summary

B. Technical finding details

C. Remediation recommendations

D. Credentials collected during the assessment in the executive summary

E. Unfiltered packet captures for every network segment

ANSWER: A B C

Explanation:

An executive summary, **technical finding details**, and **remediation recommendations** are correct. An executive summary provides management with a clear overview of the assessment scope, major risks, business impact, and overall security posture. Technical finding details give system owners enough information to identify affected assets, understand evidence, reproduce the condition where appropriate, and assess severity.

Remediation recommendations translate findings into actionable corrective measures, such as patching, configuration changes, access-control improvements, or architectural changes. A complete report should also accurately document scope, methodology, limitations, and evidence while protecting sensitive assessment data. NIST describes reporting and remediation activities within technical security assessments in NIST SP 800-115.

QUESTION NO: 16

Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security. Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

A. Simple Network Management Protocol

B. Broadcast System Protocol

C. Cisco Discovery Protocol

D. Border Gateway Protocol

ANSWER: C

Explanation:

Cisco Discovery Protocol is correct because it is a Cisco-proprietary Layer 2 discovery protocol that devices use to advertise identifying and capability information to directly connected Cisco devices. CDP advertisements can disclose details useful to a network assessor or attacker performing reconnaissance, including the device platform/model, Cisco IOS software version, interface and port information, IP addressing details, native VLAN information, and supported capabilities. This makes it possible to profile network infrastructure quickly even when management-plane access is otherwise well protected.

On Cisco IOS, CDP can be disabled globally with `no cdp run`. Where discovery is required in limited portions of the environment, it can instead be disabled selectively on exposed interfaces with `no cdp enable` under the relevant interface configuration. Disabling CDP reduces unnecessary information exposure and is consistent with hardening guidance to disable services that are not operationally required. Administrators should confirm whether any inventory, topology-management, or voice deployments depend on CDP before making the change. Cisco documents CDP operation and configuration in its CDP Configuration Guide, including the global and per-interface controls. Cisco's router hardening guidance also emphasizes minimizing enabled services: Cisco Guide to Harden Cisco IOS Devices.

QUESTION NO: 17

A web application uses cookies to maintain authenticated user sessions. Which cookie attributes should be used to reduce the risk of session theft and cross-site request attacks? (Select 3)

A. Secure

B. HttpOnly

C. SameSite

D. Server

E. Connection

ANSWER: A B C

Explanation:

Secure, **HttpOnly**, and **SameSite** are correct. The Secure attribute instructs browsers to send the cookie only over HTTPS connections, reducing exposure of the session identifier over unencrypted HTTP. The HttpOnly attribute prevents client-side JavaScript from directly reading the cookie, which reduces the impact of many cross-site scripting attacks that attempt to steal session cookies.

The SameSite attribute restricts when a browser includes a cookie in cross-site requests. Appropriate SameSite settings help reduce cross-site request forgery exposure by preventing a victim's browser from automatically sending session cookies in many cross-origin request contexts. These controls should be used together with HTTPS, strong session identifier generation, session expiration, and server-side CSRF defenses where applicable. OWASP provides guidance at the OWASP Session Management Cheat Sheet.

QUESTION NO: 18

You are running through a series of tests on your network to check for any security vulnerabilities. After normal working hours, you initiate a DoS attack against your external firewall. The firewall quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A. The firewall failed-open

B. The firewall failed-bypass

C. The firewall failed-closed

D. The firewall ACL has been purged

ANSWER: A

Explanation:

The firewall failed-open. A fail-open condition means that, when a security control encounters a fault, overload, or availability failure, it defaults to allowing traffic rather than enforcing its normal deny rules. In this scenario, the denial-of-service attack causes the external firewall to freeze and become unusable; the subsequently successful inbound FTP connection demonstrates that the firewall is no longer applying the policy that blocks FTP. The device or its traffic path has therefore adopted an allow-by-default behavior during the failure, exposing the internal network to connections that would ordinarily be denied.

Fail-open behavior prioritizes network availability, but it creates a significant security risk because policy enforcement can disappear precisely while the device is under stress or attack. Firewall resilience testing should verify that failure modes preserve the intended security boundary, with controls configured and architected to fail closed where practical. NIST discusses firewall policy enforcement and the importance of default-deny handling in its firewall guidance: NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy. The availability and security trade-off of fail-open versus fail-closed designs is also described by the OWASP Fail Safe guidance.

QUESTION NO: 19

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 account

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 D E

Explanation:

Email-related logging and message records are valuable forensic sources because they establish who communicated, what was communicated, and when it occurred. The *user account that was used to send the account* provides sender attribution and supports correlation with account-authentication, webmail, or mail-server activity. A *unique message identifier*, commonly represented by the Message-ID header, allows investigators to correlate copies of the same message across mail clients, gateways, archives, and recipient systems. The *contents of the e-mail message* can preserve the communication's body and relevant header information, supplying evidence of intent, instructions, social-engineering content, or data disclosure. The *date and time the message was sent* is essential for building an incident timeline and correlating the email with endpoint, proxy, authentication, and network events. Investigators should preserve the original message and associated records in a manner that maintains integrity, including relevant timestamps, headers, and account information. RFC 5322 defines the Internet message format and the Message-ID field used to identify messages: RFC 5322. NIST also describes preserving and analyzing email and other log evidence during incident handling: NIST SP 800-86.

QUESTION NO: 20

Lance wants to place a honeypot on his network. Which of the following would be your recommendations?

A. Use a system that has a dynamic addressing on the network

B. Use a system that is not directlyinteracing with the router

C. Use it on a system in an external DMZ in front of the firewall

D. It doesnâ€Ÿt matter as all replies are faked

ANSWER: C

Explanation:

Use it on a system in an external DMZ in front of the firewall is the appropriate recommendation because a honeypot should be deliberately exposed to unsolicited probing and attack activity while remaining segregated from production systems. An externally accessible, isolated DMZ placement makes the decoy visible to Internet-based attackers and allows defenders to collect useful evidence, such as connection attempts, exploit payloads, commands, and indicators of compromise. At the same time, network controls around the DMZ can tightly restrict inbound and, especially, outbound communications, reducing the risk that a compromised honeypot can be used as a pivot point into the internal environment or as a platform for attacks against others. Logging and alerting should be configured so interactions with the honeypot are monitored centrally and investigated promptly. NIST identifies honeypots as a form of specialized intrusion-detection technology and stresses that their use requires careful deployment and monitoring because they may be compromised. See NIST's Guide to Intrusion Detection and Prevention Systems and its full publication PDF for deployment and operational considerations.

QUESTION NO: 21

George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used. What IDS feature must George implement to meet this requirement?

A. Pattern matching

B. Statistical-based anomaly detection

C. Real-time anomaly detection

D. Signature-based anomaly detection

ANSWER: C

Explanation:

Real-time anomaly detection is the required feature because a time-based induction approach establishes an expected behavioral baseline from activity observed over time, then continually evaluates current events against that learned baseline. The IDS can identify activity whose timing, frequency, volume, protocol use, or sequence materially departs from the profile of normal operations. The essential operational characteristic is that this comparison and alerting occur as events are observed, enabling analysts to respond while suspicious behavior is underway rather than only after offline review. This is particularly appropriate when an audit requirement calls for a time-oriented behavioral detection capability: the system must both learn from historical time-based patterns and apply that model to live network or host activity. NIST describes anomaly-based detection as identifying significant deviations from established normal profiles and notes that intrusion-detection technologies may provide near-real-time analysis and alerting. See NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems and the NIST Cybersecurity Framework for guidance on continuous security monitoring and detection capabilities.

QUESTION NO: 22

What does mactime, an essential part of the coroner"s toolkit do?

A. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps

B. It can recover deleted file space and search it for datA. However, it does not allow the investigator t preview them

C. The tools scans for i-node information, which is used by other tools in the tool kit

D. It is tool specific to the MAC OS and forms a core component of the toolkit

Answer: A

Explanation:

A. However, it does not allow the investigator t preview them

B. It can recover deleted file space and search it for dat

C. The tools scans for i-node information, which is used by other tools in the tool kit

D. It is tool specific to the MAC OS and forms a core component of the toolkit

E. It processes body-file metadata and generates a chronological timeline using modification, access, and metadata-change timestamps.

ANSWER: E

Explanation:

`mactime` is a timeline-generation utility from The Sleuth Kit. It reads a body file containing filesystem metadata records and produces a chronologically ordered timeline based on MAC timestamps: modification time, access time, and metadata-change time. This lets an examiner correlate filesystem activity, identify periods of interest, and investigate the sequence in which files and directories were modified, accessed, or had their metadata changed. The resulting output can be constrained to a particular date range and is commonly used during forensic analysis to highlight activity surrounding an incident.

The key distinction is that `mactime` processes metadata records already collected into a body file; collection utilities such as `fls` can create such records from a filesystem image. Therefore, the accurate description is that it generates a MAC-time filesystem activity timeline from body-file data, rather than directly traversing a filesystem itself. The Sleuth Kit documentation describes `mactime` as creating an ASCII timeline from a body file, and its manual page documents the supported time fields and output behavior. See the The Sleuth Kit mactime manual and the fls manual.

QUESTION NO: 23

As a CHFI professional, which of the following is the most important to your professional reputation?

A. Your Certifications

B. The correct, successful management of each and every case

C. The free that you charge

D. The friendship of local law enforcement officers

ANSWER: B

Explanation:

The correct, successful management of each and every case is most important to a CHFI professional's reputation because a forensic practitioner is ultimately judged by the quality, integrity, and defensibility of casework. Successful management means applying a repeatable forensic process from evidence identification and preservation through acquisition, examination, analysis, documentation, and reporting. It also requires maintaining a complete chain of custody, protecting evidence from alteration, recording actions and findings accurately, and communicating conclusions that are technically supported and suitable for legal or organizational scrutiny. Consistent performance in these areas establishes that the examiner can be trusted with sensitive evidence and can produce findings that withstand review. EC-Council describes its CHFI program as preparing professionals to conduct digital forensic investigations using a systematic approach, reflecting the importance of reliable investigative execution in real cases. NIST likewise emphasizes preserving evidence integrity and documenting forensic activities so that results are reliable and reproducible. A professional reputation is therefore built case by case through competent, ethical handling and successful resolution of each investigation. See EC-Council CHFI and NIST SP 800-86.

QUESTION NO: 24

You are working as a Computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact law enforcement and provide them with the evidence that you have founD. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subjects computer. You inform the officer that you will not be able to comply with that request because doing so would:

A. Violate your contract

B. Cause network congestion

C. Make you an agent of law enforcement

D. Write information to the subjects hard drive

ANSWER: C

Explanation:

"Make you an agent of law enforcement" is correct because the investigator's proposed monitoring would no longer be solely a private, corporate investigative activity. The investigator has already discovered evidence during the course of a private investigation and may provide that existing evidence to police. However, after a law-enforcement officer specifically requests that the investigator deploy a network sniffer to monitor the subject, the investigator would be conducting the additional search at the government's direction. That relationship can make a nominally private actor a government agent for constitutional-search purposes.

Whether a private person is acting as a government agent generally turns on the degree of government knowledge, acquiescence, encouragement, or participation in the search, together with the private party's intent. A direct police request to perform continuing traffic interception is a significant form of government involvement. Consequently, the collection could be treated as government action and must be handled under the applicable constitutional, statutory, warrant, consent, and organizational-authority requirements. The private-search doctrine permits law enforcement to examine material already exposed through a genuinely private search, but it does not automatically authorize a new search initiated at law enforcement's request. See the Supreme Court's discussion of private searches in United States v. Jacobsen and the Department of Justice guidance on electronic surveillance at Title III Electronic Surveillance.

QUESTION NO: 25

You are performing passive reconnaissance for an authorized external assessment. Which of the following sources can provide useful information without directly probing the target organization's hosts? (Select 3)

A. Certificate Transparency logs

B. WHOIS registration records

C. TCP SYN port scanning

D. Public job postings

E. DNS AXFR requests to the authoritative server

ANSWER: A B D

Explanation:

Certificate Transparency logs, WHOIS records, and public job postings are correct passive reconnaissance sources. Certificate Transparency logs can reveal publicly issued TLS certificates and hostnames present in certificate subject alternative names. WHOIS records can provide registration and registrar information for domains where that data is available. Public job postings may disclose technologies, cloud platforms, security products, and operational roles used by the organization.

Passive reconnaissance relies on information obtained from public records, third-party services, and other sources that do not require direct interaction with the target systems. Port scanning and DNS zone-transfer requests directly communicate with target infrastructure and are active techniques. Certificate Transparency is defined in RFC 9162. ICANN provides information about registration data lookup services.

QUESTION NO: 26

You are responding to a suspected compromise of a critical server that is currently powered on. Which of the following sources of evidence are highly volatile and should generally be collected before shutting down the system? (Select 3)

A. Contents of system memory

B. Active network connections

C. Running processes

D. Archived backup tapes stored offsite

E. Printed network diagrams

ANSWER: A B C

Explanation:

Contents of system memory, **active network connections**, and **running processes** are correct. These sources can change rapidly or be lost entirely when a system is shut down. Memory may contain malware code, decrypted data, command history, credentials, encryption keys, and process artifacts that are unavailable in a static disk image. Active network connections can identify current remote sessions, command-and-control communication, and lateral movement activity. Running-process information helps identify executable paths, parent-child relationships, process identifiers, and suspicious programs active at the time of collection.

Volatile evidence should be collected using approved incident-response procedures while preserving documentation, timestamps, and chain of custody. NIST discusses volatile data acquisition and forensic collection considerations in NIST SP 800-86.