

## EC-COUNCIL.112-57.v2026-05-19.q25

|                                                                                                                                                                                       |                                               |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------|
| Exam Code:                                                                                                                                                                            | 112-57                                        |
| Exam Name:                                                                                                                                                                            | EC-Council Digital Forensics Essentials (DFE) |
| Certification Provider:                                                                                                                                                               | EC-COUNCIL                                    |
| Free Question Number:                                                                                                                                                                 | 25                                            |
| Version:                                                                                                                                                                              | v2026-05-19                                   |
| # of views:                                                                                                                                                                           | 109                                           |
| # of Questions views:                                                                                                                                                                 | 250                                           |
| <a href="https://www.freeqas.com/qa/EC-COUNCIL/112-57/EC-COUNCIL.112-57.v2026-05-19.q25.html">https://www.freeqas.com/qa/EC-COUNCIL/112-57/EC-COUNCIL.112-57.v2026-05-19.q25.html</a> |                                               |

### NEW QUESTION: 1

Benoy, a security professional at an organization, extracted Apache access log entries to view critical information about all the operations performed on a web server. The Apache access log extracted by Benoy is given below:

```
"10.10.10.10 - Jason [17/Aug/2019:00:12:34 +0300] "GET /images/content/bg_body_1.jpg HTTP/1.0" 500 1458"
```

Identify the HTTP status code in the Apache access log entry above that indicates the response was successful.

- A. +0300
- B. 500
- C. 1.0
- D. 2019

**Answer: B (LEAVE A REPLY)**

In the Apache Combined/Custom access log format, the value immediately after the quoted request (here, "GET ... HTTP/1.0") is the HTTP status code returned by the server. In the provided entry, that field is 500.

From a forensic analysis standpoint, recognizing field positions matters because investigators correlate client IPs, timestamps, requested resources, and server outcomes to reconstruct attack timelines and identify failed exploitation attempts or misconfigurations. It is important to note that successful HTTP responses are typically in the 2xx range, most commonly 200 (OK), while 3xx indicates redirects, 4xx indicates client-side errors (such as 404 Not Found), and 5xx indicates server-side failures. Specifically, 500 represents an Internal Server Error, meaning the server encountered an unexpected condition and could not fulfill the request successfully.

The other options are not HTTP status codes in this entry: +0300 is the timezone offset in the timestamp, 1.0 is the HTTP protocol version, and 2019 is part of the date. Therefore, the only HTTP status code present and the correct choice among the options is 500 (B), even though it reflects an error rather than success.

### NEW QUESTION: 2

Which of the following files belonging to the Extensible Storage Engine (ESE) stores the mail data in Microsoft Exchange Server?

- A. DataStore.edb
- B. Mail.MSMessageStore
- C. WLCalendarStore.edb
- D. Database.edb

**Answer: D (LEAVE A REPLY)**

Microsoft Exchange Server stores mailbox contents (emails, attachments, folders, and related messaging objects) inside an ESE (Extensible Storage Engine) database that uses the .edb file format. In Exchange terminology this is the Mailbox Database, and its primary persistent store is the database .edb file along with associated transaction logs that support write-ahead logging and recovery. From a forensic perspective, the

edb file is the central artifact because it contains the structured mailbox data that investigators analyze for message content, metadata (timestamps, sender/recipient fields, message IDs), and folder structure.

Among the options, Database.edb best matches the Exchange ESE mailbox database file that stores mail data.

The other options are either generic or associated with different Microsoft messaging components: Mail.

MSMessageStore relates to the Windows Mail/Modern Mail app storage model rather than Exchange Server's mailbox database, and WLCalendarStore.edb is commonly tied to Windows Live/Windows Essentials calendar or communications storage, not Exchange's server-side mailbox store. DataStore.edb is also used by other Windows services, but the recognized Exchange mailbox store is the .edb database file, making Database.edb (D) the correct answer.

### NEW QUESTION: 3

Which of the following titles of The Electronic Communications Privacy Act protects the privacy of the contents of files stored by service providers and records held about the subscriber by service providers, such as subscriber name, billing records, and IP addresses?

- A. Title II
- B. Title IV
- C. Title III
- D. Title I

**Answer: (SHOW ANSWER)**

Under the Electronic Communications Privacy Act (ECPA), Title II is commonly known as the Stored Communications Act (SCA). Digital forensics and e-discovery references treat the SCA as the key legal framework governing access to stored electronic communications and associated subscriber/account records held by service providers. The question specifically mentions (1) "contents of files stored by service providers" and (2) "records held about the subscriber ... such as subscriber name, billing records, and IP addresses." These map directly to the SCA's two broad categories: content (what a communication or stored file contains) and non-content records (subscriber identity, connection logs, billing information, IP assignment

/history, and related transactional metadata).

From an investigative perspective, Title II matters because it sets the legal process and restrictions for compelled disclosure—typically requiring different forms of legal process depending on whether the investigator seeks content versus subscriber/transactional records, and depending on factors like how the data is stored and retention timeframes. In contrast, Title I focuses on real-time interception (wiretap-style capture), and Title III addresses pen register/trap-and-trace style dialing/routing information rather than stored content.

Therefore, the correct title is Title II (Option A).

**NEW QUESTION: 4**

Below are the various steps involved in forensic readiness planning.

Keep an incident response team ready to review the incident and preserve the evidence.

Create a process for documenting the procedure.

Identify the potential evidence required for an incident.

Determine the sources of evidence.

Establish a legal advisory board to guide the investigation process.

Identify if the incident requires full or formal investigation.

Establish a policy for securely handling and storing the collected evidence.

Define a policy that determines the pathway to legally extract electronic evidence with minimal disruption.

Identify the correct sequence of steps involved in forensic readiness planning.

A. 3-->4-->8-->7-->6-->2-->5-->1

B. 2-->3-->1-->4-->6-->5-->7-->8

C. 3-->1-->4-->5-->8-->2-->6-->7

D. 1-->2-->3-->4-->5-->6-->7-->8

**Answer: A (LEAVE A REPLY)**

Forensic readiness planning focuses on ensuring an organization can legally, efficiently, and reliably collect usable digital evidence before an incident occurs. The planning sequence typically begins by defining what evidence would be needed to support likely incidents (3) and then mapping where that evidence resides across systems, services, logs,

endpoints, and network components (4). Once evidence needs and sources are known, readiness requires a legally compliant extraction pathway that minimizes business disruption and prevents evidence contamination (8). After defining extraction, an organization must formalize secure handling and storage policies (chain of custody, access control, retention, integrity protection) so collected evidence remains admissible and trustworthy (7).

With those foundations in place, the organization can define decision criteria for when an event becomes a formal investigation and triggers deeper forensic procedures (6). A structured documentation process is then set so actions taken during acquisition and analysis are repeatable and defensible (2). Governance is reinforced by establishing legal oversight/advisory support to ensure compliance with jurisdictional requirements and internal policy (5). Finally, the plan is operationalized by ensuring an incident response team is prepared to preserve evidence promptly when incidents occur (1).

Hence, 3#4#8#7#6#2#5#1 is the correct sequence.

### NEW QUESTION: 5

Which of the following tools helps a forensics investigator develop and test across multiple operating systems in a virtual machine for Mac and allows access to Microsoft Office for Windows?

- A. Riverbed Modeler
- B. Parallels Desktop 16
- C. Camtasia
- D. NetSim

**Answer: B (LEAVE A REPLY)**

A common requirement in macOS-focused forensic labs is the ability to run multiple operating systems on a single Mac for controlled testing, malware detonation in a sandbox, reproduction of user activity, and validation of artifacts across platforms. This is typically achieved through desktop virtualization, where a hypervisor hosts guest operating systems (such as Windows and various Linux distributions) inside virtual machines. Parallels Desktop 16 is a Mac virtualization solution built specifically to run Windows on macOS with strong integration features (such as shared clipboard, folder sharing, and "coherence" modes that allow Windows applications to appear alongside Mac applications). This capability aligns with the question's description: developing and testing across multiple OSs in VMs on a Mac and enabling use of Microsoft Office for Windows within that Windows guest environment.

The other tools do not fit. Riverbed Modeler and NetSim are primarily network modeling/simulation tools used for network design and training, not desktop virtualization. Camtasia is used for screen recording and video editing, which can support documentation but does not provide a VM environment. Therefore, the only option that directly provides cross-OS virtual machines on macOS and supports running Windows applications like Microsoft Office is Parallels Desktop 16 (B).

### NEW QUESTION: 6

Jack, a forensic investigator, was appointed to investigate a Windows-based security incident. In this process, he employed an Autopsy tool to recover the deleted files from unallocated space, which helps in gathering potential evidence.

Which of the following functions of Autopsy helped Jack recover the deleted files?

- A. Timeline analysis
- B. Multimedia
- C. Web artifacts
- D. Data carving

**Answer: D (LEAVE A REPLY)**

When a file is deleted on common file systems, the operating system typically removes the directory reference and marks the previously used clusters/blocks as unallocated, but the underlying file content may remain on disk until it is overwritten. Digital forensics procedures emphasize that recovering such deleted content often requires examining unallocated space rather than relying only on file system metadata. Autopsy's "Data Carving" function is specifically intended for this purpose: it scans unallocated space (and sometimes slack space) for file signatures (headers/footers and internal structure patterns) and reconstructs recoverable files even when the original filename, path, or metadata is missing.

This directly matches the scenario: Jack recovered deleted files from unallocated space, which is the classic use case for carving. The other options in Autopsy support different investigative goals. Timeline analysis correlates timestamps from multiple artifacts to reconstruct sequences of activity, but it does not itself reconstruct deleted file content from raw disk areas. Web artifacts focuses on browser history, downloads, cookies, and related traces. Multimedia helps categorize and analyze media files (e.g., images/videos), but it is not the primary mechanism for recovering deleted data from unallocated space. Therefore, the Autopsy function that enabled the recovery described is Data carving (D)

### NEW QUESTION: 7

Sam is working as a loan agent for a financial institution. He frequently receives a number of emails from clients providing their personal details for loan approval. As these emails contain sensitive data, Sam had set up a feature that directly downloads the emails on his device without storing a copy on the mail server. Which of the following protocols provides the above-discussed email features?

- A. SHA-1
- B. ICMP
- C. POP3
- D. SNMP

**Answer: C (LEAVE A REPLY)**

The scenario describes an email-retrieval configuration in which messages are downloaded to a client device and not retained on the server. This behavior aligns with POP3 (Post Office Protocol v3), a legacy but widely referenced mail access protocol that retrieves email from a server mailbox to a local client. In standard POP3 operation, the client authenticates to the mail server, issues retrieval commands (e.g., to list and download messages), and may then issue a delete command so that downloaded messages are removed from the server mailbox. Digital forensics references commonly contrast POP3 with IMAP: IMAP is designed for server-side mailbox synchronization and typically leaves mail stored on the server, whereas POP3 is oriented toward client-side storage and supports workflows where server copies are not preserved after download. The other options are unrelated to email retrieval: SHA-1 is a cryptographic hash function used for integrity checks, ICMP supports network diagnostics and control messaging, and SNMP is used for network device management and monitoring. From an investigative standpoint, POP3 usage can reduce server-resident evidence and shift evidentiary value to local artifacts (mail client databases, cache, OS traces, backups), which is consistent with the intent described in the question.

#### NEW QUESTION: 8

Which of the following measures is defined as the time to move read or write disc heads from one point to another on the disk?

- A. Delay time
- B. Seek time
- C. Access time
- D. Mean time

**Answer: B (LEAVE A REPLY)**

Seek time is the specific performance measure that describes how long a hard disk drive's actuator takes to move the read/write heads across the platters from the current track (cylinder) to the target track where the requested data resides. In traditional magnetic HDDs, the heads must be physically repositioned before any sector can be read or written, making seek time a core component of mechanical latency.

Digital forensics materials emphasize understanding this distinction because HDD mechanical behavior affects acquisition duration, the feasibility of repeated scans, and why imaging or carving operations can take longer on fragmented media. It also helps explain why solid-state drives (SSDs), which have no moving heads, do not have seek time in the same sense and therefore behave differently during large-scale reads.

The other choices are broader or unrelated: access time typically refers to the total time to retrieve data, commonly combining seek time + rotational latency + transfer time. Delay time is not the standard term for head movement in disk performance definitions. Mean time is incomplete as written and is usually part of reliability metrics like mean time between failures, not head positioning. Therefore, the correct measure for head movement time is seek time (C).

### NEW QUESTION: 9

A forensic investigator is collecting volatile data such as system information and network information present in the registries, cache, DLLs, and RAM of digital devices through its normal interface.

Identify the data acquisition method the investigator is performing.

- A. Static acquisition
- B. Live acquisition
- C. Non-volatile data acquisition
- D. Dead acquisition

**Answer: B (LEAVE A REPLY)**

The scenario describes the investigator collecting volatile artifacts—specifically information in RAM, active DLLs, system and network state, and transient data held in cache and similar runtime locations—through the device's normal interface while the system is running. In digital forensics documentation, this is the defining characteristic of live acquisition (also called live response). Live acquisition is performed when the system remains powered on so that investigators can capture evidence that would be lost on shutdown, such as running processes, open network connections, logged-on sessions, loaded modules/DLLs, encryption keys, and portions of registry data that exist in memory or are actively changing. By contrast, static acquisition and dead acquisition are conducted when the system is powered off (or the evidence drive is imaged outside the running OS), focusing primarily on persistent storage such as disk sectors and file system structures. Non-volatile data acquisition refers to collecting persistent data stored on media (e.g., files on disk), which does not match the emphasis on RAM and other volatile components in the question. Because the investigator is explicitly collecting volatile data from a running system via its normal interface, the correct method is Live acquisition (B).

### NEW QUESTION: 10

Which of the following network protocols creates secure tunneling through which content obfuscation can be achieved?

- A. SNMP
- B. ARP
- C. SSH
- D. UDP

**Answer: (SHOW ANSWER)**

SSH (Secure Shell) is specifically designed to provide an encrypted channel over an untrusted network. In digital forensics and incident response, SSH is well known for supporting tunneling/port forwarding, where traffic for another protocol (for example, HTTP, database connections, or remote desktop) is encapsulated inside an SSH session. Because the SSH session encrypts payload data (and can also protect authentication and command content), the tunneled traffic becomes obfuscated to network monitoring tools that

can only see metadata such as source/destination IPs, port numbers (often TCP/22), timing, and byte counts. This capability is frequently discussed in forensic references as a mechanism that can hinder content inspection and complicate attribution of user actions purely from packet payload analysis.

By contrast,SNMPis primarily for network management and monitoring, not secure tunneling.ARP resolves IP- to-MAC addresses on local networks and does not provide encryption or tunneling.UDPis a transport protocol that can carry data for many applications but provides no built-in security or tunneling features by itself.

Therefore, the protocol that creates secure tunneling enabling content obfuscation isSSH (C).

event logs) to establish user intent and sequence of actions. Therefore, the correct option isBrowsingHistoryView (B).

### NEW QUESTION: 11

In which of the following attacks does an attacker trick high-profile executives such as CEOs, CFOs, politicians, and celebrities to reveal critical corporate and personal information through email or website spoofing?

- A. Whaling
- B. Smishing
- C. Identity fraud
- D. Spimming

**Answer: A (LEAVE A REPLY)**

The scenario describes a targeted social-engineering attack aimed specifically at high-profile individuals (CEOs, CFOs, politicians, celebrities) and uses email or website spoofing to deceive them into disclosing sensitive information. In digital forensics and incident response documentation, this is most accurately categorized as whaling, a specialized form of phishing that focuses on "big targets" (often called "high-value targets" or "VIPs"). Whaling campaigns typically use highly tailored pretexts (e.g., legal subpoenas, board communications, invoice/payment requests, HR or executive directives) and may include spoofed sender domains, look-alike websites, or fraudulent login pages to harvest credentials and confidential corporate data.

Because executives often have access to financial systems, strategic documents, and privileged communications, attackers concentrate effort on realism and personalization, making whaling distinct from broad, generic phishing.

By contrast,smishingis phishing conducted via SMS/text messages,spimmingis spam over instant messaging platforms, andidentity fraudis a broader category involving impersonation/misuse of personal data but does not specifically denote the executive-targeted spoofing technique described. Therefore, the attack type in the question isWhaling (A).

### NEW QUESTION: 12

David, a cybercriminal, targeted a community and initiated anti-social campaigns online. In this process, he used a layer of the web that allowed him to maintain anonymity during the campaign.

Which of the following layers of the web allowed David to hide his presence during the anti-social campaign?

- A. Surface Web
- B. World Wide Web
- C. Dark Web
- D. Deep Web

**Answer: C (LEAVE A REPLY)**

The layer of the web most associated with maintaining anonymity for users and services is the Dark Web. In digital forensics terminology, the Dark Web refers to services hosted on overlay networks (such as Tor hidden services) that are not indexed by standard search engines and are typically accessible only through specialized software and configurations. Its core characteristic is that it is deliberately designed to reduce traceability by routing traffic through multiple relays and separating identifying information (like the user's real IP address) from the destination. This makes attribution and geolocation significantly harder using traditional network logs alone, which is why adversaries often choose it to conduct covert communications, host content, or coordinate campaigns.

By contrast, the Surface Web (the regular, indexed portion of the web) is generally reachable through normal browsers and is easier to monitor and attribute using conventional ISP, server, and platform logs. "World Wide Web" is a general term for web content accessed via HTTP/HTTPS and does not specifically imply anonymity. The Deep Web refers to content not indexed by search engines (e.g., webmail, databases, authenticated portals), but it is not inherently anonymizing—many deep web resources are simply private or access-controlled. Therefore, the layer enabling David to hide his presence is the Dark Web (C).

### NEW QUESTION: 13

Which of the following measures is defined as the time to move read or write disc heads from one point to another on the disk?

- A. Delay time
- B. Access time
- C. Seek time
- D. Mean time

**Answer: C (LEAVE A REPLY)**

Seek time is the specific performance measure that describes how long a hard disk drive's actuator takes to move the read/write heads across the platters from the current track (cylinder) to the target track where the requested data resides. In traditional magnetic HDDs, the heads must be physically repositioned before any sector can be read or written, making seek time a core component of mechanical latency.

Digital forensics materials emphasize understanding this distinction because HDD mechanical behavior affects acquisition duration, the feasibility of repeated scans, and why imaging or carving operations can take longer on fragmented media. It also helps explain why solid-state drives (SSDs), which have no moving heads, do not have seek time in the same sense and therefore behave differently during large-scale reads.

The other choices are broader or unrelated: access time typically refers to the total time to retrieve data, commonly combining seek time + rotational latency + transfer time. Delay time is not the standard term for head movement in disk performance definitions. Mean time is incomplete as written and is usually part of reliability metrics like mean time between failures, not head positioning. Therefore, the correct measure for head movement time is Seek time (C).

#### **NEW QUESTION: 14**

Which of the following layers of the TCP/IP model includes protocols such as Frame Relay, SMDS, Fast Ethernet, SLIP, PPP, FDDI, ATM, Ethernet, and ARP to enable a machine to deliver the desired data to other hosts in the same network?

- A. Network access layer
- B. Transport layer
- C. Application layer
- D. Internet layer

**Answer: A (LEAVE A REPLY)**

The protocols listed-Frame Relay, SMDS, Fast Ethernet, SLIP, PPP, FDDI, ATM, Ethernet, and ARP- belong to the portion of the TCP/IP model responsible for local network delivery and direct interaction with the physical media and link-layer addressing. In TCP/IP terminology, this is the Network Access layer (also called the Link layer or Network Interface layer). It combines functions that map closely to the OSI Data Link and Physical layers.

This layer is essential for delivering frames within the same network segment because it governs how devices access the medium (e.g., Ethernet), how frames are formatted and transmitted, and how hardware addressing works. ARP (Address Resolution Protocol) is especially important here: it resolves IP addresses to MAC addresses so that an IP packet can be encapsulated into a link-layer frame and delivered to the correct local host or next-hop gateway. Technologies like PPP/SLIP support point-to-point links, while Frame Relay/ATM represent WAN/link technologies, all of which still sit under IP and provide the mechanisms for moving data across the immediate network path.

The Internet layer handles IP routing between networks, the Transport layer provides end-to-end host communications (TCP/UDP), and the Application layer provides user protocols. Therefore, the correct layer is Network access layer (A).

#### **NEW QUESTION: 15**

Which of the following techniques is defined as the art of hiding data "behind" other data without the target's knowledge, thereby hiding the existence of the message itself?

- A. Password cracking
- B. Artifact wiping
- C. Steganography
- D. Program packer

**Answer: C (LEAVE A REPLY)**

Steganography is the technique of concealing a message within another seemingly harmless carrier (such as an image, audio file, video, or document) so that the existence of the hidden message is not apparent to an observer. Digital forensics references distinguish steganography from encryption: encryption scrambles content but usually leaves visible indicators that protected data exists (ciphertext), while steganography aims to make the communication look ordinary, reducing suspicion. In practice, steganographic methods often embed data into redundant or less perceptible parts of the carrier, such as modifying least significant bits in pixel values, altering frequency components in audio, or inserting data into metadata or unused file structures.

The other options do not match the definition. Password cracking is an access technique to recover authentication secrets, not a concealment method. Artifact wiping is an anti-forensics method intended to remove traces (logs, files, slack space remnants), but it does not "hide behind" other data—it destroys or overwrites evidence. Program packers compress/obfuscate executables to hinder static analysis and detection, but they still produce an executable whose presence is evident; they do not primarily hide messages inside benign files. Therefore, the described "hiding the existence of the message itself" corresponds to Steganography (C).

### NEW QUESTION: 16

Which of the following Windows system files is created in the system drive after OS installation to support the internal functions and system service dispatch stubs to executive functions?

- A. Ntoskrnl.exe
- B. Win32k.sys
- C. Ntdll.dll
- D. Kernel32.dll

**Answer: C (LEAVE A REPLY)**

Ntdll.dll is the Windows user-mode system library that provides many internal NT functions (commonly exposed as "NT Native API" routines such as Nt\*/Zw\*) and, critically, contains the system service dispatch stubs used by user-mode code to transition into kernel mode for operating system services. In standard Windows architecture, most user-mode applications call higher-level APIs (for example, Win32 APIs in Kernel32.dll), which then ultimately rely on Ntdll.dll to perform the final step of invoking the kernel through these system call stubs. This is why Ntdll.dll is a core component loaded into nearly every process and is tightly associated with the boundary between user mode and the executive components of the OS.

From a forensics viewpoint, understanding Ntdll.dll matters because it is central to how processes request privileged services, and it is frequently referenced in analyses of process execution, API call chains, and certain user-mode hooking techniques used by malware or anti-forensics tools.

By contrast, Ntoskrnl.exe is the kernel image itself (core kernel/executive), Win32k.sys is a kernel-mode graphics/windowing subsystem component, and Kernel32.dll provides higher-level Win32 APIs rather than the primary system-call stub layer. Hence, Ntdll.dll (C) is the correct answer.

**Valid 112-57 Dumps** shared by PrepPdf.com for Helping Passing 112-57 Exam! PrepPdf.com now offer the **newest 112-57 exam dumps**, the PrepPdf.com 112-57 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 112-57 dumps with Test Engine here:  
<https://www.preppdf.com/EC-COUNCIL/112-57-prepaway-exam-dumps.html> (77 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

#### NEW QUESTION: 17

Philip, a forensic officer, was tasked with investigating a crime scene. In this process, he created bit-by-bit copies of the suspect drive and retrieved all the disk images using the dd command.

Which of the following data acquisition image formats is extracted by Philip in the above scenario?

- A. Raw Format
- B. Advanced Forensic Framework 4 (AFF4)
- C. Advanced Forensics Format (AFF)
- D. Proprietary Format

**Answer: A (LEAVE A REPLY)**

The UNIX/Linux dd utility performs a bit-by-bit (sector-by-sector) copy from an input device (such as a physical disk) to an output target (another device or a flat file). In digital forensics guidance, this type of output is known as a raw (bitstream) image because it captures the exact sequence of bytes from the source media without embedding structured case metadata, compression, or container features by default. The resulting file is often referred to as a "dd image" and may use extensions like .dd or .img, but the key point is the format is raw: it represents a straightforward byte-for-byte representation of the original storage, including allocated data, unallocated space, slack space, and file system structures.

By contrast, AFF and AFF4 are forensic container formats designed to store evidence data along with metadata (and often support features such as chunking, compression, and richer integrity structures). "Proprietary format" refers to vendor-specific containers (for

example, formats created by certain commercial forensic tools) rather than the generic output produced by dd. Since Philip specifically used dd to create bit-by-bit disk images, the extracted acquisition image format is Raw Format (A).

### NEW QUESTION: 18

Bob, a professional hacker, targeted an organization to launch attacks. Bob gathered information such as network topology and a list of live hosts. Based on the collected information, he launched further attacks over the organization's network.

Identify the type of network attack Bob initiated on the target organization in the above scenario.

- A. Data modification
- B. Enumeration
- C. Session hijacking
- D. Buffer overflow

**Answer: B (LEAVE A REPLY)**

The activity described—collecting network topology details and compiling a list of live hosts—matches the reconnaissance phase commonly referred to as enumeration. In digital forensics and incident response documentation, enumeration is the systematic process of discovering and extracting information about a target environment to support later exploitation. It typically follows (or overlaps with) scanning and includes identifying active IP addresses, reachable systems, open ports/services, device roles, OS fingerprints, domain information, shared resources, user/group details, and routing or segmentation clues that reveal how the network is structured.

This information is then used to plan "further attacks," such as targeting exposed services, choosing exploit paths, locating high-value systems, and selecting lateral movement routes. From a forensic standpoint, enumeration attempts often leave traces in firewall logs, IDS alerts, and endpoint artifacts (e.g., bursts of connection attempts across many hosts/ports, ICMP echo sweeps, ARP discovery on local segments, and repeated DNS queries).

The other options do not fit: data modification involves altering data integrity; session hijacking targets active sessions/tokens; and buffer overflow is an exploitation technique against vulnerable software, not the information-gathering step described. Therefore, the correct answer is Enumeration (B).

### NEW QUESTION: 19

Cooper, a forensic analyst, was examining a RAM dump extracted from a Linux system. In this process, he employed an automated tool, Volatility Framework, to identify any malicious code hidden inside the memory.

Which of the following plugins of the Volatility Framework helps Cooper detect hidden or injected files in the memory?

- A. linux\_malfind

- B. `linux_netstat`
- C. `ip addr show`
- D. `nmap -sU localhost`

**Answer: A (LEAVE A REPLY)**

In memory forensics, "hidden or injected" malicious code typically refers to process injection, code caves, unbacked executable mappings, or regions of memory that are marked executable but do not align with normal, file-backed program segments. The Volatility Framework provides specialized plugins to locate these suspicious patterns. `linux_malfind` is the plugin designed to detect potentially injected code by scanning a process's memory mappings for characteristics that commonly indicate malicious presence—such as executable anonymous mappings, unusual permissions (e.g., RWX), and memory regions that contain shellcode-like byte patterns. This is highly relevant when malware attempts to avoid disk artifacts by living in memory or by injecting payloads into legitimate processes.

By contrast, `linux_netstat` is used to enumerate network connections and sockets from memory (useful for C2 analysis), but it does not focus on injected code regions. `ip addr show` and `nmap -sU localhost` are live-system networking commands, not Volatility plugins, and they are not suitable for analyzing a captured RAM image.

Therefore, to detect hidden/injected malicious code in a Linux RAM dump using Volatility, the correct plugin is `linux_malfind` (A).

### NEW QUESTION: 20

Bob, a forensic investigator, was instructed to review a Windows machine and identify any anonymous activities performed using it. In this process, Bob used the command "`netstat -ano`" to view all the active connections in the system and determined that the connections established by the Tor browser were closed.

Which of the following states of the connections established by Tor indicates that the Tor browser is closed?

- A. `CLOSE_WAIT`
- B. `TIME_WAIT`
- C. `ESTABLISHED`
- D. `LISTENING`

**Answer: B (LEAVE A REPLY)**

In Windows network forensics, `netstat -ano` is commonly used to correlate TCP connection states with process identifiers (PIDs) to understand which application created or used a connection. When Tor Browser is actively communicating, outbound circuits typically appear as `ESTABLISHED` connections to Tor relays (entry/guard nodes) or local loopback endpoints used by Tor components. After the browser is closed and the application tears down connections, Windows TCP/IP behavior often leaves recently closed sockets in `TIME_WAIT`.

TIME\_WAIT is a normal TCP state that appears after a connection has been actively closed. It exists to ensure delayed packets from the old session are not misinterpreted as belonging to a new session and to allow proper retransmission of the final ACK if needed. From an investigative standpoint, seeing Tor-related endpoints transition from ESTABLISHED to TIME\_WAIT strongly indicates the sessions were terminated and the application is no longer maintaining live network traffic.

By contrast, CLOSE\_WAIT usually means the remote side has closed but the local application has not fully closed its socket yet, LISTENING indicates a service waiting for inbound connections, and ESTABLISHED means the session is still active.

Therefore, TIME\_WAIT (B) best indicates Tor Browser connections have been closed.

### NEW QUESTION: 21

Which of the following tools can be used by an investigator to analyze the metadata of files in a Windows-based system?

- A. Bulk Extractor
- B. Tor browser
- C. IECachesView
- D. Paraben P2 Commander

**Answer: A (LEAVE A REPLY)**

Bulk Extractor is a digital forensics utility specifically designed to scan storage media (or forensic disk images) and automatically extract structured artifacts and metadata-like features without relying strictly on file system parsing. In Windows investigations, it is commonly used to identify and pull out items such as email addresses, URLs, domain names, credit card patterns, timestamps, GPS coordinates, and other feature records that can be treated as metadata indicators during triage and deep analysis. Because it works by scanning raw data blocks and producing feature reports, it can recover useful information even when files are deleted, partially corrupted, or when file system structures are damaged—conditions frequently encountered in forensic cases. Investigators use its outputs to correlate user activity, locate sensitive data exposure, and identify evidence-rich regions for further examination with file-level tools.

The other options do not match the requirement of analyzing file metadata broadly. Tor browser is an anonymity-focused web browser, not a forensic metadata analyzer. IECachesView is a niche utility for viewing Internet Explorer cache/history artifacts rather than general file metadata analysis. Paraben P2 Commander targets peer-to-peer investigations and related artifacts, not general metadata extraction across files. Therefore, the correct tool for analyzing metadata-like artifacts on a Windows-based system is Bulk Extractor (A).

### NEW QUESTION: 22

Jennifer, a forensics investigation team member, was inspecting a compromised system. After gathering all the evidence related to the compromised system, she disconnected the system from the network to stop the spread of the incident to other systems.

Identify the role played by Jennifer in the forensics investigation.

- A. Incident responder
- B. Incident analyzer
- C. Evidence manager
- D. Expert witness

**Answer: A (LEAVE A REPLY)**

Jennifer's actions match the responsibilities of an incident responder, whose job spans immediate containment, preservation, and stabilization activities during an active or recently active security incident. In standard digital forensics and incident response (DFIR) procedures, responders first take steps to preserve evidence (e.g., documenting the scene, capturing volatile data when appropriate, and collecting relevant system artifacts) and then execute containment measures to prevent further harm. Disconnecting a compromised host from the network is a classic containment control used to stop malware propagation, block command-and-control communications, and prevent lateral movement to other systems. An incident analyzer typically focuses on deeper technical analysis—timeline reconstruction, root cause determination, and correlating artifacts across hosts and logs—rather than performing immediate containment.

An evidence manager is primarily responsible for maintaining evidence integrity, chain of custody, storage, labeling, and access control, not operational containment. An expert witness provides formal testimony and interpretation in legal or disciplinary proceedings and is not usually involved in live containment actions.

Since Jennifer both gathered evidence and then isolated the system to stop spread, the role most consistent with documented DFIR responsibilities is Incident responder (A).

### NEW QUESTION: 23

Steve, a professional hacker, attempted to hack Alice's banking account. To accomplish his goal, Steve used an automated tool to guess Alice's login credentials. The tool uses a trial-and-error method by attempting all possible combinations of usernames and passwords to determine the valid credentials.

Identify the type of attack initiated by Steve in the above scenario.

- A. Brute-force attack
- B. Phishing attack
- C. Trojan horse attack
- D. Data manipulation attack

**Answer: A (LEAVE A REPLY)**

The scenario describes an automated, trial-and-error attempt that tries all possible combinations of usernames and passwords until a correct credential pair is found. This is the defining characteristic of a brute-force attack.

In digital forensics terminology, brute force is a direct password-guessing method that relies on exhaustive attempts (or systematically generated candidates) rather than tricking the user or exploiting a software flaw.

Investigators commonly recognize brute-force activity through artifacts such as repeated authentication failures in security logs, high-frequency login attempts from a single IP or distributed sources, account lockout events, and abnormal spikes in authentication traffic. In banking and web environments, it may also appear as repeated POST requests to login endpoints with varying credential pairs and consistent user-agent patterns, sometimes accompanied by throttling or CAPTCHA triggers.

The other options do not match the described "attempting all possible combinations" behavior.

Phishing obtains credentials by deception (fake emails/sites). A Trojan horse steals data by running malicious code on the victim's system. Data manipulation focuses on altering data integrity rather than credential guessing. Therefore, the correct attack type is Brute-force attack (A).

#### **NEW QUESTION: 24**

Bob, a forensic specialist at a newly established NGO, discovered a security loophole in the NGO's web application, which unintentionally reveals early enrolled NGO members' biodata to attackers. Bob immediately employed a content filtering mechanism to protect all the NGO's data sources and prevent further damage.

Identify the web application threat identified by Bob in the above scenario.

- A.** Buffer overflow
- B.** Information leakage
- C.** Authentication hijacking
- D.** Cookie poisoning

**Answer: (SHOW ANSWER)**

The scenario describes a web application that unintentionally reveals sensitive member biodata to attackers.

This is a classic case of information leakage, where confidential or private data becomes exposed due to poor access control, improper output handling, verbose error messages, misconfigured endpoints, insecure direct object references, or unintended exposure through pages, APIs, backups, or logs. In forensic and web security documentation, information leakage is defined by the unauthorized disclosure of data, even if the attacker does not alter the system. The key indicator here is that the application is "revealing" biodata—meaning confidentiality is breached.

Bob's response—using a content filtering mechanism—also aligns with mitigating data exposure. Content filtering can prevent sensitive fields from being returned, mask personally identifiable information, restrict responses based on user role, and sanitize outputs before they leave the server.

The other options do not match the described impact. Buffer overflow is a low-level memory corruption vulnerability, typically associated with native code execution rather than accidental biometric data exposure.

Authentication hijacking involves taking over sessions/credentials, and cookie poisoning involves manipulating cookie values to gain privileges or alter behavior—neither is explicitly indicated. Therefore, the identified threat is Information leakage (B).

### NEW QUESTION: 25

Which of the following steps in forensic readiness planning provides a backup for future reference and assists in presenting evidence in a court of law?

- A. Creating a process for documenting the procedure
- B. Identifying the potential evidence required for an incident
- C. Determining the sources of evidence
- D. Keeping an incident response team ready to review the incident

**Answer: (SHOW ANSWER)**

In forensic readiness planning, the goal is to ensure that when an incident occurs, the organization can collect, preserve, and present digital evidence in a manner that remains reliable, repeatable, and legally defensible. A key requirement for courtroom acceptance is clear documentation—often referred to as proper documentation and chain-of-custody support—showing what actions were taken, by whom, when, using which tools, and under what conditions. Creating a defined process for documenting procedures ensures investigators consistently record acquisition steps, handling methods, hashing/verification results, storage locations, access history, and any changes in evidence possession. This documentation becomes a "backup" in the sense that it preserves institutional memory of the investigation steps, allowing future reviewers (auditors, opposing experts, courts) to reconstruct and validate what occurred even long after the incident.

While identifying potential evidence (B) and determining evidence sources (C) are important readiness tasks, they do not themselves create the structured record needed to defend evidence integrity. Keeping an incident response team ready (D) supports operational response, but does not directly ensure admissibility. Therefore, the step that provides future reference and supports court presentation is Creating a process for documenting the procedure (A).

**Valid 112-57 Dumps** shared by PrepPdf.com for Helping Passing 112-57 Exam!  
PrepPdf.com now offer the **newest 112-57 exam dumps**, the PrepPdf.com 112-57 exam **questions have been updated** and **answers have been corrected** get the **newest** PrepPdf.com 112-57 dumps with Test Engine here:

<https://www.preppdf.com/EC-COUNCIL/112-57-prepaway-exam-dumps.html> (77 Q&As  
Dumps, **40%OFF** Special Discount: **Exam-Tests**)