DUMPSARENA

GIACCertified Forensics Analyst

GIAC GCFA

Version Demo

Total Demo Questions: 35

Total Premium Questions: 359

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Volume A	113
Topic 2, Volume B	100
Topic 3, Volume C	126
Total	359

QUESTION NO: 1

You use the FAT16 file system on your Windows 98 computer. You want to upgrade to the FAT32 file system. What is the advantage of the FAT32 file system over FAT16 file system?

Each correct answer represents a complete solution. Choose two.

A. It allocates disk space more efficiently.

B. On startup failure, you can start the computer by using an MS-DOS or Windows 95 bootable floppy disk.

C. It uses larger cluster sizes.

D. It supports drives up to 2 terabytes (TB) in size.

ANSWER: A D

Explanation:

FAT32 allocates disk space more efficiently because it can use substantially smaller clusters than FAT16 on partitions of comparable size. A cluster is the minimum allocation unit for a file, so unused space in the final cluster assigned to each file is wasted. By reducing the required cluster size on larger volumes, FAT32 reduces that slack space, which is particularly useful where the volume contains many small files. Microsoft describes FAT32 as improving storage efficiency by using smaller clusters than FAT16. FAT32 also expands the supported volume size dramatically. Its 32-bit file-allocation entries permit volumes far beyond FAT16's practical 2 GB partition limit; the FAT32 on-disk format supports volumes up to approximately 2 TB when using standard 512-byte sectors. This made FAT32 suitable for the much larger hard disks becoming common with Windows 98-era systems. These are file-system format advantages: more efficient use of capacity and support for much larger volumes. See Microsoft's FAT32 File System documentation and its File Allocation Tables overview.

QUESTION NO: 2

Adam works as a Computer Hacking Forensic Investigator in a law firm. He has been assigned with his first project. Adam collected all required evidences and clues. He is now required to write an investigative report to present before court for further prosecution of the case. He needs guidelines to write an investigative report for expressing an opinion. Which of the following are the guidelines to write an investigative report in an efficient way? Each correct answer represents a complete solution. Choose all that apply.

A. All ideas present in the investigative report should flow logically from facts to conclusions.

B. There should not be any assumptions made about any facts while writing the investigative report.

C. Opinion of a lay witness should be included in the investigative report.

D. The investigative report should be understandable by any reader.

ANSWER: A B D

Explanation:

"All ideas present in the investigative report should flow logically from facts to conclusions," "There should not be any assumptions made about any facts while writing the investigative report," and "The investigative report should be understandable by any reader" are sound reporting guidelines for a forensic investigator offering an opinion. A court-facing report must distinguish documented observations and validated examination results from the analyst's resulting conclusions. The reasoning path should be transparent: identify the evidence examined, describe the methods used, report the relevant findings, and then connect those findings to a conclusion using language proportionate to the supporting facts. This lets counsel, the court, and another qualified examiner evaluate the basis for the opinion.

Investigators should not fill evidentiary gaps with unstated assumptions. Where an interpretation depends on a limitation, uncertainty, or condition, it should be explicitly documented and bounded rather than presented as fact. Clear language is equally important because reports are often read by attorneys, judges, jurors, and organizational decision-makers who may not have specialized technical knowledge. Defining necessary terminology, avoiding unnecessary jargon, and presenting conclusions plainly improves accuracy and usability without sacrificing technical rigor. These practices align with the

reporting and documentation principles in NIST SP 800-86 and the documentation guidance in the National Institute of Justice electronic crime-scene guide.

QUESTION NO: 4

Which of the following log files are used to collect evidences before taking the bit-stream image of the BlackBerry? Each correct answer represents a complete solution. Choose all that apply.

A. Roam and Radio

B. user history

C. Radio status

D. Transmit/Receive

ANSWER: A B C D

Explanation:

Before a bit-stream acquisition of a legacy BlackBerry device, an examiner should document volatile and diagnostic information that can be altered by device interaction, loss of power, radio changes, or the imaging process. **Roam and Radio**, **user history**, **Radio status**, and **Transmit/Receive** are relevant BlackBerry diagnostic/history views that can preserve useful pre-acquisition evidence. Together, they can record the handset's network registration and roaming context, current radio state, traffic and transmission-related status, and user/device event history. Capturing these views first helps establish device condition and communications context at the time of seizure, supports later timeline interpretation, and documents information that may not be represented clearly in a filesystem-level image. The examiner should photograph or otherwise contemporaneously record the displayed data, preserve acquisition notes, and minimize interaction with the handset before creating the forensic image. This approach follows the general mobile-forensics principle of preserving volatile data and documenting the device's condition before undertaking actions that could modify evidence. See NIST's Guidelines on Mobile Device Forensics and the archived BlackBerry knowledge base information on BlackBerry support and device documentation.

QUESTION NO: 5

Which of the following registry hives contains information about all users who have logged on to the system?

A. HKEY_CLASSES_ROOT

B. HKEY_CURRENT_USERS

C. HKEY_USERS

D. HKEY_CURRENT_CONFIG

ANSWER: C

Explanation:

HKEY_USERS is the correct answer because it is the predefined Registry key that exposes user-specific Registry information organized by security identifier (SID). Each SID-named subkey corresponds to a user profile that is loaded on the system, and it contains that user's per-user configuration data, including the contents normally viewed through HKEY_CURRENT_USER for the active user. In a forensic context, examining HKEY_USERS allows an analyst to identify and correlate user profile SIDs with user-specific artifacts and settings. HKEY_CURRENT_USER is not an independent hive; it is a convenience mapping to the currently interactive user's subkey under HKEY_USERS. Consequently, HKEY_USERS is the appropriate Registry location when the question concerns user-level information across profiles rather than only the current user. Microsoft documents HKEY_USERS as containing subkeys that correspond to user profiles and notes that HKEY_CURRENT_USER maps to one of these user-profile keys. See Microsoft's predefined Registry keys documentation and Microsoft's Registry hives overview.

QUESTION NO: 6

Which of the following tools is used to block email, Instant Message, Web site, or other media if inappropriate words such as pornography, violence etc. is used?

A. iProtect

B. Reveal

C. iProtectYou

D. Child Exploitation Tracking System

ANSWER: C

Explanation:

iProtectYou is the correct answer. It was a content-filtering and parental-control product designed to monitor and control Internet activity based on configured policy rules. A core capability was keyword- and category-based filtering: an administrator or parent could define terms and content categories associated with material such as pornography or violence, then have the software block or restrict access when those terms appeared in web content, email, instant-message conversations, or other monitored communications. This directly matches the question's emphasis on preventing delivery or viewing of media containing inappropriate words or subjects.

From a forensic and security-policy perspective, this is an example of content filtering: inspection of communications or web material against organizational or parental rules, followed by an enforcement action such as blocking, logging, or alerting. Content filtering is commonly implemented as part of acceptable-use, child-safety, and data-protection controls. NIST's security-control catalog describes policy-based controls relevant to restricting and monitoring information-system use and communications; see NIST SP 800-53 Rev. 5. For broader context on safe online behavior and protective controls for children, see CISA Online Safety.

QUESTION NO: 7

Which of the following is used to store configuration settings and options on Microsoft Windows operating systems?

A. Windows Config file

B. Group policy editor

C. Windows setting

D. Windows Registry

ANSWER: D

Explanation:

The Windows Registry is the hierarchical database Windows uses to store a broad range of operating-system, hardware, application, and user-specific configuration settings. Its data is organized into keys, subkeys, and values, and it includes settings that control such things as installed software, device configuration, startup behavior, services, file associations, security-related settings, and user preferences. For forensic analysis, Registry artifacts are particularly valuable because the underlying hive files can preserve evidence of system configuration and user activity. Common hives include SYSTEM, SOFTWARE, SAM, SECURITY, NTUSER.DAT, and UsrClass.dat. An examiner can use the Registry to reconstruct facts such as attached devices, executed programs, network profiles, persistence locations, and account-related information, while accounting for the relevant user profile and the time at which a hive was acquired. Microsoft describes the Registry as a central hierarchical database for low-level settings for Windows and applications that use it. Microsoft's documentation also identifies Registry Editor as the tool for viewing and modifying Registry data. See Microsoft's Windows Registry overview and Microsoft guidance on Registry Editor.

QUESTION NO: 8

Which of the following statements are true about routers?

Each correct answer represents a complete solution. Choose all that apply.

A. Routers organize addresses into classes, which are used to determine how to move packets from one network to another.

B. Routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow.

C. Routers do not limit physical broadcast traffic.

D. Routers act as protocol translators and bind dissimilar networks.

ANSWER: A B D

Explanation:

Routers make forwarding decisions at the network layer, selecting an appropriate next hop and path for packets destined for other networks. This is the central routing function: a router uses its routing table and the destination network portion of an IP address to determine where traffic should be sent. Address classes are part of the historical classful IPv4 model used to identify network boundaries; modern routing normally uses classless inter-domain routing and prefix lengths, but the underlying concept remains that routers use logical network addressing to move packets between networks.

Routers also separate broadcast domains. They do not forward ordinary Layer 2 broadcast frames from one routed interface to another, which makes them important boundaries between LANs. When joining networks that use different Layer 2 technologies, a router removes the incoming frame encapsulation, processes the Layer 3 packet, and encapsulates it appropriately for the outbound interface. In that practical sense, routers bind dissimilar networks and provide the necessary translation between their local link-layer formats while routing the network-layer traffic. RFC 1812 describes an IP router as a device that forwards IP datagrams between networks, and Cisco summarizes routing as connecting networks and directing traffic between them. See RFC 1812 and Cisco: What Is a Router?.

QUESTION NO: 9 - (HOTSPOT)

HOTSPOT

Identify the port in the image given below, which can be connected to the hub to extend the number of ports, and up to 127 devices can be connected to it?

Hot Area:



ANSWER:



Explanation:

The correct selection is the group of rectangular USB Type-A ports highlighted in green. USB is designed around a host-and-hub topology: a computer's USB host controller connects to a root hub, and additional hubs can be attached to provide more downstream ports for peripherals. This is the interface family associated with the stated limit of up to 127 devices on a single USB bus, including hubs and other USB functions in the topology. The highlighted connectors match the standard physical appearance of USB Type-A receptacles commonly found in stacks on a desktop motherboard's rear I/O panel. They are appropriate for attaching USB hubs as well as devices such as keyboards, mice, external storage, printers, cameras, and other peripherals. A hub expands the number of usable physical connections while allowing the attached devices to communicate through the same USB bus hierarchy. The USB Implementers Forum's overview of USB describes USB as an interface used to connect hosts, hubs, and peripherals, while the USB specifications define the addressing and hub-based architecture that supports this device limit. See the USB Implementers Forum and Microsoft's USB hub architecture documentation for supporting technical background. Therefore, the marker belongs on the stacked USB receptacles shown in the center-right area of the image.

QUESTION NO: 10

By gaining full control of router, hackers often acquire full control of the network. Which of the following methods are commonly used to attack Routers? Each correct answer represents a complete solution. Choose all that apply.

A. By launching Social Engineering attack

B. By launching Max Age attack

C. Route table poisoning

D. By launching Sequence++ attack

ANSWER: B C D

Explanation:

By launching Max Age attack, **Route table poisoning**, and **By launching Sequence++ attack** are recognized attacks against dynamic routing, particularly OSPF. OSPF distributes link-state advertisements throughout an area so each participating router can construct a consistent topology database and calculate routes. An attacker able to inject, replay, or otherwise influence these advertisements can affect routing decisions across the network.

A Max Age attack uses a link-state advertisement with its age set to the maximum value, causing recipients to flush the referenced advertisement from their link-state databases. Route table poisoning introduces false or malicious route information so that traffic can be redirected, blackholed, or routed through an attacker-controlled path. A Sequence++ attack uses an artificially high OSPF link-state advertisement sequence number. Since OSPF favors the most recent instance of an advertisement, the forged update can supersede the legitimate one and persist until the legitimate router originates a still-newer update.

These risks are why routing-protocol authentication, adjacency controls, and monitoring for unexpected link-state database changes are important defensive practices. OSPF's advertisement aging, sequence-number processing, and flooding behavior are specified in RFC 2328; Cisco also describes OSPF authentication and related security configuration in its OSPF Authentication documentation.

QUESTION NO: 11

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He enters the following command on the Linux terminal:

chmod 741 secure.c

Considering the above scenario, which of the following statements are true? Each correct answer represents a complete solution. Choose all that apply.

A. By the octal representation of the file access permission, John is restricting the group members to only read the secure.c file.

B. The textual representation of the file access permission of 741 will be -rwxr--rw-.

C. John is restricting a guest to only write or execute the secure.c file.

D. John is providing all rights to the owner of the file.

ANSWER: A D

Explanation:

The numeric mode `741` is interpreted as three independent octal permission sets, in the order owner, group, and others. The first digit, `7`, combines read (4), write (2), and execute (1), so the file owner receives all three standard permissions. Therefore, “John is providing all rights to the owner of the file.” is correct. The second digit, `4`, grants read permission and no write or execute permission to the file’s group. Accordingly, “By the octal representation of the file access permission, John is restricting the group members to only read the secure.c file.” is also correct. In symbolic form, these permissions correspond to owner `rwx`, group `r--`, and others `--x`. Numeric modes are an established `chmod` mechanism: each permission bit has an octal value, and the values in each permission class are added together. This lets an analyst accurately determine effective discretionary access from a command such as `chmod 741 secure.c`. See the GNU Coreutils documentation on changing permissions and the Linux chmod manual page.

QUESTION NO: 12

What are the purposes of audit records on an information system? Each correct answer represents a complete solution. Choose two.

A. Backup

B. Investigation

C. Upgradation

D. Troubleshooting

ANSWER: B D

Explanation:

Audit records support **Investigation** by preserving evidence of security-relevant and operational events, including user activity, authentication attempts, access to resources, process execution, and configuration changes. During a suspected incident, analysts can use timestamps, account identifiers, source information, and event sequences to reconstruct what occurred, establish a timeline, determine the scope of activity, and correlate actions across systems. This makes properly collected and protected audit data an important forensic resource.

Audit records also support **Troubleshooting**. Administrators and incident responders review system and application logs to identify errors, service failures, unexpected behavior, resource problems, and the sequence of events preceding an outage. Event records provide the factual context needed to isolate the affected component and validate whether corrective actions restored normal operation. NIST identifies audit-log management as essential for analyzing events and responding to operational and security issues, while its incident-handling guidance emphasizes using logs and other data sources for incident analysis and recovery. See NIST SP 800-92, Guide to Computer Security Log Management and NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide.

QUESTION NO: 13

Which of the following is used for remote file access by UNIX/Linux systems?

A. NetWare Core Protocol (NCP)

B. Common Internet File System (CIFS)

C. Server Message Block (SMB)

D. Network File System (NFS)

ANSWER: D

Explanation:

Network File System (NFS) is the traditional network file-sharing protocol for UNIX and Linux environments. It allows a client system to mount a directory exported by a remote server so that the remote files and directories appear within the client's local filesystem hierarchy. After mounting an NFS export, normal filesystem operations—including reading, writing, listing directories, and examining file metadata—can be performed through the mount point, subject to server export rules and filesystem permissions.

For forensic work, recognizing NFS is important because NFS mount configuration, server export definitions, and authentication or access-control settings can identify remotely available storage and help establish how a system accessed data. On Linux, NFS client mounts are commonly recorded in configuration sources such as `/etc/fstab` and may be visible in current mount information. NFS is standardized by the IETF; the current NFS version 4 specification defines its protocol and filesystem access behavior. See RFC 7530: Network File System Version 4 Protocol and the Red Hat documentation on mounting NFS shares.

QUESTION NO: 14

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He enters a single quote in the input field of the login page of the We-are-secure Web site and receives the following error message:

Microsoft OLE DB Provider for ODBC Drivers error '0x80040E14'

This error message shows that the We-are-secure Website is vulnerable to _____.

A. An XSS attack

B. A SQL injection attack

C. A Denial-of-Service attack

D. A buffer overflow

ANSWER: B

Explanation:

A SQL injection attack is the correct answer. A single quotation mark is a significant test character because SQL commonly uses single quotes to delimit string literals. If an application directly concatenates login input into a database query without appropriate parameterization or validation, the added quote can terminate the expected string and cause malformed SQL syntax. The returned Microsoft OLE DB Provider for ODBC Drivers error indicates that database-query processing was exposed to the user and that the submitted input influenced the SQL statement sent through the ODBC data-access layer. This is a classic indicator of potential SQL injection during initial error-based testing. Although an error alone does not prove that data can be extracted or authentication bypassed, it establishes that the application should be investigated for unsafe query construction. Proper remediation is to use parameterized queries (prepared statements), ensure database errors are handled server-side rather than disclosed in HTTP responses, and use an account with only the database permissions the application requires. OWASP describes SQL injection as occurring when untrusted data changes the meaning of an SQL

command, and recommends parameterized interfaces as the primary defense. See the OWASP SQL Injection overview and the OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 15

Which of the following statements are NOT true about volume boot record or Master Boot Record?

Each correct answer represents a complete solution. Choose all that apply.

A. The end of MBR marker is h55CC.

B. The actual program can be 512 bytes long.

C. Volume boot sector is present at cylinder 0, head 0, and sector 1 of the default boot drive.

D. Four 16 bytes master partition records are present in MBR.

ANSWER: A B C

Explanation:

The statements “The end of MBR marker is h55CC,” “The actual program can be 512 bytes long,” and “Volume boot sector is present at cylinder 0, head 0, and sector 1 of the default boot drive” are not true. A conventional MBR is one 512-byte sector and ends with the two-byte boot signature `0x55AA`, stored at offsets 510 and 511; `0x55CC` is not the valid MBR boot signature. The MBR bootstrap-program region is limited to the first 446 bytes because the same sector also contains four 16-byte partition-table entries (64 bytes total) and the two-byte signature. Likewise, a volume boot record/sector cannot devote all 512 bytes to executable bootstrap code because it includes required filesystem boot-sector data and the terminal boot signature. Finally, cylinder 0, head 0, sector 1 historically identifies the first sector of a disk, where an MBR may reside on an MBR-partitioned disk. A volume boot sector resides at the first sector of its own volume or partition, not necessarily at the beginning of the physical boot disk. See the OSDev MBR layout reference and Microsoft’s Master Boot Records documentation.

QUESTION NO: 16

You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to allow direct access to the filesystems data structure. Which of the following Unix commands can you use to accomplish the task?

A. du

B. debugfs

C. df

D. dosfsck

ANSWER: B

Explanation:

`debugfs` is correct because it is an interactive filesystem debugger designed to provide direct, low-level access to an ext-family filesystem’s internal data structures. It can open a filesystem device or image and lets an authorized examiner inspect and manipulate metadata such as superblocks, group descriptors, inodes, directory entries, allocation bitmaps, and data blocks. This capability is especially relevant in forensic work, where examining filesystem structures directly can reveal information that is not readily available through ordinary file-level commands.

The utility is supplied by the e2fsprogs project and is intended for use with ext2, ext3, and ext4 filesystems. Its command interface supports activities such as viewing inode contents, navigating directories within the filesystem image, locating blocks, and examining deleted-file-related metadata where it remains recoverable. Because direct metadata modification can damage a filesystem, forensic best practice is to work from a verified image or use read-only access unless an intentional

repair or test operation is required. The e2fsprogs debugfs manual page describes it as an interactive filesystem debugger, while the Linux ext4 documentation provides context on the filesystem structures it can examine.

QUESTION NO: 17

Which of the following IP addresses are private addresses?

Each correct answer represents a complete solution. Choose all that apply.

A. 19.3.22.17

B. 192.168.15.2

C. 192.166.54.32

D. 10.0.0.3

ANSWER: B D

Explanation:

192.168.15.2 and **10.0.0.3** are private IPv4 addresses because each falls within an address block reserved for private internets by RFC 1918. The RFC defines three private-use ranges: 10.0.0.0 through 10.255.255.255 (10.0.0.0/8), 172.16.0.0 through 172.31.255.255 (172.16.0.0/12), and 192.168.0.0 through 192.168.255.255 (192.168.0.0/16). Thus, 10.0.0.3 belongs to the 10.0.0.0/8 range, while 192.168.15.2 belongs to the 192.168.0.0/16 range. These addresses are intended for use inside private networks, such as organizational LANs and home networks, and are not globally unique or publicly routable on the Internet. In forensic investigations, recognizing RFC 1918 space helps distinguish internal addressing information from public Internet addressing when interpreting logs, network captures, and system configuration artifacts. The authoritative definitions are available in RFC 1918; IANA also identifies these allocations in its IPv4 Special-Purpose Address Registry.

QUESTION NO: 18

Adam works as a Security Administrator for Umbrella Technology Inc. He reported a breach in security to his senior members, stating that "security defenses has been breached and exploited for 2 weeks by hackers." The hackers had accessed and downloaded 50,000 addresses containing customer credit cards and passwords. Umbrella Technology was looking to law enforcement officials to protect their intellectual property. The intruder entered through an employee's home machine, which was connected to Umbrella Technology's corporate VPN network. The application called BEAST Trojan was used in the attack to open a "back door" allowing the hackers undetected access. The security breach was discovered when customers complained about the usage of their credit cards without their knowledge. The hackers were traced back to Shanghai, China through e-mail address evidence. The credit card information was sent to that same e-mail address. The passwords allowed the hackers to access Umbrella Technology's network from a remote location, posing as employees. Which of the following actions can Adam perform to prevent such attacks from occurring in future?

A. Apply different security policy to make passwords of employees more complex.

B. Replace the VPN access with dial-up modem access to the company's network.

C. Disable VPN access to all employees of the company from home machines

D. Allow VPN access but replace the standard authentication with biometric authentication.

ANSWER: C

Explanation:

Disable VPN access to all employees of the company from home machines is the appropriate answer because the compromise originated on an employee-owned or home-based endpoint that had a trusted VPN connection into the corporate environment. Once the endpoint was infected with a backdoor Trojan, the attacker could use that established remote-access path and stolen credentials to reach internal resources while appearing to be a legitimate employee.

Removing home-machine VPN connectivity eliminates this specific ingress path and prevents unmanaged, potentially compromised home systems from being directly trusted as network clients.

Remote access materially expands an organization's attack surface because endpoint compromise can be converted into access to internal services and data. NIST's telework security guidance emphasizes that organizations must manage the security risks introduced by remote clients and remote access methods, including the protection and control of client devices. In the scenario presented, the most direct preventive containment measure is to prohibit VPN access from home machines rather than continue to rely on them as trusted connection points. See NIST SP 800-46 Rev. 2, Guide to Enterprise Telework, Remote Access, and BYOD Security and CISA Malware guidance.

QUESTION NO: 19

Which of the following types of firewall functions at the Session layer of OSI model?

A. Application-level firewall

B. Switch-level firewall

C. Packet filtering firewall

D. Circuit-level firewall

ANSWER: D

Explanation:

Circuit-level firewall is correct because it operates by controlling and validating connections at the OSI Session layer. Rather than inspecting the contents of every application message, a circuit-level gateway evaluates whether a requested session is legitimate and establishes a controlled virtual circuit between the client and destination. This allows the firewall to enforce connection policies while concealing internal network details from external systems. A common implementation approach is to proxy the connection handshake, such as with SOCKS, so that the external host communicates with the gateway rather than directly with the internal client. Once the session is approved and the circuit is established, traffic can pass according to the gateway's configured policy. This session-oriented behavior is the defining characteristic tested by the question: the firewall's decision focuses on establishing, maintaining, and terminating communications sessions. Cisco's firewall overview discusses circuit-level gateways as an intermediary connection mechanism, while Fortinet's glossary describes circuit-level gateways as operating at the session layer and monitoring TCP handshakes and session establishment. See Cisco's firewall overview and Fortinet's circuit-level gateway definition.

QUESTION NO: 20 - (DRAG DROP)

Maria works as a professional Ethical Hacker. She recently got a project to test the security of www.we-are-secure.com. Arrange the three pre-test phases of the attack to test the security of weare-secure.

Select and Place:



ANSWER:



Explanation:

The correct pre-test sequence is **Footprinting**, followed by **Identifying the active system**, and then **Enumerating the system**. Footprinting is the initial reconnaissance activity. It develops a baseline understanding of the target organization and its exposed presence by collecting information such as domains, IP address ranges, DNS records, public-facing infrastructure, employee information, and technology clues. This intelligence helps define what should be assessed while keeping early activity focused and methodical.

After collecting that context, identifying the active system establishes which discovered hosts are actually reachable and responsive. In practical terms, this means determining the systems that are alive on the relevant network ranges and are therefore candidates for further assessment. Identifying live systems narrows the scope from possible addresses and assets to systems that can be examined directly.

Enumeration comes next because it builds on the live-host results. Enumeration obtains more specific technical details from the accessible systems, such as exposed services, service banners, accounts, shares, naming information, and other data that may inform later testing. NIST describes reconnaissance as collecting information about a target before an attack and recognizes scanning and enumeration-related activities as foundational discovery work; see NIST SP 800-115, Technical Guide to Information Security Testing and Assessment. The broader structure also aligns with the reconnaissance and scanning concepts described in the MITRE CAPEC attack-pattern framework. Together, the three selected steps progress from broad intelligence gathering, to confirmation of active assets, to detailed discovery of those assets.

QUESTION NO: 21

Which of the following can be monitored by using the host intrusion detection system (HIDS)? Each correct answer represents a complete solution. Choose two.

A. Computer performance

B. System files

C. File system integrity

D. Storage space on computers

ANSWER: B C

Explanation:

Host-based intrusion detection systems monitor activity and artifacts on an individual endpoint rather than observing only network traffic. **System files** are a core HIDS monitoring target because unexpected creation, deletion, permission changes, ownership changes, or modifications to operating-system binaries, configuration files, and other sensitive files can indicate compromise or unauthorized administrative activity. A HIDS can collect these events from the host and generate alerts for investigation.

File system integrity is also a primary HIDS capability. File-integrity monitoring establishes a known-good baseline for selected files and directories, commonly using cryptographic hashes plus metadata such as permissions, size, and timestamps. Subsequent scans or real-time checks compare the current state with that baseline. This enables an analyst to identify potentially malicious tampering, including altered executables, changed startup configurations, or modified security settings. The NIST intrusion-detection guidance identifies host-based systems as examining host audit data and system activity, while the OSSEC HIDS documentation specifically describes file-integrity monitoring as checking for changes to

critical system files. See NIST SP 800-94: Guide to Intrusion Detection and Prevention Systems and Wazuh File Integrity Monitoring documentation.

QUESTION NO: 22

Which status is a problem, assigned when its cause has been recognized?

A. Incident

B. Request for Change

C. Known Error

D. Work-around

ANSWER: C

Explanation:

Known Error is the correct term because IT service management defines a known error as a problem for which the root cause has been identified and understood. Problem management investigates the underlying cause of one or more incidents; once that investigation establishes the cause, the problem is recorded as a known error. This classification preserves the diagnostic findings so service teams can recognize the condition quickly if it recurs and can plan or prioritize a permanent resolution. A known error record commonly includes the cause, affected services or configurations, symptoms, and any available workaround. The existence of a workaround is helpful but is not what creates the known-error status: recognizing and documenting the cause is the defining condition. This terminology is central to ITIL problem management and the use of a known-error database to make established knowledge available to support staff. See the AXELOS ITIL glossary and Atlassian's overview of ITSM problem management for the relationship between problems, known errors, root-cause analysis, and workarounds.

QUESTION NO: 23

Which of the following files in LILO booting process of Linux operating system stores the location of Kernel on the hard drive?

A. /boot/map

B. /boot/boot.b

C. /etc/lilo.conf

D. /sbin/lilo

ANSWER: A

Explanation:

`/boot/map` is correct because it is LILO's map file: a file created when the `lilo` installation program processes the boot configuration and records the disk-sector locations needed to load the selected kernel image and associated boot components. At boot time, LILO's early-stage loader has only limited filesystem-awareness, so it relies on this precomputed map of physical disk locations rather than locating the kernel by pathname in a mounted filesystem. This design is also why LILO must be rerun after changing a kernel image, relocating it, or modifying relevant boot settings: rerunning the installer regenerates the map with current sector addresses. The LILO manual identifies the map file as containing the sector locations of the kernel and other boot images and notes that it is generated by the installer. Conventionally, distributions place this file at `/boot/map`, although its path can be configured. See the LILO manual page and the Linux LILO HOWTO for details on LILO's map-based boot loading process.

QUESTION NO: 24

Which of the following commands is used to enforce checking of a file system even if the file system seems to be clean?

A. e2fsck -f

B. e2fsck -p

C. e2fsck -b

D. e2fsck -c

ANSWER: A

Explanation:

The correct command is `e2fsck -f`. The `-f` (force) option instructs `e2fsck` to perform a filesystem check even when the filesystem appears clean according to its metadata and journal state. Normally, `e2fsck` may skip a full check if the filesystem is marked clean, which avoids an unnecessary and potentially lengthy scan. In forensic, incident-response, and system-recovery contexts, forcing the check can be appropriate when an analyst or administrator needs validation of filesystem consistency regardless of that clean status.

`e2fsck` is the consistency-checking utility for ext-family filesystems, including ext2, ext3, and ext4. Before checking or repairing a filesystem, it should generally be unmounted; checking a mounted writable filesystem can cause further inconsistency or damage. A forensic examiner should work from an acquired image or other verified copy rather than alter original evidence. The e2fsprogs manual documents that `-f` forces checking even if the filesystem seems clean. See the e2fsck manual page and the Linux kernel ext4 documentation.

QUESTION NO: 26

Your network has a Windows 2000 Server computer with FAT file system, shared by several users.

This system stores sensitive data. You decide to encrypt this data to protect it from unauthorized access. You want to accomplish the following goals:

□□ Data should be secure and encrypted.

□□ Administrative efforts should be minimum.

□□ You should have the ability to recover encrypted files in case the file owner leaves the company.

□□ Other permissions on encrypted files should be unaffected.

□□ File-level security is required on the disk where data is stored.

□□ Encrypting or decrypting of files should not be the responsibility of the file owner.

You take the following steps to accomplish these goals :

□□ Convert the FAT file system to Windows 2000 NTFS file system.

□□ Use Encrypting File System (EFS) to encrypt data.

Which of the following goals will you be able to accomplish?

Each correct answer represents a complete solution. Choose all that apply.

A. File-level security is available on the disk where data is stored.

B. You have the ability to recover encrypted files in case the file owner leaves the company.

C. Encrypting or decrypting of files is no longer the responsibility of the file owner.

D. Data are secured and encrypted.

E. Administrative efforts are minimum.

F. Other permissions on encrypted files are unaffected.

ANSWER: A B C D E F

Explanation:

Converting the volume from FAT to NTFS enables NTFS discretionary access controls, so *File-level security is available on the disk where data is stored.* EFS requires NTFS and encrypts file contents at rest, fulfilling *Data are secured and encrypted.* EFS is designed to be transparent during normal use: an authorized user opening or saving an EFS-protected file has encryption and decryption performed by the operating system, so *Encrypting or decrypting of files is no longer the responsibility of the file owner.*

EFS also preserves the file's normal NTFS access-control entries rather than replacing them, supporting *Other permissions on encrypted files are unaffected.* Access to protected content combines the ordinary NTFS authorization check with EFS cryptographic authorization. In a Windows domain, EFS recovery-agent policy provides a recovery mechanism, allowing *You have the ability to recover encrypted files in case the file owner leaves the company.* This centralized recovery capability avoids reliance solely on the departing user's private key. Finally, EFS uses certificates and keys automatically once policy is configured, which supports *Administrative efforts are minimum.* Microsoft documents EFS as an NTFS-based feature with transparent encryption and recovery support in its File Encryption documentation and describes NTFS access-control behavior in its file security and access-rights documentation.

QUESTION NO: 27

Adam works as a professional Computer Hacking Forensic Investigator. He has been called by the FBI to examine data of the hard disk, which is seized from the house of a suspected terrorist. Adam decided to acquire an image of the suspected hard drive. He uses a forensic hardware tool, which is capable of capturing data from IDE, Serial ATA, SCSI devices, and flash cards. This tool can also produce MD5 and CRC32 hash while capturing the data. Which of the following tools is Adam using?

A. Wipe MASSter

B. ImageMASSter 4002i

C. ImageMASSter Solo-3

D. FireWire DriveDock

ANSWER: C

Explanation:

ImageMASSter Solo-3 is the correct tool because it is a dedicated forensic acquisition device designed to create bitstream images from the broad mix of storage interfaces described, including IDE/PATA, Serial ATA, SCSI, and removable flash media. Its acquisition workflow includes integrity verification through calculated hash values, including MD5 and CRC32, while data is being captured. Those features directly match the scenario: the examiner needs a hardware-based imager that can handle both conventional hard disks and flash-card evidence while producing values that can later be used to demonstrate that the acquired image remains unchanged. In forensic practice, a cryptographic hash recorded at acquisition is a key part of documenting image integrity and supporting later verification of the evidence copy. NIST's guidance on integrating forensic techniques specifically describes preserving data and validating forensic copies as central acquisition activities: NIST SP 800-86, Guide to Integrating Forensic Techniques into Incident Response. The broader NIST Computer Forensics Tool Testing program also provides evaluation resources for forensic acquisition tools and the functions they perform: NIST CFTT Program.

QUESTION NO: 28

The promiscuous mode is a configuration of a network card that makes the card pass all traffic it receives to the central processing unit rather than just packets addressed to it. Which of the following tools works by placing the host system network card into the promiscuous mode?

A. Snort

B. THC-Scan

C. Sniffer

D. NetStumbler

ANSWER: C

Explanation:

Sniffer is correct because packet-sniffing tools capture and inspect network frames observed by a network interface. To collect traffic not specifically addressed to the local host, a sniffer commonly requests that the network adapter operate in promiscuous mode. In that mode, the adapter delivers a broader set of received frames to the operating system's packet-capture facility, enabling the analyst to examine network communications for forensic or troubleshooting purposes. This is the core operating concept implied by the term "sniffer": observing packets traversing the local network segment rather than only the host's own network conversations. Actual visibility still depends on network architecture; for example, on a switched Ethernet network, promiscuous mode alone does not provide traffic from other switch ports unless traffic is mirrored, tapped, or otherwise delivered to the capture interface. Wireshark's capture documentation describes promiscuous mode as a mechanism for capturing packets addressed to other machines, while noting that capture capabilities depend on the interface and environment. See the Wireshark User's Guide: Capture Options and the pcap manual documentation for further details on packet capture and promiscuous-mode operation.

QUESTION NO: 29

You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to print the super block and block the group information for the filesystem present on a system. Which of the following Unix commands can you use to accomplish the task?

A. e2fsck

B. dump

C. e2label

D. dumpe2fs

ANSWER: D

Explanation:

The correct command is `dumpe2fs`. It displays detailed metadata for an ext2, ext3, or ext4 filesystem, including the filesystem's superblock and the block-group descriptor information. This makes it useful during forensic examination or low-level filesystem administration when an analyst needs to identify properties such as the filesystem UUID, block size, inode size, feature flags, mount information, group layout, free-block and free-inode counts, and locations of inode tables and bitmaps.

For example, running `dumpe2fs /dev/sda1` reads the filesystem structures from the specified device and prints the primary superblock followed by information for each block group. The `-h` switch can be used when only the superblock information is needed, while the default output includes block-group details. Because these structures describe how data blocks and inodes are organized, the command is especially relevant to filesystem analysis and recovery workflows. The e2fsprogs manual documents that `dumpe2fs` prints the superblock and block-group information for a filesystem. See the dumpe2fs manual page and the e2fsprogs project resources.

QUESTION NO: 30

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He wants to test the effect of a virus on the We-are-secure server. He injects the virus on the server and, as a result, the server becomes infected with the virus even though an established antivirus program is installed on the server. Which of the following do you think are the reasons why the antivirus installed on the server did not detect the virus injected by John?

Each correct answer represents a complete solution. Choose all that apply.

A. The mutation engine of the virus is generating a new encrypted code.

B. The virus, used by John, is not in the database of the antivirus program installed on the server.

C. John has created a new virus.

D. John has changed the signature of the virus.

ANSWER: A B C D

Explanation:

Signature-based antivirus detection depends substantially on previously identified malware samples and stable, recognizable byte patterns. “The virus, used by John, is not in the database of the antivirus program installed on the server” is therefore a complete reason: an unknown or newly encountered sample may have no matching detection signature. “John has created a new virus” can produce the same zero-day condition, particularly before the sample has been submitted, analyzed, and incorporated into vendor detection content.

“The mutation engine of the virus is generating a new encrypted code” is also a complete reason. Polymorphic malware can alter its observable code representation, including encryption and decryptor routines, across infections while retaining its harmful function. This reduces the reliability of static signatures tied to a prior sample. Likewise, “John has changed the signature of the virus” describes modifying the malware’s detectable code characteristics so that a signature intended to identify an earlier variant may no longer match. These limitations are why modern endpoint protection combines signatures with behavioral, heuristic, reputation, and cloud-based analysis rather than relying on one detection method alone. CISA describes malware as software designed to compromise systems and emphasizes layered defensive practices in its malware guidance; Microsoft also documents how behavioral and telemetry-based investigation supports detection beyond static file indicators.

QUESTION NO: 31 - (SIMULATION)

SIMULATION

Fill in the blank with the appropriate file system.

Alternate Data Streams (ADS) is a feature of the_____ file system, which allows more than one data stream to be associated with a filename.

ANSWER: See the explanation for the answer

Explanation:

Answer: `NTFS`

Alternate Data Streams (ADS) are a feature of the `NTFS` (New Technology File System) file system. NTFS permits multiple data streams to be associated with a single filename, commonly referenced using the syntax `filename:streamname`.

QUESTION NO: 33

Which of the following file systems cannot be used to install an operating system on the hard disk drive? Each correct answer represents a complete solution. Choose two.

A. Windows NT file system (NTFS)

B. High Performance File System (HPFS)

C. Log-structured file system (LFS)

D. Compact Disc File System (CDFS)

E. Novell Storage Services (NSS)

ANSWER: C D

Explanation:

Log-structured file system (LFS) and **Compact Disc File System (CDFS)** are the intended selections. LFS is a specialized filesystem design in which modifications are written sequentially to a log rather than updated in place. It originated as a research-oriented Unix filesystem architecture and is not a conventional installation target supported by mainstream operating-system installers in the context of this question. Its purpose is to optimize write handling and crash recovery through log-based organization, rather than to provide the broadly supported boot-volume format expected for hard-disk OS installation. The original LFS design is described by UC Berkeley in The Design and Implementation of a Log-Structured File System.

CDFS is specifically designed for compact-disc media and represents the CD-ROM filesystem support used by Windows. Compact discs are optical media and are ordinarily read-only when distributed; CDFS therefore does not provide an installable, writable hard-disk filesystem for an operating system. Microsoft's filesystem documentation identifies CDFS as the format used for CD-ROM media; see Filesystem Functionality Comparison. These characteristics make LFS and CDFS unsuitable as hard-drive OS installation filesystems under the stated scenario.

QUESTION NO: 34

Which of the following directories in Linux operating system contains device files, which refers to physical devices?

A. /boot

B. /etc

C. /dev

D. /bin

ANSWER: C

Explanation:

`/dev` is the Linux filesystem directory that contains device nodes: special files through which user-space programs and the operating system interact with hardware and certain virtual devices. Examples include disk devices such as `/dev/sda` or `/dev/nvme0n1`, terminal devices such as `/dev/tty`, and pseudo-devices such as `/dev/null` and `/dev/zero`. These entries are not ordinary files holding device contents; instead, they provide an interface to device drivers in the kernel. Device nodes are commonly categorized as block devices, which support buffered, block-oriented access such as storage media, and character devices, which provide stream-oriented access such as terminals.

For forensic work, recognizing `/dev` is essential because acquisition tools may read a storage device directly through its corresponding device node. Modern Linux systems typically use `devtmpfs` for the basic device-node filesystem and `udev` to manage device naming and related metadata dynamically. The Linux Filesystem Hierarchy Standard identifies `/dev` as the location for device files, and the Linux kernel documentation describes the device model and userspace device-management mechanisms. See the Filesystem Hierarchy Standard: /dev and the Linux kernel documentation.

QUESTION NO: 35

You work as a professional Computer Hacking Forensic Investigator. A project has been assigned to you to investigate the DoS attack on a computer network of SecureEnet Inc. Which of the following methods will you perform to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. Look for unusual traffic on Internet connections and network segments.

B. Seize all computers and transfer them to the Forensic lab.

C. Look for core files or crash dumps on the affected systems.

D. Sniff network traffic to the failing machine.

ANSWER: A C D

Explanation:

“Look for unusual traffic on Internet connections and network segments,” “Look for core files or crash dumps on the affected systems,” and “Sniff network traffic to the failing machine” are appropriate complementary actions when investigating a denial-of-service incident. Network-level inspection establishes whether abnormal packet volume, connection rates, protocol patterns, source distribution, or traffic directed at a particular service corresponds to the reported outage. Capturing traffic near the affected host preserves evidence of the packets and sessions reaching that system, allowing an analyst to identify the attack pattern and assess whether the condition is ongoing.

Host-based crash artifacts are also valuable because resource exhaustion, malformed traffic, or exploitation attempts may cause a service, operating system component, or network application to fail. Core files and crash dumps can retain process state, fault information, loaded modules, and other forensic details that help correlate host failure with the observed network activity. Together, these measures support containment and recovery while collecting volatile evidence needed to characterize scope, impact, indicators, and timeline. NIST incident-handling guidance emphasizes collecting and analyzing relevant incident data throughout detection, analysis, containment, and recovery; see NIST SP 800-61 Rev. 2. CISA also describes network monitoring and packet analysis as important practices for understanding distributed denial-of-service activity: CISA DDoS resources.