DUMPSBOSS.

GIAC Certified Enterprise Defender

GIAC GCED

Version Demo

Total Demo Questions: 11

Total Premium Questions: 114

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Defensible Network Architecture	43
Topic 2, Network Security Monitoring	20
Topic 3, Endpoint Security Monitoring	20
Topic 4, Incident Response and Threat Hunting	28
Topic 5, Mix Questions	3
Total	114

QUESTION NO: 1

What is the BEST sequence of steps to remove a bot from a system?

A. Terminate the process, remove autoloading traces, delete any malicious files

B. Delete any malicious files, remove autoloading traces, terminate the process

C. Remove autoloading traces, delete any malicious files, terminate the process

D. Delete any malicious files, terminate the process, remove autoloading traces

ANSWER: A

Explanation:

Terminate the process, remove autoloading traces, delete any malicious files is the best sequence because remediation must first stop the bot's active execution. An active process can continue communicating with command-and-control infrastructure, perform malicious actions, and potentially recreate files or persistence mechanisms while cleanup is underway. Once execution has stopped, responders should remove the bot's autoloading traces, such as scheduled tasks, services, startup entries, registry run keys, login items, or other persistence mechanisms. This prevents the malware from restarting when the system, user session, or relevant service is restarted. The malicious executable and supporting files can then be deleted after their active execution and restart paths have been eliminated.

This order reflects a practical eradication workflow: stop the immediate threat, disable its ability to return, and then remove its remaining on-disk components. In a real incident, responders should also preserve appropriate evidence before destructive actions, validate that no additional persistence or related payloads remain, and monitor for recurrence after remediation. NIST describes eradication as eliminating malware and other compromised artifacts as part of incident handling, while CISA provides guidance for containing and recovering from malware incidents. See NIST SP 800-61 Rev. 2 and CISA Malware guidance.

QUESTION NO: 2

Requiring criminal and financial background checks for new employees is an example of what type of security control?

A. Detective Support Control

B. Detective Operational Control

C. Detective Technical Control

D. Detective Management Control

ANSWER: B

Explanation:

Detective Operational Control is correct because personnel background investigations are part of personnel security activities performed through organizational processes rather than through a software or hardware mechanism. Criminal-history and financial checks examine information about a prospective employee to identify indicators of risk, such as prior misconduct, fraud exposure, or circumstances that may warrant additional review before access is granted. This gives the activity a detective purpose: it discovers relevant security concerns from available records. It is also operational because the control is carried out by people and established personnel-security procedures, often involving human resources, security staff, and screening providers.

NIST identifies personnel security as an operational security-control area. Its Personnel Screening control specifically addresses screening individuals before authorizing access to systems and information, including suitability determinations and background investigations appropriate to the role and risk. The broader personnel-security requirements in federal information-security guidance likewise support screening personnel as an organizational operational activity. See NIST SP 800-53 Rev. 5 and FIPS 200.

QUESTION NO: 3

What is needed to be able to use taskkill to end a process on remote system?

A. Svchost.exe running on the remote system

B. Domain login credentials

C. Port 445 open

D. Windows 7 or higher on both systems

ANSWER: B

Explanation:

Credentials for an account authorized to manage processes on the remote computer are needed to use `taskkill` against a remote system. The command supports the `/s` parameter to identify the target computer and the `/u` and `/p` parameters to supply an account context when the current user's credentials are not appropriate. In an enterprise environment, this is commonly a domain account, which is why "domain login credentials" is often used as the shorthand answer. More precisely, the account must be recognized by the remote host and have sufficient rights to terminate the targeted process; an administrator-level account is normally used for this purpose. The command can also use the currently logged-on user's security context when that identity already has the required remote access and process-management permissions, so the essential requirement is authorized credentials rather than membership in a domain specifically. Microsoft's command reference documents the remote-system and alternate-user parameters for Taskkill at Taskkill. Microsoft also describes remote administration as requiring authenticated access and appropriate permissions in its Remote command documentation.

QUESTION NO: 4

What does the following WMIC command accomplish?

process where name='malicious.exe' delete

A. Removes the 'malicious.exe' process form the Start menu and Run registry key

B. Terminates all currently running process instances named 'malicious.exe'

C. Removes the executable 'malicious.exe' from the file system

D. Stops the 'malicious.exe' process from running and being restarted at the next reboot

ANSWER: B

Explanation:

The command terminates every currently running process instance whose executable name is `malicious.exe`. In WMIC, `process` is an alias for the WMI `Win32_Process` class. The `where name='malicious.exe'` clause filters the class instances to processes with that image name, and `delete` invokes the class's `Delete` method on each matching instance. For `Win32_Process`, the Delete method terminates the process, which ends its execution and causes the operating system to release the resources and handles owned by that process in the normal consequence of process termination.

This is a process-control action against running instances, so it is useful during incident response when an analyst needs to stop a known malicious executable that is active in memory. The command is name-based, meaning it can affect more than one matching process if multiple instances are running. WMIC itself is deprecated on current Windows versions, but the underlying WMI `Win32_Process.Delete` behavior remains the relevant mechanism. Microsoft documents the method as terminating the process in the Win32_Process Delete method documentation; the associated class and its properties are described in the Win32_Process documentation.

QUESTION NO: 5

Which of the following tools is the most capable for removing the unwanted add-on in the screenshot below?

A. ProcessExplorer

B. Taskkill

C. Paros

D. Hijack This

ANSWER: D

Explanation:

Hijack This is the most capable tool for this purpose because it was designed to enumerate and remediate browser-related persistence and configuration entries, including browser helper objects, toolbars, startup entries, and related registry settings. An unwanted browser add-on commonly persists through one or more of these locations, so effective removal requires identifying the configuration entry that causes the add-on to load and then removing or repairing that entry. HijackThis produces a detailed log of these browser and startup integration points and allows an analyst to select suspicious entries for remediation. This makes it especially useful when an add-on is unwanted, difficult to remove through the browser interface, or returns after a browser restart. Its results should be reviewed carefully, ideally against a known-good baseline or with supporting investigation, because the utility exposes both legitimate and malicious configuration items. The maintained HijackThis project documents its purpose as a diagnostic and log-analysis utility for system and browser settings: HijackThis GitHub repository. Microsoft also documents the browser extension model and browser helper objects that historically integrated with Internet Explorer: Microsoft Browser Helper Objects documentation.

QUESTION NO: 6

An internal host at IP address 10.10.50.100 is suspected to be communicating with a command and control whenever a user launches browser window. What features and settings of Wireshark should be used to isolate and analyze this network traffic?

A. Filter traffic using ip.src == 10.10.50.100 and tcp.srcport == 80, and use Expert Info

B. Filter traffic using ip.src == 10.10.50.100 and tcp.dstport == 53, and use Expert Info

C. Filter traffic using ip.src == 10.10.50.100 and tcp.dstport == 80, and use Follow TCP stream

D. Filter traffic using ip.src == 10.10.50.100, and use Follow TCP stream

ANSWER: D

Explanation:

Filtering traffic using `ip.src == 10.10.50.100`, and using Follow TCP Stream is the appropriate approach because it first isolates all outbound packets sent by the suspected internal host, without prematurely assuming that the suspected command-and-control communication uses a particular destination port. Browser-triggered activity may use standard web ports, but it can also use alternate ports; starting with the host source-address filter preserves visibility into the full set of connections initiated when the browser opens. Wireshark display filters use the `==` equality operator, and `ip.src` selects packets whose IPv4 source address matches the specified host. After identifying connections of interest by timing, destination, protocol, or unusual behavior, Follow TCP Stream reconstructs the bidirectional application conversation for the selected TCP flow. This enables an analyst to inspect HTTP requests and responses, headers, hostnames, redirects, commands, or other content available in the capture, and to correlate the stream with the browser-launch event. Wireshark

documents IP-address display filtering in its display-filter reference and explains stream reconstruction through Follow Stream in the User's Guide.

QUESTION NO: 7

What would a penetration tester expect to access after the following metasploit payload is delivered successfully?

Set PAYLOAD windows / shell / reverse _ tcp

A. VNC server session on the target

B. A netcat listener on the target

C. A meterpreter prompt on the target

D. A command prompt on the target

ANSWER: D

Explanation:

The correct result is **A command prompt on the target**. The `windows/shell/reverse_tcp` payload is a Windows reverse TCP shell payload. After it executes, the compromised Windows system initiates an outbound TCP connection back to the listener configured by the tester, typically using the specified `LHOST` and `LPORT` settings. When that reverse connection is received, Metasploit provides an interactive Windows command-shell session through which the tester can issue standard command-line commands in the security context of the exploited process.

This payload name is significant: `shell` denotes a conventional command shell, while `reverse_tcp` describes the connection direction and transport. Reverse shells are especially useful in assessments because outbound connections may be more likely to traverse network filtering than unsolicited inbound connections to a target. The session is returned to the Metasploit handler, allowing the tester to interact with the target's command interpreter and perform authorized post-exploitation validation. Metasploit's payload documentation distinguishes shell payloads from other payload families and explains payload selection and handler behavior. See the Rapid7 Metasploit payload documentation and the Metasploit documentation on how payloads work.

QUESTION NO: 8

Which statement below is the MOST accurate about insider threat controls?

A. Classification of information assets helps identify data to protect.

B. Security awareness programs have a minimal impact on reducing the insider threat.

C. Both detective and preventative controls prevent insider attacks.

D. Rotation of duties makes an insider threat more likely.

E. Separation of duties encourages one employee to control a great deal of information.

ANSWER: A

Explanation:

Classification of information assets helps identify data to protect. is the most accurate statement because an organization cannot apply proportionate insider-threat safeguards without first understanding what information it owns, where it resides, its sensitivity, and the business impact of unauthorized disclosure, modification, or destruction. A formal classification scheme assigns handling requirements to data—for example, access restrictions, encryption, retention, monitoring, and approved sharing methods—so that the strongest controls are directed toward the information whose compromise would have the greatest consequence.

For enterprise defenders, classification also provides essential context for insider-threat detection and response. It enables security teams to distinguish routine activity from potentially harmful access, such as an employee retrieving unusually large amounts of restricted intellectual property or customer data. Classification should be coupled with data inventory, ownership, least-privilege access decisions, and periodic review as information and business processes change. NIST's guidance on protecting controlled information emphasizes identifying and categorizing information so organizations can apply appropriate protection requirements. CISA likewise identifies data protection and the identification of critical assets as foundational components of an insider-threat mitigation program. See NIST SP 800-171 Rev. 3 and CISA Insider Threat Mitigation.

QUESTION NO: 9

An incident response team investigated a database breach, and determined it was likely the result of an internal user who had a default password in place. The password was changed. A week later, they discover another loss of database records. The database admin provides logs that indicate the attack came from the front-end web interface. Where did the incident response team fail?

A. They did not eradicate tools left behind by the attacker

B. They did not properly identify the source of the breach

C. They did not lock the account after changing the password

D. They did not patch the database server after the event

ANSWER: B

Explanation:

They did not properly identify the source of the breach. Changing the suspected internal user's default password addressed an initial hypothesis, but the subsequent database-record loss and web-interface logs show that the team had not established the actual intrusion path. Effective incident analysis requires responders to validate the evidence, determine the root cause and scope of compromise, and identify all affected systems and attack vectors before considering eradication complete. In this case, the front-end web interface may have provided the attacker with a continuing route to the database, such as through an application flaw, compromised web credentials, malicious server-side code, or an exposed administrative function. Because that access path remained available, changing only the database-related password did not remove the cause of the incident. NIST incident-response guidance emphasizes analysis to understand the nature and extent of an incident, followed by eradication actions that remove the cause and associated artifacts. See NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide. SANS also describes incident handling as a lifecycle in which identification and containment must be based on validated evidence: Incident Handler's Handbook.

QUESTION NO: 10

Which tasks would a First Responder perform during the Identification phase of Incident Response?

A. Verify the root cause of the incident and apply any missing security patches.

B. Install or reenable host-based firewalls and anti-virus software on suspected systems.

C. Search for sources of data and information that may be valuable in confirming and containing an incident.

D. Disconnect network communications and search for malicious executables or processes.

ANSWER: C

Explanation:

Search for sources of data and information that may be valuable in confirming and containing an incident is correct because identification (often called detection and analysis) is the stage in which responders determine whether an event is actually an incident, establish its likely scope and impact, and collect the information needed to support an informed response. A first responder reviews available evidence such as endpoint telemetry, SIEM alerts, authentication records, firewall and proxy logs, network-flow data, packet captures, threat-intelligence matches, and reports from users or system owners. These

sources help validate the suspected activity, identify affected assets and accounts, determine relevant indicators of compromise, and provide the context needed to make containment decisions. This work also requires preserving useful evidence and documenting observations so the incident can be escalated and handled consistently. NIST's incident-handling guidance describes detection and analysis as the process of validating precursors and indicators, analyzing incident-related data, and documenting findings before or alongside response actions. The SANS Incident Handler's Handbook likewise frames identification as recognizing and verifying an incident through analysis of alerts and other available information. See NIST SP 800-61 Rev. 2 and the SANS Incident Handler's Handbook.

QUESTION NO: 11

What is the primary benefit of sending endpoint, firewall, DNS, and authentication logs to a centralized log-management system?

A. Correlation of related events across multiple systems

B. Elimination of the need to synchronize system clocks

C. Prevention of all unauthorized network connections

D. Automatic removal of malware from endpoints

ANSWER: A

Explanation:

Correlation of related events across multiple systems is correct because a centralized platform collects records from different sources into a common location where analysts can search, normalize, retain, and correlate them. An incident that appears insignificant in one data source may become clear when related endpoint execution, DNS lookups, firewall connections, and authentication events are reviewed together.

Central collection also reduces reliance on logs stored only on a potentially compromised host and supports consistent retention, access control, alerting, and time-based investigation. For useful correlation, participating systems should use reliable time synchronization and produce sufficient contextual fields. NIST identifies centralized log management and event correlation as important practices for improving monitoring and incident response. See NIST SP 800-92, Guide to Computer Security Log Management.