Free Questions for 212-82 by actualtestdumps

Shared by George on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The IH&R team in an organization was handling a recent malware attack on one of the hosts connected to the organization's network. Edwin, a member of the IH&R team, was involved in reinstating lost data from the backup medi

a. Before performing this step, Edwin ensured that the backup does not have any traces of malware.

Identify the IH&R step performed by Edwin in the above scenario.

Options:

A- Eradication

B- Incident containment

C- Notification

D- Recovery

Answer:

D

Explanation:

Recovery is the IH&R step performed by Edwin in the above scenario. IH&R (Incident Handling and Response) is a process that involves identifying, analyzing, containing, eradicating, recovering from, and reporting on security incidents that affect an organization's network or system. Recovery is the IH&R step that involves restoring the normal operation of the system or network after eradicating the incident. Recovery can include reinstating lost data from the backup media, applying patches or updates, reconfiguring settings, testing functionality, etc. Recovery also involves ensuring that the backup does not have any traces of malware or compromise . Eradication is the IH&R step that involves removing all traces of the incident from the system or network, such as malware, backdoors, compromised files, etc. Incident containment is the IH&R step that involves implementing appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization. Notification is the IH&R step that involves informing relevant stakeholders, authorities, or customers about the incident and its impact.

Question 2

Question Type: MultipleChoice

Warren, a member of IH&R team at an organization, was tasked with handling a malware attack launched on one of servers connected to the organization's network. He immediately implemented appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization.

Identify the IH&R step performed by Warren in the above scenario.

Options:

A- Containment

B- Recovery

C- Eradication

D- Incident triage

Answer:

A

Explanation:

Containment is the IH&R step performed by Warren in the above scenario. IH&R (Incident Handling and Response) is a process that involves identifying, analyzing, containing, eradicating, recovering from, and reporting on security incidents that affect an organization's network or system. Containment is the IH&R step that involves implementing appropriate measures to stop the infection from spreading to other organizational assets and to prevent further damage to the organization . Containment can be done by isolating the affected system or network, blocking malicious traffic or communication, disabling or removing malicious accounts or processes, etc. Recovery is the IH&R step that involves restoring the normal operation of the system or network after eradicating the incident. Eradication is the IH&R step that involves removing all traces of the incident from the system or network, such as malware, backdoors, compromised files, etc. Incident triage is the IH&R step that involves prioritizing incidents based on their severity, impact, and urgency.

Question 3

Question Type: MultipleChoice

Nancy, a security specialist, was instructed to identify issues related to unexpected shutdown and restarts on a Linux machine. To identify the incident cause, Nancy navigated to a directory on the Linux system and accessed a log file to troubleshoot problems related to improper shutdowns and unplanned restarts.

Identify the Linux log file accessed by Nancy in the above scenario.

Options:

A- /var/log/secure

B- /var/log/kern.log

C- /var/log/boot.log

D- /var/log/lighttpd/

Answer:

C

Explanation:

/var/log/boot.log is the Linux log file accessed by Nancy in the above scenario. Linux is an open-source operating system that logs various events and activities on the system or network. Linux log files are stored in the /var/log directory, which contains different types of log files for different purposes. /var/log/boot.log is the type of log file that records events related to the booting process of the Linux system, such as loading drivers, services, modules, etc. /var/log/boot.log can help identify issues related to unexpected shutdowns and restarts on a Linux machine . /var/log/secure is the type of log file that records events related to security and authentication, such as logins, logouts, password changes, sudo commands, etc. /var/log/kern.log is the type of log file that records events related to the kernel, such as kernel messages, errors, warnings, etc. /var/log/lighttpd/ is the directory that contains log files related to the lighttpd web server, such as access logs, error logs, etc.

Question 4

Question Type: MultipleChoice

Tenda, a network specialist at an organization, was examining logged data using Windows Event Viewer to identify attempted or successful unauthorized activities. The logs analyzed by Tenda include events related to Windows security; specifically, log-on/log-off activities, resource access, and also information based on Windows system's audit policies.

Identify the type of event logs analyzed by Tenda in the above scenario.

Options:

A- Application event log

B- Setup event log

C- Security event log

D- System event log

Answer:

C

Explanation:

Security event log is the type of event log analyzed by Tenda in the above scenario. Windows Event Viewer is a tool that displays logged data about various events that occur on a Windows system or network. Windows Event Viewer categorizes event logs into different types based on their source and purpose. Security event log is the type of event log that records events related to Windows security; specifically, log-on/log-off activities, resource access, and also information based on Windows system's audit policies . Security event log can help identify attempted or successful unauthorized activities on a Windows system or network. Application event log is the type of event log that records events related to applications running on a Windows system, such as errors, warnings, or information messages. Setup event log is the type of event log that records events related to the installation or removal of software or hardware components on a Windows system. System event log is the type of event log that records events related to the operation of a Windows system or its components, such as drivers, services, processes, etc.

Question 5

Question Type: MultipleChoice

Leilani, a network specialist at an organization, employed Wireshark for observing network traffic. Leilani navigated to the Wireshark menu icon that contains items to manipulate, display and apply filters, enable, or disable the dissection of protocols, and configure user-specified decodes.

Identify the Wireshark menu Leilani has navigated in the above scenario.

Options:

A- Statistics

B- Capture

C- Main toolbar

D- Analyze

Answer:

B

Explanation:

Capture is the Wireshark menu that Leilani has navigated in the above scenario. Wireshark is a network analysis tool that captures and displays network traffic in real-time or from saved files. Wireshark has various menus that contain different items and options for manipulating, displaying, and analyzing network data. Capture is the Wireshark menu that contains items to start, stop, restart, or save a live capture of network traffic. Capture also contains items to configure capture filters, interfaces, options, and preferences . Statistics is the Wireshark menu that contains items to display various statistics and graphs of network traffic, such as packet lengths, protocols, endpoints, conversations, etc. Main toolbar is the Wireshark toolbar that contains icons for quick access to common functions, such as opening or saving files, starting or stopping a capture, applying display filters, etc. Analyze is the Wireshark menu that contains items to manipulate, display and apply filters, enable or disable the dissection of protocols, and configure user-specified decodes.

Question 6

Question Type: MultipleChoice

Anderson, a security engineer, was Instructed to monitor all incoming and outgoing traffic on the organization's network to identify any suspicious traffic. For this purpose, he employed an analysis technique using which he analyzed packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit.

Identify the type of attack signature analysis performed by Anderson in the above scenario.

Options:

A- Context-based signature analysis

B- Atomic-signature-based analysis

C- Composite-signature-based analysis

D- Content-based signature analysis

Answer:

D

Explanation:

Content-based signature analysis is the type of attack signature analysis performed by Anderson in the above scenario. Content-based signature analysis is a technique that analyzes packet header fields such as IP options, IP protocols, IP fragmentation flags, offset, and identification to check whether any fields are altered in transit. Content-based signature analysis can help detect attacks that manipulate packet headers to evade detection or exploit vulnerabilities . Context-based signature analysis is a technique that analyzes packet payloads such as application data or commands to check whether they match any known attack patterns or signatures. Atomic-signature-based analysis is a technique that analyzes individual packets to check whether they match any known attack patterns or signatures. Composite-signature-based analysis is a technique that analyzes multiple packets or sessions to check whether they match any known attack patterns or signatures.

Question 7

Question Type: MultipleChoice

Steve, a network engineer, was tasked with troubleshooting a network issue that is causing unexpected packet drops. For this purpose, he employed a network troubleshooting utility to capture the ICMP echo request packets sent to the server. He identified that certain packets are dropped at the gateway due to poor network connection.

Identify the network troubleshooting utility employed by Steve in the above scenario.

Options:

A- dnsenurn

B- arp

C- traceroute

D- ipconfig

Answer:

C

Explanation:

Traceroute is the network troubleshooting utility employed by Steve in the above scenario. Traceroute is a utility that traces the route of packets from a source host to a destination host over a network. Traceroute sends ICMP echo request packets with increasing TTL

(Time to Live) values and records the ICMP echo reply packets from each intermediate router or gateway along the path. Traceroute can help identify the network hops, latency, and packet loss between the source and destination hosts . Dnsenum is a utility that enumerates DNS information from a domain name or an IP address. Arp is a utility that displays and modifies the ARP (Address Resolution Protocol) cache of a host. Ipconfig is a utility that displays and configures the IP (Internet Protocol) settings of a host.

Question 8

Question Type: MultipleChoice

Jaden, a network administrator at an organization, used the ping command to check the status of a system connected to the organization's network. He received an ICMP error message stating that the IP header field contains invalid information. Jaden examined the ICMP packet and identified that it is an IP parameter problem.

Identify the type of ICMP error message received by Jaden in the above scenario.

Options:

A- Type =12

B- Type = 8

C- Type = 5

D- Type = 3

Answer:

A

Explanation:

Type = 12 is the type of ICMP error message received by Jaden in the above scenario. ICMP (Internet Control Message Protocol) is a protocol that sends error and control messages between network devices. ICMP error messages are categorized by types and codes, which indicate the cause and nature of the error. Type = 12 is the type of ICMP error message that indicates an IP parameter problem, which means that the IP header field contains invalid information . Type = 8 is the type of ICMP message that indicates an echo request, which is used to test the connectivity and reachability of a destination host. Type = 5 is the type of ICMP error message that indicates a redirect, which means that a better route to the destination host is available. Type = 3 is the type of ICMP error message that indicates a destination unreachable, which means that the destination host or network cannot be reached.

Question 9

Question Type: MultipleChoice

Ryleigh, a system administrator, was instructed to perform a full back up of organizational data on a regular basis. For this purpose, she used a backup technique on a fixed date when the employees are not accessing the system i.e., when a service-level down time is allowed a full backup is taken.

Identify the backup technique utilized by Ryleigh in the above scenario.

Options:

A- Nearline backup

B- Cold backup

C- Hot backup

D- Warm backup

Answer:

B

Explanation:

Cold backup is the backup technique utilized by Ryleigh in the above scenario. Cold backup is a backup technique that involves taking a full backup of data when the system or database is offline or shut down. Cold backup ensures that the data is consistent and not corrupted by any ongoing transactions or operations. Cold backup is usually performed on a fixed date or time when the service-level downtime is allowed or scheduled . Nearline backup is a backup technique that involves storing data on a medium that is not

immediately accessible, but can be retrieved within a short time. Hot backup is a backup technique that involves taking a backup of data while the system or database is online or running. Warm backup is a backup technique that involves taking a backup of data while the system or database is partially online or running.