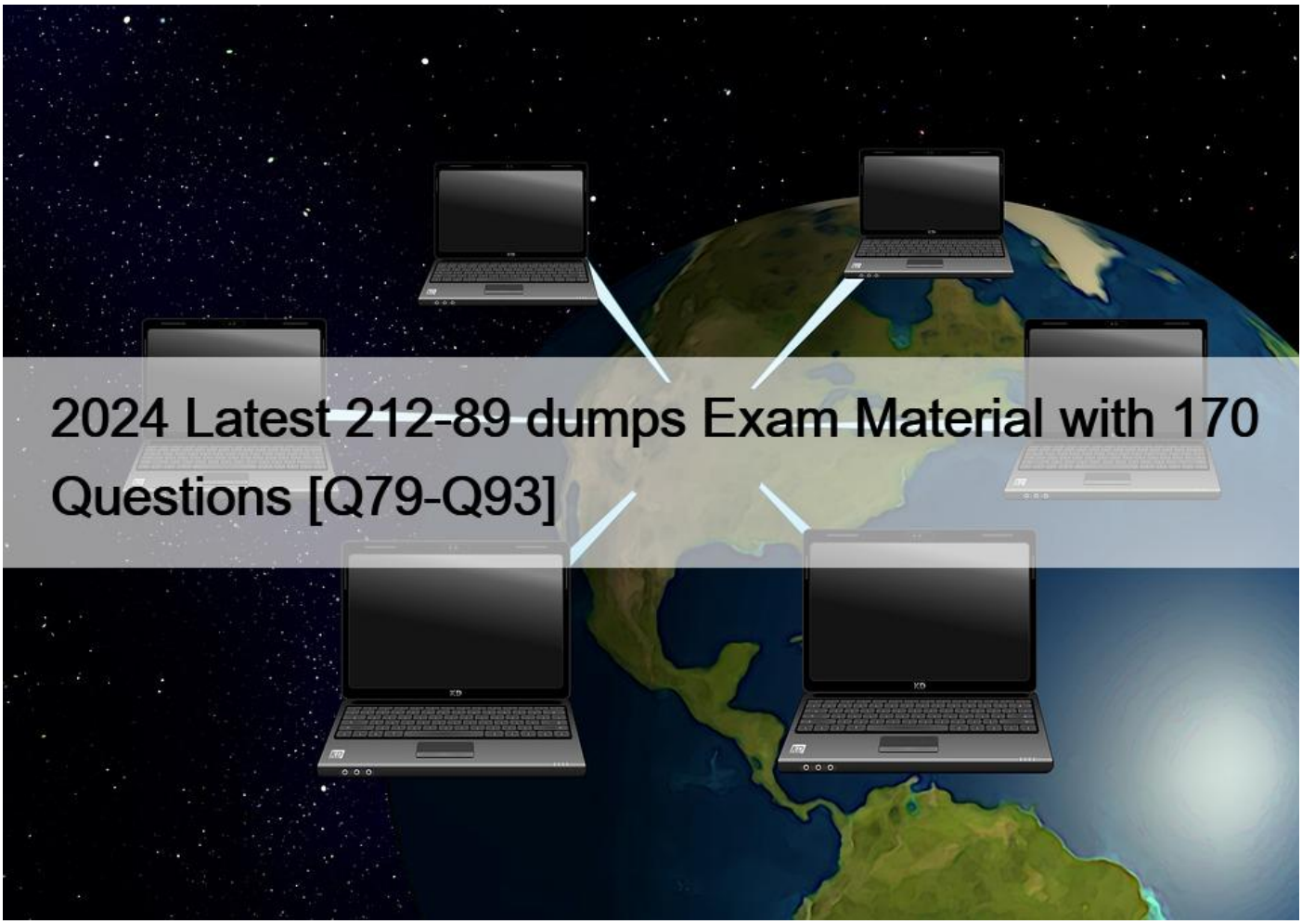
2024 Latest 212-89 dumps Exam Material with 170 Questions [Q79-Q93



2024 Latest 212-89 dumps Exam Material with 170 Questions EC-COUNCIL 212-89 Questions and Answers Guarantee you Oass the Test Easily

The ECIH v2 exam covers a range of topics related to incident handling and response, including incident management, incident response, and incident investigation. Candidates are required to have a deep understanding of the incident response process, including the ability to identify and classify incidents, gather evidence, and contain and mitigate the impact of incidents. 212-89 exam also covers the use of incident response tools and techniques, such as vulnerability scanning, network forensics, and threat intelligence.

NO.79 Chandler is a professional hacker who is targeting an organization called Technote. He wants to obtain important organizational information that is being transmitted between different hierarchies. In the process, he sniffs the data packets transmitted through the network and then analyzes them to gather packet details such as network, ports, protocols, devices, issues in network transmission, and other network specifications.

Which of the following tools can Chandler employ to perform packet analysis?
* IDA Pro
* BeEf
* Omni peek
* shARP

NO.80 Which of the following GPG 18 and Forensic readiness planning (SPF) principles states that “organizations should adopt a scenario based Forensic Readiness Planning approach that learns from experience gained within the business”?
* Principle 3
* Principle 5
* Principle 2
* Principle 7

NO.81 A US Federal Agency network was the target of a DoS attack that prevented and impaired the normal authorized functionality of the networks. According to the agency’s reporting timeframe guidelines, this incident should be reported within 2h of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate the activity.

Which incident category of US Federal Agency does this incident belong to?
* CAT 5
* CAT 6
* CAT 2
* CAT 1

NO.82 Which of the following tools helps incident handlers to view the file system, retrieve deleted data, perform timeline analysis, web artifacts, etc., during an incident response process?
* Autopsy
* netstat
* Process Explorer
* nblslal

NO.83 XYZ Inc. was affected by a malware attack and James, being the incident handling and response (IH&R) team personnel handling the incident, found out that the root cause of the incident is a backdoor that has bypassed the security perimeter due to an existing vulnerability in the deployed firewall. James had contained the spread of the infection and removed the malware completely. Now the organization asked him to perform incident impact assessment to identify the impact of the incident over the organization and he was also asked to prepare a detailed report of the incident.

Which of the following stages in IH&R process is James working on?
* Notification
* Evidence gathering and forensics analysis
* Post-incident activities
* Eradication

NO.84 Drake is an incident handler in Dark CLoud Inc. He is intended to perform log analysis in order to detect traces of malicious activities within the network infrastructure.

Which of the following tools Drake must employ in order to view logs in real time and identify malware propagation within the network?
* Splunk
* HULK
* Hydra

* LOIC

Splunk is a powerful tool for log analysis, capable of collecting, analyzing, and visualizing data from various sources in real time. For an incident handler like Drake, intending to detect traces of malicious activities within the network infrastructure, Splunk can efficiently parse large volumes of log data, enabling the identification of patterns and anomalies that may indicate malware propagation or other security incidents. Its real-time analysis capabilities make it an ideal tool for monitoring network activities and responding to incidents promptly.

NO.85 Ikeo Corp.hired an incident response team to assess the enterprise security. As part of the incident handling and response process, the IR team is reviewing the current se cunty policies implemented by the enterprise. The IR team finds that employees of the organization do not have any restrictions on Internet access: they are allowed to visit any site, download any appl cation, and access a computer or network from a remote location. Considering this as the main security threat, the IR team plans to change this policy as it can be easily exploited by attackers.

Which of the following security policies is the IR team planning to modify?

* Promiscuous policy
* Paranoid policy
* Permissive policy
* Prudent policy

NO.86 Removing or eliminating the root cause of the incident is called:

* Incident Eradication
* Incident Protection
* Incident Containment
* Incident Classification

NO.87 lkeo Corp. has hired an incident response team to assess the enterprise security. As a part of the incident handing and response process, the IR team is reviewing the current security policies implemented by the enterprise. The IR team finds out that employees of the organization do not have any restrictions on Internet access, which means that they are allowed to visit any site, download any application, and access a computer or a network from a remote location. Considering this as a main security threat, the IR team plans to change this policy as it can be easily exploited by the attackers. Identify the security policy that the IR team is planning to modify.

* Promiscuous pol cy
* Prudent policy
* Permissive policy
* Paranoid policy

NO.88 Farheen is an incident responder at reputed IT Firm based in Florida. Farheen was asked to investigate a recent cybercrime faced by the organization. As part of this process, she collected static data from a victim system.

She used DD tool command to perform forensic duplication to obtain an NTFS image of the original disk. She created a sector-by-sector mirror imaging of the disk and saved the output image file as image.dd.

Identify the static data collection process step performed by Farheen while collecting static data.

* Comparison
* Administrative consideration
* System preservation
* Physical presentatio

Farheen’s activity of using the DD tool to create a sector-by-sector mirror image of the original disk is an example of system preservation. This process is crucial in digital forensics for creating an exact copy of a storage device to ensure that the original data remains unchanged during the investigation. By making a forensic duplication, or image, of the disk, Farheen ensures that the static

data on the disk is preserved in its current state for thorough analysis, without altering the original evidence. This step allows investigators to work with a precise replica of the data, protecting the integrity of the original evidence.References:The Incident Handler (ECIH v3) certification materials discuss various methods and tools for data acquisition and preservation, highlighting the importance of system preservation in the initial stages of forensic analysis.

NO.89 Which of the following is a standard framework that provides recommendations for implementing information security controls for organizations that initiate, implement, or maintain information security management systems (ISMSs)?
* ISO/IEC 27002
* ISO/IEC 27035
* PCI DSS
* RFC 219G

ISO/IEC 27002 is a standard that provides best practice recommendations on information security controls for use by those responsible for initiating, implementing, or maintaining information security management systems (ISMSs). It covers areas such as risk assessment, human resource security, operational security, and communications security, among others, providing a framework for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS. ISO/IEC 27035 pertains to information security incident management, PCI DSS (Payment Card Industry Data Security Standard) deals with the security of cardholder data, and RFC 2196 is a guide for computer security incident response teams (CSIRTs), not a standard for implementing ISMSs.References:The ECIH v3 curriculum includes the study of various standards and frameworks that support information security management and governance, including ISO/IEC 27002, highlighting its role in guiding organizations in implementing effective security controls.

NO.90 The insider risk matrix consists of technical literacy and business process knowledge vectors. Considering the matrix, one can conclude that:
* If the insider’s technical literacy is low and process knowledge is high, the risk posed by the threat will be insignificant.
* If the insider’s technical literacy and process knowledge are high, the risk posed by the threat will be insignificant.
* If the insider’s technical literacy is high and process knowledge is low, the risk posed by the threat will be high.
* If the insider’s technical literacy and process knowledge are high, the risk posed by the threat will be high.

NO.91 CSIRT can be implemented at:
* Internal enterprise level
* National, government and military level
* Vendor level
* All the above

NO.92 While analyzing a file, Ryan discovered that an attacker used an anti-forensics method, wherein the attacker embedded a hidden message inside an image file.

What type of method is this?
* Program packers
* Golden ticket
* Steganography
* Password protection

NO.93 The insider risk matrix consists of technical literacy and business process knowledge vectors. Considering the

matrix, one can conclude that:
* If the insider’s technical literacy is low and process knowledge is high, the risk posed by the threat will be

insignificant.
* If the insider’s technical literacy and process knowledge are high, the risk posed by the threat will be

insignificant.
* If the insider’s technical literacy is high and process knowledge is low, the risk posed by the threat will be

high.
* If the insider’s technical literacy and process knowledge are high, the risk posed by the threat will be high.

Share Latest 212-89 DUMP Questions and Answers: https://www.actualtests4sure.com/212-89-test-questions.html]