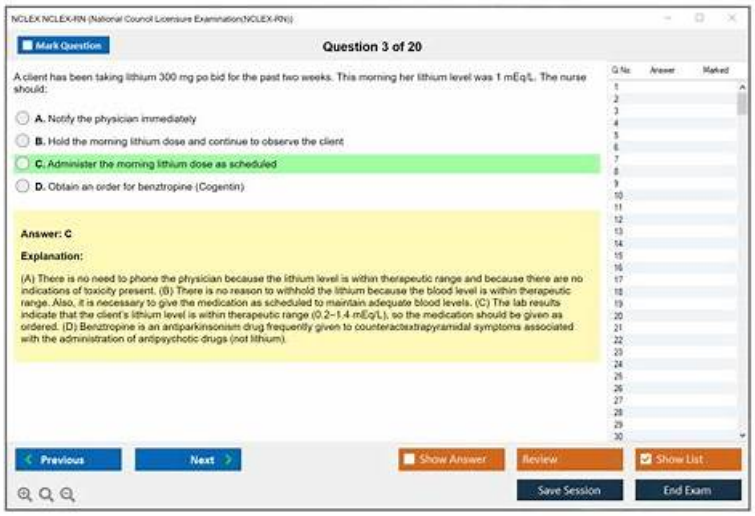
112-57 Braindumps, 112-57 Practice Test, 112-57 Real Dumps



P.S. Free 2026 EC-COUNCIL 112-57 dumps are available on Google Drive shared by Test4Cram: https://drive.google.com/open?id=10Vggk-nvpRecdoF6bLdGyYGrKZvk1g9p

It is a truth well-known to all around the world that no pains and no gains. There is another proverb that the more you plough the more you gain. When you pass the 112-57 exam which is well recognized wherever you are in any field, then acquire the 112-57 certificate, the door of your new career will be open for you and your future is bright and hopeful. Our 112-57 guide torrent will be your best assistant to help you gain your certificate.

EC-COUNCIL 112-57 Exam Syllabus Topics:

Topic	Details
Topic 1	• Investigating Email Crimes: This module covers the basics of email systems and the process of investigating suspicious emails to identify potential cybercrime evidence.
Topic 2	• Investigating Web Attacks: This module focuses on analyzing web application attacks through server logs and detecting malicious activities targeting web servers and applications.
Topic 3	• Computer Forensics Fundamentals: This module introduces the core concepts of computer forensics, including digital evidence, forensic readiness, and the role of investigators. It also explains legal and compliance requirements involved in forensic investigations.
Topic 4	• Network Forensics: This module introduces network forensic concepts, including event correlation, analyzing network logs, identifying indicators of compromise, and investigating network traffic.
Topic 5	• Linux and Mac Forensics: This module explains forensic analysis techniques for Linux and Mac systems. It focuses on analyzing system data, file systems, and memory to recover digital evidence.
Topic 6	• Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity.
Topic 7	• Computer Forensics Investigation Process: This module explains the phases of the forensic investigation process, including pre-investigation, investigation, and post-investigation. It also covers evidence integrity methods such as hashing and disk imaging.

>> Latest 112-57 Exam Book <<

100% Pass Quiz 2026 Useful EC-COUNCIL Latest 112-57 Exam Book

More and more people look forward to getting the 112-57 certification by taking an exam. However, the exam is very difficult for a lot of people. Especially if you do not choose the correct study materials and find a suitable way, it will be more difficult for you to pass the exam and get the EC-COUNCIL related certification. If you want to get the related certification in an efficient method, please choose the 112-57 learning dumps from our company. We can guarantee that the study materials from our company will help you pass the exam and get the certification in a relaxed and efficient method.

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) Sample Questions (Q66-Q71):

NEW QUESTION # 66
Bob, a network specialist in an organization, is attempting to identify malicious activities in the network. In this process, Bob analyzed specific data that provided him a summary of a conversation between two network devices, including a source IP and source port, a destination IP and destination port, the duration of the conversation, and the information shared during the conversation.
Which of the following types of network-based evidence was collected by Bob in the above scenario?

- A. Full content data
- B. Statistical data
- C. Session data
- D. Alert data

Answer: C

Explanation:
The description matchessession data, often calledflow records(for example, NetFlow/IPFIX-style evidence).
In network forensics, session/flow evidence summarizes a communication "conversation" between two endpoints using the5-tuple(source IP, source port, destination IP, destination port, and protocol) and typically addsstart/end time or duration,bytes/packets sent, and sometimes directionality. This allows an investigator to reconstructwho talked to whom, when, and for how long, even when packet payloads are unavailable (because of encryption, storage limits, or privacy constraints).
"Full content data" refers to complete packet captures (PCAP) containing payload bytes; that is far more detailed and would include the actual transmitted content, not just a summary. "Statistical data" is broader aggregate metrics (overall bandwidth trends, interface counters) and generally lacks per-conversation attribution. "Alert data" comes from IDS/IPS/SIEM detections and represents triggered events or signatures, not a neutral conversation summary.
Because Bob's evidence contains per-connection identifiers (IPs/ports) and conversation duration-typical of flow/session summaries-the correct evidence type isSession data (C).

NEW QUESTION # 67
Wesley, a professional hacker, deleted a confidential file in a compromised system using the "/bin/rm/" command to deny access to forensic specialists.
Identify the operating system on which Don has performed the file carving act.

- A. Mac OS
- B. Linux
- C. Windows
- D. Android

Answer: B

Explanation:
The command path /bin/rm is a hallmark of UNIX/POSIX-style operating systems, where core userland utilities are commonly stored under directories such as /bin, /sbin, and /usr/bin. The utility rm (remove) is the standard UNIX command used to delete directory entries that reference a file's data blocks on disk. This layout and command structure do not match Windows, whichuses different filesystem conventions (drive letters, backslashes, and Windows-native executables) and does not provide /bin/rm as a native path. Android, while Linux-kernel-based, typically exposes shell utilities through environments like /system/bin (and newer

systems may use toybox/busybox variants), not the classic /bin hierarchy expected on general-purpose UNIX systems. Between the remaining options, both Linux and macOS are UNIX-like and can include an rm command; however, in digital forensics training and examination contexts, the explicit reference to /bin/rm is most commonly used to indicate a Linux/UNIX command-line environment on a compromised host.
Therefore, the best single-choice answer from the provided options is Linux (D).

NEW QUESTION # 68
Cooper, a forensic analyst, was examining a RAM dump extracted from a Linux system. In this process, he employed an automated tool, Volatility Framework, to identify any malicious code hidden inside the memory.
Which of the following plugins of the Volatility Framework helps Cooper detect hidden or injected files in the memory?

- A. linux_malfind
- B. ip addr show
- C. linux_netstat
- D. nmap -sU localhost

Answer: A

Explanation:
In memory forensics, "hidden or injected" malicious code typically refers toprocess injection,code caves, unbacked executable mappings, or regions of memory that aremarked executablebut do not align with normal, file-backed program segments. The Volatility Framework provides specialized plugins to locate these suspicious patterns.linux_malfindis the plugin designed to detectpotentially injected codeby scanning a process's memory mappings for characteristics that commonly indicate malicious presence-such asexecutable anonymous mappings, unusual permissions (e.g., RWX), and memory regions that contain shellcode-like byte patterns. This is highly relevant when malware attempts to avoid disk artifacts by living in memory or by injecting payloads into legitimate processes.
By contrast,linux_netstatis used to enumerate network connections and sockets from memory (useful for C2 analysis), but it does not focus on injected code regions.ip addr showandnmap -sU localhostare live-system networking commands, not Volatility plugins, and they are not suitable for analyzing a captured RAM image.
Therefore, to detect hidden/injected malicious code in a Linux RAM dump using Volatility, the correct plugin islinux_malfind (A).

NEW QUESTION # 69
Given below is a regex signature used by security professionals for detecting an XSS attack:
/((%3C)|<)[