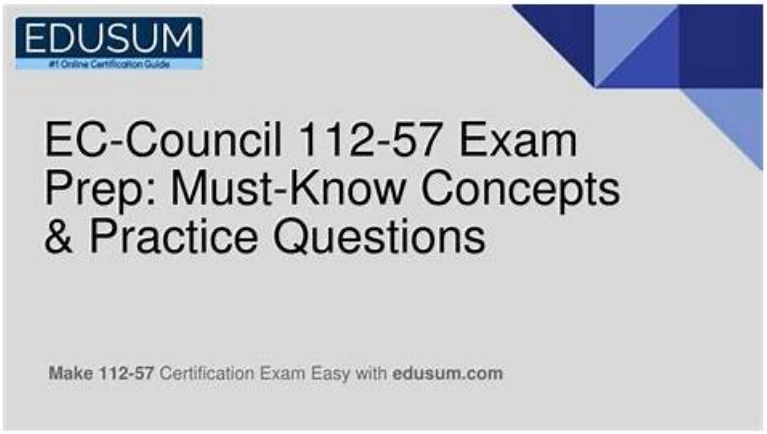
Choose EC-COUNCIL 112-57 Exam Questions for Successful Preparation



P.S. Free 2026 EC-COUNCIL 112-57 dumps are available on Google Drive shared by Lead2Passed: https://drive.google.com/open?id=1Sj9p3t87Kbhq1WdMTjVu8LBTglzK6kvR

Are you planning to attempt the EC-COUNCIL 112-57 exam of the 112-57 certification? The first hurdle you face while preparing for the EC-Council Digital Forensics Essentials (DFE) (112-57) exam is not finding the trusted brand of accurate and updated 112-57 exam questions. If you don't want to face this issue then you are at the trusted spot. Lead2Passed is offering actual and Latest 112-57 Exam Questions that ensure your success in the EC-COUNCIL 112-57 certification exam on your maiden attempt.

EC-COUNCIL 112-57 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• 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 3	• Defeating Anti-forensics Techniques: This module discusses anti-forensic methods used to hide or destroy evidence. It also explains techniques investigators use to detect hidden data and recover deleted or protected information.
Topic 4	• 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 5	• Windows Forensics: This module covers forensic investigation in Windows systems, including analysis of memory, registry data, browser artifacts, and file metadata to identify system and user activities.
Topic 6	• Dark Web Forensics: This module explains the investigation of dark web activities, including analyzing artifacts related to the Tor browser and identifying dark web usage on systems.
Topic 7	• Investigating Web Attacks: This module focuses on analyzing web application attacks through server logs and detecting malicious activities targeting web servers and applications.
Topic 8	• Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity.

Topic 9	• Investigating Email Crimes: This module covers the basics of email systems and the process of investigating suspicious emails to identify potential cybercrime evidence.
Topic 10	• Understanding Hard Disks and File Systems: This module covers disk structures, types of storage drives, and operating system boot processes. It also explains how investigators analyze file systems and recover deleted data.

>> Accurate 112-57 Prep Material <<

Free PDF EC-COUNCIL 112-57 First-grade Accurate EC-Council Digital Forensics Essentials (DFE) Prep Material

Constant improvements are the inner requirement for one person. As one person you can't be satisfied with your present situation and must keep the pace of the times. You should constantly update your stocks of knowledge and practical skills. So you should attend the certificate exams such as the test EC-COUNCIL certification to improve yourself and buying our 112-57 Latest Exam file is your optimal choice. Our 112-57 exam questions combine the real exam's needs and the practicability of the knowledge. The benefits after you pass the test EC-COUNCIL certification are enormous and you can improve your social position and increase your wage.

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) Sample Questions (Q39-Q44):

NEW QUESTION # 39
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. nmap -sU localhost
- C. ip addr show
- D. linux_netstat

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 # 40
An organization decided to strengthen the security of its network by studying and analyzing the behavior of attackers. For this purpose, Steven, a security analyst, was instructed to deploy a device to bait attackers.
Steven selected a solution that appears to contain very useful information to lure attackers and find their locations and techniques.
Identify the type of device deployed by Steven in the above scenario.

- A. Firewall
- B. Router
- C. Intrusion detection system

- D. Honeypot

Answer: D

Explanation:
Ahoneypotis a deliberately deployed decoy system or service designed toattract attackersby appearing valuable or vulnerable, thereby enabling defenders to observe malicious behavior in a controlled manner.
Digital forensics and incident response references describe honeypots as tools forthreat intelligence and evidence collection, because they can record interaction details such as connection sources, exploited services, commands executed, malware dropped, and attempted privilege escalation. This directly matches the scenario: Steven deployed something that "appears to contain very useful information" tolure attackersand help identify theirlocations and techniques. Honeypots are typically instrumented with extensive logging and monitoring, making them especially useful for building timelines, extracting indicators of compromise, and understanding adversary tactics, techniques, and procedures.
The other options do not align with the "bait attackers" goal. AnIDSprimarily detects and alerts on suspicious activity but is not intended to impersonate a valuable target. Afirewallenforces access control rules to block
/allow traffic, not entice attackers. Arouterforwards packets and provides network connectivity; it is not a deception platform.
Therefore, the device type described is aHoneypot (C).

NEW QUESTION # 41
Which of the following folders of macOS stores all the files, documents, applications, library folders, etc.
pertaining to a particular user?

- A. Finder
- B. Home Directory
- C. Spotlight
- D. Time Machine

Answer: B

Explanation:
In macOS, each user account is assigned aHome Directorythat serves as the primary container for that user's data and profile-specific configuration. This directory typically resides under/Users/<username>/and includes standard subfolders such asDesktop,Documents,Downloads,Pictures,Movies,Music, and crucially the user' sLibraryfolder (~/Library). From a digital forensics standpoint, the Home Directory is one of the most important evidence locations because it holds user-generated content and a large volume of user activity artifacts: application preferences and settings (plist files), browser data, caches, saved state, key application databases, recent items, and other per-user traces. Although some applications are installed system-wide under /Applications, macOS also supports per-user application storage and extensive per-user data under the Home Directory's Library structure.
The other options are not user-data containers.Spotlightis a search/indexing service (it creates indexes, not a user's complete data store).Time Machineis a backup mechanism that stores versioned backups rather than the live per-user working directory.Finderis the graphical file manager, not a storage folder. Therefore, the folder that stores files and user-specific libraries for a particular user is theHome Directory (D).

NEW QUESTION # 42
Below is an extracted Apache error log entry.
"[Wed Aug 28 13:35:38.878945 2020] [core:error] [pid 12356:tid 8689896234] [client 10.0.0.8] File not found: /images/folder/pic.jpg" Identify the element in the Apache error log entry above that represents the IP address from which the request was made.

- A. 0
- B. 13:35:38.878945
- C. 10.0.0.8
- D. 1

Answer: C

Explanation:
Apache error logs record key metadata about server-side events in a structured format that is widely used in web attack investigations. In the provided entry, each bracketed field represents a specific attribute: the first bracket contains the timestamp, the

next contains the module and severity (e.g.,core:error), then the process
/thread identifiers (pidandtid), followed by the client identifier. The client field is explicitly labeled[client ...], and it captures thesource IP address(or sometimes hostname) that initiated the HTTP request which resulted in the logged error.
Here,[client 10.0.0.8]indicates that the request originated from IP address10.0.0.8. This is the critical element investigators use to attribute suspicious activity (such as probing for missing files, scanning directories, or exploitation attempts) to a specific network source. The other values are not the client IP:13:35:38.878945is the time component of the timestamp,12356is the Apache process ID, and8689896234is the thread ID handling the request. Therefore, the IP address from which the request was made is10.0.0.8 (C).

NEW QUESTION # 43
Sam is working as a loan agent for a financial institution. He frequently receives a number of emails from clients providing their personal details for loan approval. As these emails contain sensitive data, Sam had set up a feature that directly downloads the emails on his device without storing a copy on the mail server. Which of the following protocols provides the above-discussed email features?

- A. SHA-1
- B. POP3
- C. SNMP
- D. ICMP

Answer: B

Explanation:
The scenario describes an email-retrieval configuration in which messages aredownloaded to a client device andnot retained on the server. This behavior aligns withPOP3 (Post Office Protocol v3), a legacy but widely referenced mail access protocol that retrieves email from a server mailbox to a local client. In standard POP3 operation, the client authenticates to the mail server, issues retrieval commands (e.g., to list and download messages), and may then issue a delete command so that downloaded messages are removed from the server mailbox. Digital forensics references commonly contrast POP3 with IMAP:IMAP is designed for server-side mailbox synchronization and typically leaves mail stored on the server, whereas POP3 is oriented towardclient-side storageand supports workflows where server copies are not preserved after download. The other options are unrelated to email retrieval:SHA-1is a cryptographic hash function used for integrity checks,ICMPsupports network diagnostics and control messaging, andSNMPis used for network device management and monitoring. From an investigative standpoint, POP3 usage can reduce server-resident evidence and shift evidentiary value tolocal artifacts(mail client databases, cache, OS traces, backups), which is consistent with the intent described in the question.

NEW QUESTION # 44
.....

Once you have used our 112-57 exam training guide in a network environment, you no longer need an internet connection the next time you use it, and you can choose to use 112-57 exam training at your own right. Our 112-57 exam training do not limit the equipment, do not worry about the network, this will reduce you many learning obstacles, as long as you want to use 112-57 Test Guide, you can enter the learning state. And you will find that our 112-57 training material is the best exam material for you to pass the 112-57 exam.

- Pass Guaranteed 2026 EC-COUNCIL 112-57: EC-Council Digital Forensics Essentials (DFE) –High-quality Accurate Prep Material □ Search for { 112-57 } and download exam materials for free through ⇛ www.examcollectionpass.com ⇚ □ □112-57 Reliable Test Materials
- Valid Accurate 112-57 Prep Material - Pass 112-57 Exam □ Search for ➤ 112-57 □ and download it for free immediately on ➽ www.pdfvce.com □ ✈112-57 Valid Exam Testking
- EC-COUNCIL Accurate 112-57 Prep Material - www.prepawayete.com - Leader in Qualification Exams - Trusted 112-57 Exam Resource □ Simply search for { 112-57 } for free download on { www.prepawayete.com } □Latest 112-57 Exam Bootcamp
- Valid Accurate 112-57 Prep Material - Pass 112-57 Exam □ Go to website □ www.pdfvce.com □ open and search for [112-57] to download for free □112-57 Latest Exam Dumps
- 112-57 Valid Exam Testking □ 112-57 Test Dumps Free □ New 112-57 Braindumps Sheet □ Simply search for { 112-57 } for free download on 「 www.dumpsquestion.com 」 □112-57 Reliable Exam Questions
- sashaubfy357232.bcbloggers.com, mysocialguides.com, bookmarkboom.com, rotatesites.com, alvinwjom055287.wikicarrier.com, deniseivr912718.ziblogs.com, bookmarkingalpha.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, emilyeddq657531.elbloglibre.com, skillplus.lk, Disposable vapes

BTW, DOWNLOAD part of Lead2Passed 112-57 dumps from Cloud Storage: https://drive.google.com/open?id=1Sj9p3t87Kbhq1WdMTjVu8LBTglzK6kvR