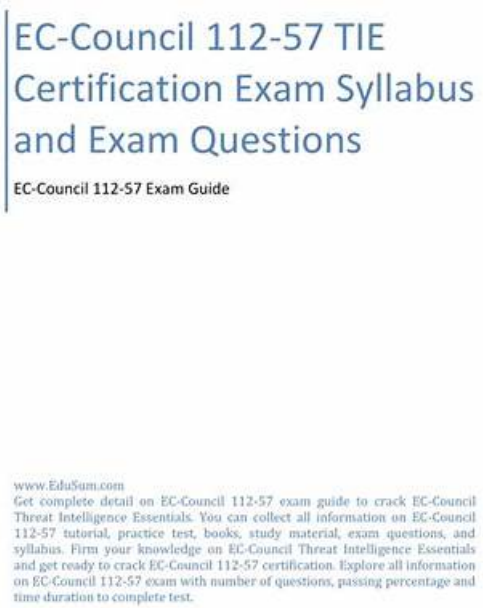
Newest 112-57 Interactive Practice Exam - Pass 112-57 Exam Easily



DOWNLOAD the newest PracticeVCE 112-57 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1dIONNaM0IgacASlT6ctGbP3WUujKXw16

Our 112-57 guide torrent will be the best choice for you to save your time. Because our products are designed by a lot of experts and professors in different area, our 112-57 exam questions can promise twenty to thirty hours for preparing for the exam. If you decide to buy our 112-57 test guide, which means you just need to spend twenty to thirty hours before you take your exam. By our 112-57 Exam Questions, you will spend less time on preparing for exam, which means you will have more spare time to do other thing. So do not hesitate and buy our 112-57 guide torrent.

EC-COUNCIL 112-57 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity.
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	• Data Acquisition and Duplication: This module focuses on methods for collecting and duplicating digital evidence. It explains acquisition techniques, formats, and procedures used to create forensic images and capture system memory.
Topic 5	• Investigating Web Attacks: This module focuses on analyzing web application attacks through server logs and detecting malicious activities targeting web servers and applications.
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	• 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 8	• Investigating Email Crimes: This module covers the basics of email systems and the process of investigating suspicious emails to identify potential cybercrime evidence.

112-57 Practice Exam Materials: EC-Council Digital Forensics Essentials (DFE) and 112-57 Study Guide - PracticeVCE

In order to help these people who have bought the 112-57 study materials of our company, There is a team of expert in our company, which is responsible to renovate and update the 112-57 study materials provided by our company. We are going to promise that we will have a lasting and sustainable cooperation with customers who want to buy the 112-57 Study Materials from our company. If you decide to buy our 112-57 study materials, you will never miss any important information. In addition, we can promise the updating system is free for you.

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) Sample Questions (Q11-Q16):

NEW QUESTION # 11
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. Windows
- B. Android
- C. Mac OS
- D. Linux

Answer: D

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 # 12

Which of the following Tor relay nodes in the Tor circuit is designed to transfer data in an encrypted format?

- A. Middle relay
- B. Exit relay
- C. Entry relay
- D. Guard relay

Answer: A

Explanation:
In a standard Tor circuit, a client typically builds a three-hop path:Entry/Guard # Middle # Exit. Tor uses onion routing, where the client wraps the payload in multiple encryption layers-one for each hop. Each relay removes (decrypts) only its own layer to learn thenext hop, but not the complete route or the original payload in the clear. Themiddle relayis specifically positioned toforward traffic between the entry/guard and the exit while it remains onion-encrypted end-to-end within the Tor network. Because it neither connects to the user's local network (like the entry/guard) nor to the public destination (like the exit), its primary role isencrypted transit/forwarding, helping break the linkage between source and destination. By contrast, theexit relayis where traffic leaves Tor; unless the application layer uses TLS/HTTPS, the exit may deliver data to the destination inunencryptedform on the open Internet. Theentry/guardprotects against certain traffic-correlation risks by being stable, but it is not uniquely "the" encrypted-transfer node. Therefore, the best single answer isMiddle relay (D).

NEW QUESTION # 13
James, a forensic specialist, was appointed to investigate an incident in an organization. As part of the investigation, James is attempting to identify whether any external storage devices are connected to the internal systems. For this purpose, he employed a utility to capture the list of all devices connected to the local machine and removed suspicious devices.
Identify the tool employed by James in the above scenario.

- A. ESEDatabaseView
- B. PromiscDetect
- C. DriveLetterView
- D. ProcDump

Answer: C

NEW QUESTION # 14
Kane, an investigation specialist, was appointed to investigate an incident in an organization's network. In this process, Kane executed a command and identified that a network interface is running in the promiscuous mode and is allowing all incoming packets without any restriction.
In the above scenario, which of the following commands did Kane use to check whether the network interface is set to the promiscuous mode?

- A. netstat -i
- B. ifconfig <interface name>
- C. ipconfig <interface name>
- D. nmap -sT localhost

Answer: B

Explanation:
Promiscuous mode is a network interface configuration in which the NIC passesall observed framesto the operating system, not only frames addressed to that host's MAC address. In investigations, this matters because promiscuous mode is commonly enabled bypacket sniffers, certain intrusion tools, or misconfigured monitoring software, and it can indicate covert traffic capture on a host. On UNIX/Linux systems, the traditional command used to view interface flags and status isifconfig < interface name>. When an interface is set to promiscuous mode,ifconfigdisplays aPROMISCflag in the interface's status line, allowing an investigator to confirm whether the NIC is accepting all frames. This directly matches Kane's goal of checking if the interface is running in promiscuous mode.
The other commands do not provide this specific interface flag.nmap -sT localhostscans for open TCP ports, not interface modes.ipconfigis a Windows command (and does not take an interface name in that form to show PROMISC status), and it primarily reports IP configuration.netstat -ishows network interface statistics (packets, errors, drops) but typically does not explicitly indicate promiscuous mode. Therefore, the correct command isifconfig <interface name> (C).

NEW QUESTION # 15
Which of the following standards and criteria version of SWGDE mandates that any action with the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner?

- A. Standards and Criteria 1.7
- B. Standards and Criteria 1.1
- C. Standards and Criteria 1.5
- D. Standards and Criteria 1.3

Answer: A

Explanation:
The statement in the question matchesSWGDE Principle 1, Standards and Criteria 1.7, which explicitly requires thatany action that could alter, damage, or destroy original digital evidence must be performed by qualified personnel in a forensically sound manner. In digital forensics doctrine, this requirement exists because digital evidence is highly fragile: routine interactions (booting a system, opening a file, connecting storage, running commands) can change timestamps, overwrite unallocated space, modify logs, or trigger encryption/key rotation. SWGDE's emphasis on "qualified persons" and "forensically sound manner" aligns with core evidentiary expectations: minimizing changes to original media, using controlled and repeatable methods (e.g., write-blocking, validated imaging, documented procedures), and ensuring actions are defensible under scrutiny.
Options 1.1, 1.3, and 1.5 relate to broader quality and procedural requirements (quality systems, SOP review, appropriate tools), but they do not contain the specific mandate about potentially altering original evidence.
The exact phrasing about alteration/damage/destruction and qualified handling is associated withStandards and Criteria 1.7, makingBthe correct choice.

NEW QUESTION # 16
.....

Many candidates find the EC-Council Digital Forensics Essentials (DFE) (112-57) exam preparation difficult. They often buy expensive study courses to start their EC-Council Digital Forensics Essentials (DFE) (112-57) certification exam preparation. However, spending a huge amount on such resources is difficult for many EC-COUNCIL 112-57 Exam applicants. The latest EC-COUNCIL 112-57 exam dumps are the right option for you to prepare for the EC-Council Digital Forensics Essentials (DFE) (112-57) certification test at home.