

Latest 112-57 Reliable Exam Pattern, Latest 112-57 Test Cram

PEARSON EXAM CRAM NCLEX RN TEST 1 MED SURG QNS & ANS LATEST UPDATE 2024/2025 GRADED A+

A client with ascites is scheduled for a paracentesis. Which instruction should be given to the client before the procedure?

- a "You will need to lay flat during the procedure."
- b. "You need to empty your bladder before the procedure."
- c. "You will be asleep during the procedure."
- d. "The doctor will inject a medication during the procedure." - CORRECT ANSWERS b. "You need to empty your bladder before the procedure."

A client's lab values reveal Hgb 12.6, WBC 6500cu.mm, K+ 1.9, uric acid 7.0, Na+ 136, and platelets 178,000cu.mm. The nurse evaluates that the client is experiencing which of the following?

- Hypernatremia
- b Hypokalemia
- Myelosuppression
- Leukopenia - CORRECT ANSWERS b Hypokalemia

Due to a high census, it has been necessary for a number of clients to be transferred to other units within the hospital. Which client should be transferred to the postpartum unit?

- a A 66-year-old female with gastroenteritis
- b A 40-year-old female with a hysterectomy
- c A 27-year-old male with severe depression
- d A 28-year-old male with ulcerative colitis - CORRECT ANSWERS b A 40-year-old female with a hysterectomy

Before administering Theo-Dur (theophylline), the nurse should check the patient's:

- a output
- b Blood pressure
- c Pulse
- d Temperature - CORRECT ANSWERS c Pulse

P.S. Free & New 112-57 dumps are available on Google Drive shared by NewPassLeader: <https://drive.google.com/open?id=1two2U3bRUDnAxnrkg2KgVwy66GbQJYRd>

Our EC-Council Digital Forensics Essentials (DFE) guide torrent is equipped with time-keeping and simulation test functions, it's of great use to set up a time keeper to help adjust the speed and stay alert to improve efficiency. Our expert team has designed a high efficient training process that you only need 20-30 hours to prepare the exam with our 112-57 Certification Training. With an overall 20-30 hours' training plan, you can also make a small to-do list to remind yourself of how much time you plan to spend in a day with 112-57 test torrent.

EC-COUNCIL 112-57 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none"> • 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 2	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> Investigating Email Crimes: This module covers the basics of email systems and the process of investigating suspicious emails to identify potential cybercrime evidence.
Topic 4	<ul style="list-style-type: none"> Network Forensics: This module introduces network forensic concepts, including event correlation, analyzing network logs, identifying indicators of compromise, and investigating network traffic.
Topic 5	<ul style="list-style-type: none"> 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 6	<ul style="list-style-type: none"> 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.
Topic 7	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 9	<ul style="list-style-type: none"> Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity.
Topic 10	<ul style="list-style-type: none"> 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.

>> 112-57 Reliable Exam Pattern <<

Valid EC-COUNCIL 112-57 Questions: 100% Authentic [2026]

Most people are nervous and anxious to take part in the 112-57 exam for the first time. Then it is easy for them to make mistakes. So it is important to get familiar with the real test environment. Also, the real test environment of the 112-57 Study Materials can help you control time. After all, you must submit your practice in limited time in 112-57 practice materials. Trust in our 112-57 training guide, and you will get success for sure.

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) Sample Questions (Q75-Q80):

NEW QUESTION # 75

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

Answer: C

Explanation:

In memory forensics, "hidden or injected" malicious code typically refers to process injection, code caves, unbacked executable mappings, or regions of memory that are marked executable but do not align with normal, file-backed program segments. The Volatility Framework provides specialized plugins to locate these suspicious patterns. `linux_malfind` is the plugin designed to detect potentially injected code by scanning a process's memory mappings for characteristics that commonly indicate malicious presence—such as executable 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_netstat` is used to enumerate network connections and sockets from memory (useful for C2 analysis), but it does not focus on injected code regions. `ip addr show` and `nmmap -sU localhost` are 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 is `linux_malfind` (A).

NEW QUESTION # 76

Which of the following tools helps forensic experts analyze user activity in the Microsoft Edge browser?

- A. `BrowsingHistoryView`
- B. `ChromeHistoryView`
- C. `MZCacheView`
- D. `MZHistoryView`

Answer: A

Explanation:

In Windows forensics, analyzing Microsoft Edge user activity commonly involves extracting and correlating browser artifacts such as visited URLs, visit counts, timestamps, download references, and cached content indicators. A practical forensic approach is to use a tool that can parse and normalize history artifacts across multiple browsers, because investigations often require comparing activity between Edge and other installed browsers on the same workstation. `BrowsingHistoryView` is designed specifically for that purpose: it aggregates browsing history from different browsers and presents it in a unified timeline-style view, which supports rapid triage and cross-validation of user activity.

By contrast, `MZHistoryView` and `MZCacheView` are associated with Mozilla-family artifacts (history and cache), making them appropriate for Firefox-related examinations rather than Edge. `ChromeHistoryView` is specialized for Google Chrome history databases and does not target Edge artifacts as its primary source. In forensic workflow terms, a multi-browser history tool is valuable because it helps identify patterns such as repeated access to specific domains, time windows of browsing activity, and correlation with other Windows artifacts (prefetch, jump lists,

NEW QUESTION # 77

A forensic investigator is collecting volatile data such as system information and network information present in the registries, cache, DLLs, and RAM of digital devices through its normal interface.

Identify the data acquisition method the investigator is performing.

- A. Live acquisition
- B. Static acquisition
- C. Non-volatile data acquisition
- D. Dead acquisition

Answer: A

Explanation:

The scenario describes the investigator collecting volatile artifacts—specifically information in RAM, active DLLs, system and network state, and transient data held in cache and similar runtime locations—through the device's normal interface while the system is running. In digital forensics documentation, this is the defining characteristic of live acquisition (also called live response). Live acquisition is performed when the system remains powered on so that investigators can capture evidence that would be lost on shutdown, such as running processes, open network connections, logged-on sessions, loaded modules/DLLs, encryption keys, and portions of registry data that exist in memory or are actively changing.

By contrast, static acquisition and dead acquisition are conducted when the system is powered off (or the evidence drive is imaged outside the running OS), focusing primarily on persistent storage such as disk sectors and file system structures. Non-volatile data acquisition refers to collecting persistent data stored on media (e.g., files on disk), which does not match the emphasis on RAM and other volatile components in the question. Because the investigator is explicitly collecting volatile data from a running system via its normal interface, the correct method is live acquisition (A).

NEW QUESTION # 78

Bob, a professional hacker, targeted an organization to launch attacks. Bob gathered information such as network topology and a list of live hosts. Based on the collected information, he launched further attacks over the organization's network.

Identify the type of network attack Bob initiated on the target organization in the above scenario.

- A. Buffer overflow
- B. Session hijacking
- C. Enumeration
- D. Data modification

Answer: C

Explanation:

The activity described—collecting network topology details and compiling a list of live hosts—matches the reconnaissance phase commonly referred to as enumeration. In digital forensics and incident response documentation, enumeration is the systematic process of discovering and extracting information about a target environment to support later exploitation. It typically follows (or overlaps with) scanning and includes identifying active IP addresses, reachable systems, open ports/services, device roles, OS fingerprints, domain information, shared resources, user/group details, and routing or segmentation clues that reveal how the network is structured.

This information is then used to plan "further attacks," such as targeting exposed services, choosing exploit paths, locating high-value systems, and selecting lateral movement routes. From a forensic standpoint, enumeration attempts often leave traces in firewall logs, IDS alerts, and endpoint artifacts (e.g., bursts of connection attempts across many hosts/ports, ICMP echo sweeps, ARP discovery on local segments, and repeated DNS queries).

The other options do not fit: data modification involves altering data integrity; session hijacking targets active sessions/tokens; and buffer overflow is an exploitation technique against vulnerable software, not the information-gathering step described. Therefore, the correct answer is Enumeration (C).

NEW QUESTION # 79

Bob, a forensic investigator, is investigating a live Windows system found at a crime scene. In this process, Bob extracted subkeys containing information such as SAM, Security, and software using an automated tool called FTK Imager. Which of the following Windows Registry hives' subkeys provide the above information to Bob?

- A. HKEY_CURRENT_CONFIG
- B. HKEY_CLASSES_ROOT
- C. HKEY_LOCAL_MACHINE
- D. HKEY_CURRENT_USER

Answer: C

Explanation:

In Windows forensics, the Registry is organized into logical root keys ("hives") that aggregate configuration and security data. The items named in the question—SAM, SECURITY, and SOFTWARE—are system-wide registry hives stored on disk (typically under the system's configuration directory) and loaded at runtime under HKEY_LOCAL_MACHINE (HKLM). Investigators rely on these hives because they contain high-value evidence: the SAM hive stores local account database information (including user and group identifiers and credential-related material), the SECURITY hive holds system security policy and LSA-related settings, and the SOFTWARE hive contains installed software, application configuration, and many operating system settings relevant for program execution and persistence analysis.

Tools like FTK Imager can extract these hives (or their live-memory representations) during triage to preserve volatile context and enable offline parsing while maintaining evidentiary integrity. The other root keys do not match these specific hives: HKEY_CURRENT_USER is per-user profile data, HKEY_CURRENT_CONFIG reflects current hardware profile, and HKEY_CLASSES_ROOT is primarily file association/COM class mapping (largely derived from HKLM\Software\Classes and HKCU\Software\Classes). Therefore, the correct hive root that provides SAM, SECURITY, and SOFTWARE subkeys is HKEY_LOCAL_MACHINE (C).

NEW QUESTION # 80

.....

As for the 112-57 study materials themselves, they boost multiple functions to assist the learners to learn the study materials efficiently from different angles. For example, the function to stimulate the exam can help the exam candidates be familiar with the atmosphere and the pace of the Real 112-57 Exam and avoid some unexpected problem occur. Briefly speaking, our 112-57 training guide gives priority to the quality and service and will bring the clients the brand new experiences and comfortable feelings to pass the 112-57 exam.

Latest 112-57 Test Cram: <https://www.newpassleader.com/EC-COUNCIL/112-57-exam-preparation-materials.html>

- Reliable 112-57 Exam Book □ 112-57 Certification Dump □ New 112-57 Test Syllabus □ Enter □ www.pdf.dumps.com □ and search for ➡ 112-57 □ to download for free □ 112-57 Exam Tips
- 112-57 Latest Demo □ Reliable 112-57 Exam Book □ New 112-57 Mock Exam □ Enter ➡ www.pdfvce.com □□□ and search for ➡ 112-57 □ to download for free □ 112-57 New Learning Materials
- 112-57 Exam Tips □ 112-57 New Learning Materials □ 112-57 Reliable Test Duration □ Easily obtain ➤ 112-57 □ for free download through (www.exam4labs.com) □ 112-57 New Learning Materials
- Pass 112-57 Exam with Updated 112-57 Reliable Exam Pattern by Pdfvce □ Open ➡ www.pdfvce.com □□□ and search for ➡ 112-57 □ to download exam materials for free □ 112-57 Exam Brain Dumps
- 112-57 Reliable Exam Pattern - High-Efficient Latest 112-57 Test Cram and Correct EC-Council Digital Forensics Essentials (DFE) Mock Test □ Open 【 www.troytecdumps.com 】 and search for ✓ 112-57 □ ✓ □ to download exam materials for free □ New 112-57 Test Syllabus
- 112-57 Actual Collection: EC-Council Digital Forensics Essentials (DFE) - 112-57 Quiz Braindumps - 112-57 Exam Guide □ Go to website 《 www.pdfvce.com 》 open and search for ✨ 112-57 □ ✨ □ to download for free □ Exam 112-57 Guide
- 112-57 Latest Demo □ 112-57 Exam Brain Dumps □ New 112-57 Mock Exam □ Search for “ 112-57 ” and download exam materials for free through □ www.dumpsmaterials.com □ □ 112-57 Reliable Test Duration
- New Soft 112-57 Simulations □ Pass4sure 112-57 Study Materials □ New 112-57 Mock Exam □ Search for ✨ 112-57 □ ✨ □ and easily obtain a free download on ✨ www.pdfvce.com □ ✨ □ □ Useful 112-57 Dumps
- Pass 112-57 Exam with Updated 112-57 Reliable Exam Pattern by www.torrentvce.com □ Go to website ▷ www.torrentvce.com ◁ open and search for ▷ 112-57 ◁ to download for free □ 112-57 Certification Dump
- 112-57 New Learning Materials □ New Soft 112-57 Simulations □ 112-57 Latest Demo □ Enter ▷ www.pdfvce.com ◁ and search for ▷ 112-57 ◁ to download for free □ 112-57 Exam Tips
- 112-57 Real Sheets □ Valid 112-57 Test Topics □ 112-57 New Learning Materials ↗ Easily obtain 《 112-57 》 for free download through ➤ www.practicevce.com □ □ Sure 112-57 Pass
- gedsimekong.org, rsakuls637365.buscawiki.com, harleyumfm575976.blog4youth.com, jeanfjlo170273.idblogmaker.com, e-bookmarks.com, sabrinnajvo254936.theideasblog.com, marvinnibh722927.elbloglibre.com, ineszvjh665109.59bloggers.com, top100bookmark.com, geraldvrnc353789.salesmanwiki.com, Disposable vapes

BONUS!!! Download part of NewPassLeader 112-57 dumps for free: <https://drive.google.com/open?id=1two2U3bRUDnAxnrkg2KgVwy66GbQJYRd>