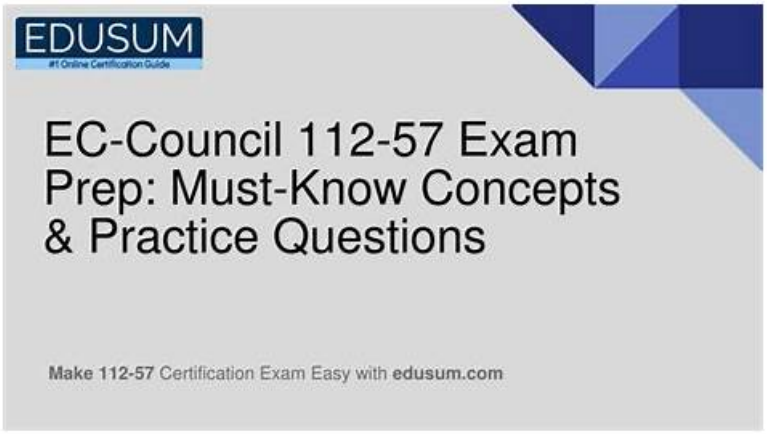
EC-COUNCIL 112-57 Study Material & Latest 112-57 Dumps Questions



BONUS!!! Download part of TestPDF 112-57 dumps for free: https://drive.google.com/open?id=19l6skjFG6rxkGl3FC-EDLSQF53EPgtM1

Our 112-57 learning guide is very efficient tool in the world. As is known to us, in our modern world, everyone is looking for to do things faster, better, smarter, so it is no wonder that productivity hacks are incredibly popular. So we must be aware of the importance of the study tool. In order to promote the learning efficiency of our customers, our 112-57 Training Materials were designed by a lot of experts from our company. Our 112-57 study materials will be very useful for all people to improve their learning efficiency.

While attempting the exam, take heed of the clock ticking, so that you manage the EC-COUNCIL 112-57 Questions in a time-efficient way. Even if you are completely sure of the correct answer to a question, first eliminate the incorrect ones, so that you may prevent blunders due to human error.

>> EC-COUNCIL 112-57 Study Material <<

112-57 Test Braindumps: EC-Council Digital Forensics Essentials (DFE) - 112-57 Pass-Sure Torrent & 112-57 Ttest Questions

Choosing our 112-57 learning guide is not only an enrichment of learning content, but also an opportunity to improve our own discovery space. Our 112-57 study guide materials could bring huge impact to your personal development, because in the process of we are looking for a job, hold a 112-57 certificate you have more advantage than your competitors, the company will be a greater probability of you. After using our 112-57 Study Guide materials, users can devote more time and energy to focus on their major and makes themselves more and more prominent in the professional field.

EC-COUNCIL 112-57 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• Investigating Web Attacks: This module focuses on analyzing web application attacks through server logs and detecting malicious activities targeting web servers and applications.

Topic 4	• 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 5	• 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 6	• 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 7	• Network Forensics: This module introduces network forensic concepts, including event correlation, analyzing network logs, identifying indicators of compromise, and investigating network traffic.
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.

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) Sample Questions (Q70-Q75):

NEW QUESTION # 70
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. Android
- B. Linux
- C. Windows
- D. Mac OS

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 # 71
Which of the following types of phishing attacks allows an attacker to exploit instant messaging platforms by employing IM as a tool to spread spam?

- A. Spear phishing
- B. Whaling
- C. Pharming
- D. Spimming

Answer: D

Explanation:
Spimmingis defined in digital forensics and cybercrime references asspam over instant messaging (IM). It is a social-engineering variant where attackers use instant messaging platforms (and sometimes chat apps) to deliver unsolicited bulk messages containing malicious links, fraudulent offers, credential-harvesting lures, or malware downloads. Because IM messages are often delivered in real time and can appear to come from known contacts (via compromised accounts), spimming can achieve higher click-through rates than traditional email spam. For investigators, spimming incidents commonly leave artifacts such as chat logs, message timestamps, sender identifiers, embedded URLs, and sometimes downloaded payload traces on the endpoint.
These artifacts help establish attacker infrastructure (domains, IPs), victim interaction (click events, file creation), and timeline correlation with network logs.
The other options do not match the "IM as a tool to spread spam" description.Whalingtargets high-profile individuals via highly tailored phishing, typically email-based.Pharmingredirects users to fraudulent websites (often via DNS or host-file manipulation) without relying on bulk IM spam.Spear phishingis targeted phishing toward specific individuals or groups, not necessarily IM spam.
Therefore, the phishing/spam attack that exploits instant messaging platforms isSpimming (C).

NEW QUESTION # 72
Jack, a forensic investigator, was appointed by an organization to perform a security audit on a Linux system.
In this process, Jack collected information about the present status of the system and listed all the applications running on various ports to detect malicious programs.
Which of the following commands can help Jack determine any programs/processes associated with open ports?

- A. netstat -i
- B. netstat -tulpn
- C. netstat -rn
- D. ip r

Answer: B

Explanation:
On Linux, a key step in a forensic triage or security audit is mappingopen/listening portsto theowning processso investigators can identify suspicious services (backdoors, unauthorized daemons, rogue remote- access tools) and correlate them with binaries, users, startup mechanisms, and timestamps. The command netstat -tulpnis designed for exactly this purpose. In this switch set:-tlimits output to TCP sockets,-uincludes UDP sockets,-lshows only listening sockets (open ports awaiting connections),-pdisplays the owningprocess name and PID, and-nprevents name resolution by showing numeric IP addresses and ports (faster and avoids altering evidence via DNS queries). This combination yields a concise list of active listening ports and the processes bound to them, which is highly valuable for detecting unexpected services and attributing network exposure to a specific executable.
The other options do not provide process-to-port attribution:netstat -ishows interface statistics,ip rshows the routing table, andnetstat -rndisplays the routing table in numeric form. Therefore, the correct command is netstat -tulpn(D).

NEW QUESTION # 73
Clark, a digital forensic expert, was assigned to investigate a malicious activity performed on an organization' s network. The organization provided Clark with all the information related to the incident. In this process, he assessed the impact of the incident on the organization, reasons for and source of the incident, steps required to tackle the incident, investigation team required to handle the case, investigative procedures, and possible outcome of the forensic process.
Identify the type of analysis performed by Clark in the above scenario.

- A. Case analysis
- B. Traffic analysis
- C. Data analysis
- D. Log analysis

Answer: A

Explanation:
The activities described align withcase analysis, which is the structured, high-level evaluation performed at the beginning (and throughout) a digital forensic investigation to define scope, strategy, resources, and expected deliverables. Case analysis focuses on understanding theoverall incident context: how the organization is affected (business/operational impact), what is believed to have happened (incident reasons and likely source), and what must be done to control and investigate it (containment steps and

investigative approach). It also includes planning elements such as identifying theinvestigation team composition(roles, skills, authority), definingproceduresto be followed (evidence handling, chain of custody, acquisition priorities, legal/HR requirements), and anticipating thepossible outcomes(reports, remediation actions, disciplinary/legal actions, or prosecution support).
By contrast,traffic analysisis narrowly focused on examining network packets/flows to infer communications and attacker behavior;log analysiscenters on parsing and correlating event records (firewall, server, endpoint logs); anddata analysistypically refers to examining acquired artifacts (files, memory images, timelines) for evidentiary content. Because Clark is assessing impact, cause/source, response steps, staffing, procedures, and outcomes-an overall investigative planning and evaluation function-the correct choice isCase analysis (B).

NEW QUESTION # 74
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. Data modification
- B. Buffer overflow
- C. Session hijacking
- D. Enumeration

Answer: D

Explanation:
The activity described-collectingnetwork topologydetails and compiling alist of live hosts-matches the reconnaissance phase commonly referred to asenumeration. 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 modificationinvolves altering data integrity;session hijackingtargets active sessions/tokens; andbuffer overflowis an exploitation technique against vulnerable software, not the information-gathering step described. Therefore, the correct answer isEnumeration (B)

NEW QUESTION # 75
.....

- Actual 112-57 EC-Council Digital Forensics Essentials (DFE) Exam Questions with accurate answers □ Download （ 112-57 ） for free by simply searching on ➤ www.pdfvce.com □ □Valid Braindumps 112-57 Sheet
- 112-57 Preparation □ 112-57 Reliable Practice Materials □ Valid Braindumps 112-57 Sheet □ Search for 【 112-57 】 and obtain a free download on ☀ www.prepawayexam.com □☀□ □112-57 Sure Pass
- 112-57 latest study torrent - 112-57 practice download pdf □ Search for 【 112-57 】 and easily obtain a free download on □ www.pdfvce.com □ □112-57 Sure Pass
- Cert 112-57 Exam □ Actual 112-57 Test Answers □ Free 112-57 Test Questions □ Search for ▹ 112-57 ◃ and easily obtain a free download on □ www.vce4dumps.com □ □Free 112-57 Test Questions
- 112-57 latest study torrent - 112-57 practice download pdf □ The page for free download of 【 112-57 】 on 「 www.pdfvce.com 」 will open immediately ↪112-57 Preparation
- 112-57 Test Torrent □ Actual 112-57 Test Answers □ 112-57 Valid Exam Discount □ Go to website ☀ www.verifieddumps.com □☀□ open and search for 「 112-57 」 to download for free □112-57 Valid Exam Discount
- shaunamkyz862854.buscawiki.com, nelsonnbvx670750.blogacep.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, maroonbookmarks.com, bookmarkshome.com, mohamadipva859962.wikimeglio.com, thesocialroi.com, aprilueys917717.59bloggers.com, zbookmarkhub.com, jaysonczmk149015.wikibestproducts.com, Disposable vapes

DOWNLOAD the newest TestPDF 112-57 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=19l6skjFG6rxkGl3FC-EDLSQF53EPgtM1