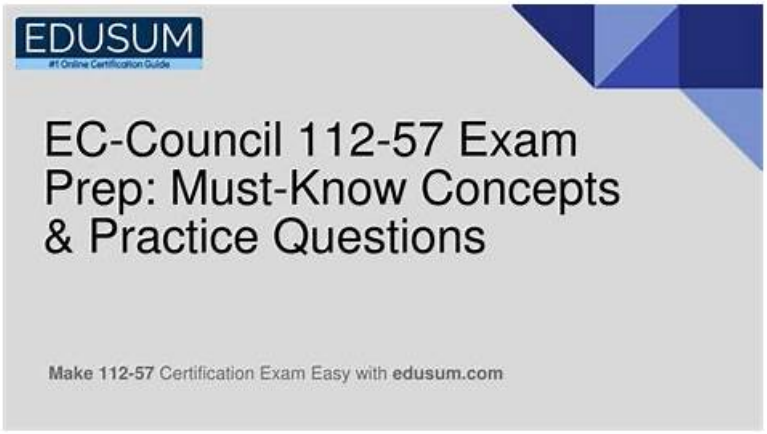
Valid 112-57 Practice Tests - Success in EC-COUNCIL 112-57 Exam is Easy



P.S. Free 2026 EC-COUNCIL 112-57 dumps are available on Google Drive shared by PDFVCE: https://drive.google.com/open?id=1VJD06rqrfLKHDoPWqjgyPGn_7Zepf92k

To those time-sensitive exam candidates, our high-efficient 112-57 actual dumps comprised of important news will be best help. Only by practicing our 112-57 learning guide on a regular base, you will see clear progress happened on you. Besides, rather than waiting for the gain of our 112-57 Practice Engine, you can download them immediately after paying for it, so just begin your journey toward success now.

The EC-COUNCIL 112-57 exam questions are designed and verified by experienced and qualified EC-COUNCIL 112-57 exam trainers. So you rest assured that with EC-Council Digital Forensics Essentials (DFE) (112-57) exam dumps you can streamline your 112-57 exam preparation process and get confidence to pass EC-Council Digital Forensics Essentials (DFE) (112-57) exam in first attempt.

>> 112-57 Practice Tests <<

2026 EC-COUNCIL 112-57: Reliable EC-Council Digital Forensics Essentials (DFE) Practice Tests

PDFVCE is a dumps pdf provider that ensures you pass the EC-COUNCIL braindumps exam with high rate. You may wonder how we can guarantee the high pass rate. You can rest assured that the 112-57 braindumps questions and learning materials are created by our IT teammates who have rich experience in the 112-57 Top Questions. And we constantly keep the updating of vce dumps to ensure the accuracy of questions and answers.

EC-COUNCIL 112-57 Exam Syllabus Topics:

Topic	Details
Topic 1	• Network Forensics: This module introduces network forensic concepts, including event correlation, analyzing network logs, identifying indicators of compromise, and investigating network traffic.
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	• Investigating Web Attacks: This module focuses on analyzing web application attacks through server logs and detecting malicious activities targeting web servers and applications.

Topic 5	• 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 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	• 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 8	• 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 9	• 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 10	• 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 (Q12-Q17):

NEW QUESTION # 12
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 # 13
In which of the following attacks does an attacker trick high-profile executives such as CEOs, CFOs, politicians, and celebrities to reveal critical corporate and personal information through email or website spoofing?

- A. Spimming
- B. Smishing
- C. Whaling

- D. Identity fraud

Answer: C

Explanation:
The scenario describes a targeted social-engineering attack aimed specifically athigh-profile individuals (CEOs, CFOs, politicians, celebrities) and usesemail or website spoofingto deceive them into disclosing sensitive information. In digital forensics and incident response documentation, this is most accurately categorized aswhaling, a specialized form of phishing that focuses on "big targets" (often called "high-value targets" or "VIPs"). Whaling campaigns typically use highly tailored pretexts (e.g., legal subpoenas, board communications, invoice/payment requests, HR or executive directives) and may include spoofed sender domains, look-alike websites, or fraudulent login pages to harvest credentials and confidential corporate data.
Because executives often have access to financial systems, strategic documents, and privileged communications, attackers concentrate effort on realism and personalization, making whaling distinct from broad, generic phishing.
By contrast,smishingis phishing conducted via SMS/text messages,spimmingis spam over instant messaging platforms, andidentity fraudis a broader category involving impersonation/misuse of personal data but does not specifically denote the executive-targeted spoofing technique described. Therefore, the attack type in the question isWhaling (A).

NEW QUESTION # 14
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. Whaling
- B. Pharming
- C. Spimming
- D. Spear phishing

Answer: C

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 # 15
A disk drive has 16,384 cylinders, 80 heads, and 63 sectors per track, and each sector can store 512 bytes of data.
What is the total size of the disk?

- A. 42,278,584,340 bytes
- B. 43,278,584,320 bytes
- C. 42,278,584,320 bytes
- D. 42,279,584,320 bytes

Answer: C

Explanation:
In classic hard-disk geometry, total capacity is computed fromCHS parameters(Cylinders × Heads × Sectors per track) multiplied bybytes per sector. Forensic examiners learn this because it helps validate whether an image acquisition size is consistent with the physical disk geometry and to spot anomalies caused by misreported device geometry or capture errors.
First compute total addressable sectors:
16,384 cylinders × 80 heads = 1,310,720 tracks(because each head provides a track per cylinder).

Then multiply by sectors per track:
1,310,720 × 63 = 82,575,360 sectors.
Convert sectors to bytes using the sector size:
82,575,360 sectors × 512 bytes/sector = 42,278,584,320 bytes.
This matches optionAexactly. In practice, modern drives often use LBA and may report different logical geometries, but the forensic principle remains the same: capacity equals the number of logical blocks times the logical block size, and CHS-style values are a structured way to perform that verification.

NEW QUESTION # 16
A system that a cybercriminal was suspected to have used for performing an anti-social activity through the Tor browser. James reviewed the active network connections established using specific ports via Tor.
Which of the following port numbers does Tor use for establishing a connection via Tor nodes?

- A. 3024/4092
- B. 1026/64666
- C. 9150/9151
- D. 31/456

Answer: C

Explanation:
In Tor Browser deployments, Tor typically runs a local client ("tor" process) that exposes aSOCKS proxyfor applications (the browser) to send traffic into the Tor network and, optionally, acontrol interfacefor managing circuits and obtaining runtime status. In many forensic lab guides and Tor Browser bundle configurations, the default local SOCKS listening port is9150, and the associated Tor control port is commonly9151. This pairing is frequently referenced in investigations because endpoint triage (e.g., netstat outputs, firewall logs, EDR socket telemetry) may show local loopback connections from the browser to127.0.0.1:9150(SOCKS) and management communications involving9151(control).
From a network-forensics viewpoint, these ports help distinguish Tor Browser activity from other proxy tools:
the browser does not directly connect to Tor relays; instead, it hands traffic to the local SOCKS proxy, which then establishes encrypted circuits to Tor nodes. While Tor can be configured to use different ports, the question asks about the specific ports used for establishing Tor connections in typical Tor Browser setups, which aligns with9150/9151. Therefore, the correct option isD.

NEW QUESTION # 17
.....

for free download on ⇒ www.practicevce.com ⇐ □112-57 Prepaway Dumps

- Free PDF Quiz EC-COUNCIL - 112-57 –High Pass-Rate Practice Tests □ Search for " 112-57 " and download exam materials for free through [www.pdfvce.com] □PDF 112-57 Cram Exam
- 112-57 Latest Exam Dumps □ Technical 112-57 Training □ 112-57 Test Sample Online □ Search for ➠ 112-57 □ □ and easily obtain a free download on ➤ www.exam4labs.com □ □112-57 Dump Check
- jessengen850195.wikimidpoint.com, tamzinknkr549833.pennywiki.com, bookmarkworm.com, kingslists.com, rsawxow811614.blogaritma.com, keybookmarks.com, caraqcie348401.wikibyby.com, bookmarksurl.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

DOWNLOAD the newest PDFVCE 112-57 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1VJD06rqrfLKHDoPWqjgyPGn_7Zepf92k