Hot Test 112-57 Cram Review & Valid EC-COUNCIL Certification Training - 100% Pass-Rate EC-COUNCIL EC-Council Digital Forensics Essentials (DFE)

P.S. Free 2026 EC-COUNCIL 112-57 dumps are available on Google Drive shared by GuideTorrent: https://drive.google.com/open?id=1iSFUzXeuiq5ccgrASWKrq73vvgCHSOYX

GuideTorrent wants to win the trust of EC-COUNCIL 112-57 exam candidates at any cost. To achieve this objective GuideTorrent is offering some top features with 112-57 exam practice questions. These prominent features hold high demand and are specifically designed for quick and complete EC-Council Digital Forensics Essentials (DFE) (112-57) exam questions preparation.

EC-COUNCIL 112-57 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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 2	• 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 3	• Network Forensics: This module introduces network forensic concepts, including event correlation, analyzing network logs, identifying indicators of compromise, and investigating network traffic.
Topic 4	• Investigating Email Crimes: This module covers the basics of email systems and the process of investigating suspicious emails to identify potential cybercrime evidence.
Topic 5	• 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 6	• 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 7	• 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 8	• 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 9	• Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity.

>> Test 112-57 Cram Review <<

Get EC-COUNCIL 112-57 Exam Questions - 100% Success Guaranteed [2026]

EC-COUNCIL is obliged to give you 12 months of free update checks to ensure the validity and accuracy of the EC-COUNCIL 112-57 exam dumps. We also offer you a 100% money-back guarantee, in the very rare case of failure or unsatisfactory results. This puts your mind at ease when you are EC-COUNCIL 112-57 Exam preparing with us.

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

NEW QUESTION # 39
Cheryl, a forensic expert, was recruited to investigate a malicious activity performed by an anonymous hackers' group on an organization's systems. Using an automated tool, Cheryl was able to extract the malware file and analyze the assembly code instructions, which helped him understand the malware's purpose.
Which of the following tools helped Cheryl extract and analyze the assembly code of the malware?

- A. OllyDbg
- B. QualNet
- C. Virtual Box
- D. VMware vSphere

Answer: A

Explanation:
To understand a malware sample's purpose at the instruction level, investigators usereverse-engineering toolsthat candisassemblecompiled binaries intoassembly codeand often allowinteractive debuggingto observe runtime behavior (API calls, unpacking routines, decryption loops, process injection, and control-flow decisions).OllyDbgis a classic Windows user-mode debugger widely referenced in malware analysis workflows because it provides an integrated view ofdisassembly, CPU registers, memory, breakpoints, and execution tracing. This makes it suitable for extracting behavioral insight from the actual assembly instructions, especially when malware uses obfuscation or packers that require stepping through execution to reach the real payload.
The other options do not primarily perform assembly-level analysis.VirtualBoxandVMware vSphereare virtualization platforms; they help safely run malware in isolated environments, but they are not disassemblers /debuggers for examining assembly instructions.QualNetis a network simulation tool used for modeling network behavior, not binary reverse engineering. Because the question specifically emphasizesanalyzing assembly code instructionsto understand malware purpose, the correct tool among the choices isOllyDbg (C).

NEW QUESTION # 40
Bob, a forensic specialist at a newly established NGO, discovered a security loophole in the NGO's web application, which unintentionally reveals early enrolled NGO members' biodata to attackers. Bob immediately employed a content filtering mechanism to protect all the NGO's data sources and prevent further damage.
Identify the web application threat identified by Bob in the above scenario.

- A. Buffer overflow
- B. Information leakage
- C. Authentication hijacking
- D. Cookie poisoning

Answer: B

Explanation:
The scenario describes a web application thatunintentionally reveals sensitive member biodatato attackers.

This is a classic case ofinformation leakage, where confidential or private data becomes exposed due to poor access control, improper output handling, verbose error messages, misconfigured endpoints, insecure direct object references, or unintended exposure through pages, APIs, backups, or logs. In forensic and web security documentation, information leakage is defined by theunauthorized disclosure of data, even if the attacker does not alter the system. The key indicator here is that the application is "revealing" biodata-meaning confidentiality is breached.
Bob's response-using acontent filtering mechanism-also aligns with mitigating data exposure. Content filtering can prevent sensitive fields from being returned, mask personally identifiable information, restrict responses based on user role, and sanitize outputs before they leave the server.
The other options do not match the described impact.Buffer overflowis a low-level memory corruption vulnerability, typically associated with native code execution rather than accidental biodata exposure.
Authentication hijackinginvolves taking over sessions/credentials, andcookie poisoninginvolves manipulating cookie values to gain privileges or alter behavior-neither is explicitly indicated. Therefore, the identified threat isInformation leakage (B).

NEW QUESTION # 41
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. Smishing
- B. Identity fraud
- C. Whaling
- D. Spimming

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 # 42
Which of the following acts was passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

- A. Sarbanes-Oxley Act (SOX)
- B. The Electronic Communications Privacy Act
- C. General Data Protection Regulation (GDPR)
- D. Information Privacy Act 2014

Answer: A

Explanation:
TheSarbanes-Oxley Act (SOX)was enacted by the U.S. Congress in2002in response to major corporate accounting scandals and was specifically designed toprotect investorsby improving the accuracy, reliability, and integrity of corporate disclosures and financial reporting. SOX strengthens governance and accountability by requiring executive management (notably the CEO and CFO) to certify the correctness of financial statements and by mandating stronger internal controls over financial reporting. From a digital forensics and compliance perspective, SOX is closely tied to the need for reliableaudit trails, properrecords retention, and demonstrable control over systems that store or process financial data. Investigators frequently rely on SOX- driven logging, access controls, and change management records to determine who accessed financial systems, what changes were made, and whether those actions align with authorized procedures.
The other options do not match the question's purpose or jurisdiction: theElectronic Communications Privacy Actaddresses interception and access to electronic communications,GDPRis an EU data protection regulation (not a 2002 U.S. act focused on

investor protection), and "Information Privacy Act 2014" is not the 2002 U.S.
corporate anti-fraud legislation. Therefore, the correct answer isSarbanes-Oxley Act (SOX) (C).

NEW QUESTION # 43
Which of the following techniques is defined as the art of hiding data "behind" other data without the target's knowledge, thereby hiding the existence of the message itself?

- A. Password cracking
- B. Steganography
- C. Program packer
- D. Artifact wiping

Answer: B

Explanation:
Steganographyis the technique of concealing a messagewithin another seemingly harmless carrier(such as an image, audio file, video, or document) so that theexistence of the hidden message is not apparentto an observer. Digital forensics references distinguish steganography from encryption: encryption scrambles content but usually leaves visible indicators that protected data exists (ciphertext), while steganography aims to make the communication look ordinary, reducing suspicion. In practice, steganographic methods often embed data into redundant or less perceptible parts of the carrier, such as modifying least significant bits in pixel values, altering frequency components in audio, or inserting data into metadata or unused file structures.
The other options do not match the definition.Password crackingis an access technique to recover authentication secrets, not a concealment method.Artifact wipingis an anti-forensics method intended to remove traces (logs, files, slack space remnants), but it does not "hide behind" other data-it destroys or overwrites evidence.Program packerscompress/obfuscate executables to hinder static analysis and detection, but they still produce an executable whose presence is evident; they do not primarily hide messages inside benign files. Therefore, the described "hiding the existence of the message itself" corresponds toSteganography (C).

NEW QUESTION # 44
.....

With the rapid development of the world economy and frequent contacts between different countries, looking for a good job has become more and more difficult for all the people. So it is very necessary for you to get the 112-57 certification, in order to look for a good job, you have to increase your competitive advantage in the labor market and make yourself distinguished from other job-seekers. And our 112-57 Exam Questions are specially desiged for you as we can help you pass the 112-57 exam successfully with the least time and effort. Just come and buy our 112-57 practice guide!

- 112-57 Certification Exam Dumps ✌ Exam 112-57 Tutorials □ 100% 112-57 Correct Answers ↪ Enter { www.prepawaypdf.com } and search for □ 112-57 □ to download for free □Valid 112-57 Exam Tutorial
- haseebjhfs972234.blog2news.com, mariammrhi563717.laowaiblog.com, tegancmfj021026.dekaronwiki.com, deacontjhn261830.blogs100.com, finalmasterclass.com, setbookmarks.com, esgsolusi.id, izaakienm573235.ziblogs.com, bookmarkchamp.com, janicejuep400621.ssnblog.com, Disposable vapes

What's more, part of that GuideTorrent 112-57 dumps now are free: https://drive.google.com/open?id=1iSFUzXeuiq5ccgrASWKrq73vvgCHSOYX