EC-COUNCIL 112-57 New Test Materials: EC-Council Digital Forensics Essentials (DFE) - Dumpkiller Updated Download

P.S. Free 2026 EC-COUNCIL 112-57 dumps are available on Google Drive shared by Dumpkiller: https://drive.google.com/open?id=1Bd7kV-VD0DQpNvRuh1lqmTlAaHljGHOy

With a high quality, we can guarantee that our 112-57 practice quiz will be your best choice. There are three different versions of our 112-57 guide dumps: the PDF, the software and the online. The three versions of our 112-57 learning engine are all good with same questions and answers. Our products have many advantages, I am going to introduce you the main advantages of our112-57 Study Materials, I believe it will be very beneficial for you and you will not regret to use our products.

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	• Investigating Web Attacks: This module focuses on analyzing web application attacks through server logs and detecting malicious activities targeting web servers and applications.
Topic 3	• 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 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	• Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity.
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	• 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	• Investigating Email Crimes: This module covers the basics of email systems and the process of investigating suspicious emails to identify potential cybercrime evidence.

Get High-quality 112-57 New Test Materials and High Pass-Rate 112-57 Trusted Exam Resource

Our company is open-handed to offer benefits at intervals, with 112-57 learning questions priced with reasonable prices. Almost all kinds of working staffs can afford our price, even the students. And we will give some discounts from time to time. Although our 112-57 practice materials are reasonably available, their value is in-estimate. We offer hearty help for your wish of certificate of the 112-57 exam.

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

NEW QUESTION # 11
Steve, a professional hacker, attempted to hack Alice's banking account. To accomplish his goal, Steve used an automated tool to guess Alice's login credentials. The tool uses a trial-and-error method by attempting all possible combinations of usernames and passwords to determine the valid credentials.
Identify the type of attack initiated by Steve in the above scenario.

- A. Phishing attack
- B. Brute-force attack
- C. Data manipulation attack
- D. Trojan horse attack

Answer: B

Explanation:
The scenario describes an automated, trial-and-error attempt that triesall possible combinations of usernames and passwordsuntil a correct credential pair is found. This is the defining characteristic of abrute-force attack.
In digital forensics terminology, brute force is a direct password-guessing method that relies on exhaustive attempts (or systematically generated candidates) rather than tricking the user or exploiting a software flaw.
Investigators commonly recognize brute-force activity through artifacts such as repeated authentication failures in security logs, high-frequency login attempts from a single IP or distributed sources, account lockout events, and abnormal spikes in authentication traffic. In banking and web environments, it may also appear as repeated POST requests to login endpoints with varying credential pairs and consistent user-agent patterns, sometimes accompanied by throttling or CAPTCHA triggers.
The other options do not match the described "attempting all possible combinations" behavior.
Phishingobtains credentials by deception (fake emails/sites). ATrojan horsesteals data by running malicious code on the victim's system.Data manipulationfocuses on altering data integrity rather than credential guessing. Therefore, the correct attack type isBrute-force attack (A).

NEW QUESTION # 12
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. nmap -sT localhost
- B. netstat -i
- C. ipconfig <interface name>
- D. ifconfig <interface name>

Answer: D

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 # 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. Whaling
- B. Identity fraud
- C. Smishing
- D. Spimming

Answer: A

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

- A. Middle relay
- B. Entry relay
- C. Guard relay
- D. Exit 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 # 15
Williams, a forensic specialist, was tasked with performing a static malware analysis on a suspect system in an organization. For this purpose, Williams used an automated tool to perform a string search and saved all the identified strings in a text file. After analyzing

the strings, he determined all the harmful actions that were performed by malware.
Identify the tool employed by Williams in the above scenario.

- A. Snagit
- B. Ezvid
- C. ResourcesExtract
- D. R-Drive Image

Answer: C

Explanation:
Instatic malware analysis, one of the quickest ways to infer capability is to extract and reviewstringsembedded in a binary. Strings frequently reveal command-and-control domains/IPs, mutex names, file paths, registry keys, user-agent values, suspicious commands (PowerShell/cmd), API names, error messages, encryption markers, and configuration fragments. Investigators often use automated utilities to extract these readable artifacts andexport them to a text filefor later triage, keyword searching, and correlation with other evidence (network logs, endpoint telemetry, and threat intel).
Among the provided options,ResourcesExtractbest matches this workflow. It is designed to extract embedded content from executable files-particularly Windows PE resources-and can export extracted textual items (including resource strings/strings tables and related embedded text) into external files for analysis. This aligns with "performed a string search and saved all the identified strings in a text file." The other choices do not fit:R-Drive Imageis a disk imaging/backup tool;Ezvidis for screen recording; andSnagitis for screenshots/screen capture. They do not perform automated extraction of strings from malware binaries as a static-analysis step. Therefore, the correct answer isResourcesExtract (B).

NEW QUESTION # 16
.....

bookmarking.com, idajbem370680.empirewiki.com, privatebookmark.com, olivebookmarks.com, woodyzmsn308650.wizzardsblog.com, nicoleddmh848939.iyublog.com, thesocialvibes.com, yoursocialpeople.com, Disposable vapes

What's more, part of that Dumpkiller 112-57 dumps now are free: https://drive.google.com/open?id=1Bd7kV-VD0DQpNvRuh1lqmTlAaHljGHOy