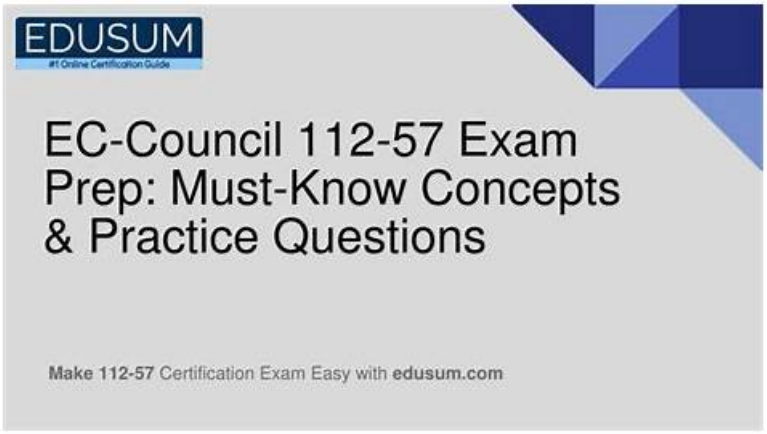
EC-COUNCIL 112-57 Reliable Test Objectives, New Guide 112-57 Files



P.S. Free & New 112-57 dumps are available on Google Drive shared by DumpStillValid: https://drive.google.com/open?id=1vgKcGSgw9NwIhLr0SFZc8fXZZ6dcnqC2

Our EC-COUNCIL 112-57 can help you clear exams at first shot. We promise that we provide you with best quality EC-COUNCIL 112-57 original questions and competitive prices. We provide one year studying assist service and one year free updates downloading of EC-Council Digital Forensics Essentials (DFE) exam questions.

Along with EC-Council Digital Forensics Essentials (DFE) (112-57) self-evaluation exams, 112-57 dumps PDF is also available at DumpStillValid. These 112-57 questions can be used for quick EC-Council Digital Forensics Essentials (DFE) (112-57) preparation. Our 112-57 dumps PDF format works on a range of Smart devices, such as laptops, tablets, and smartphones. Since 112-57 Questions Pdf are easily accessible, you can easily prepare for the test without time and place constraints. You can also print this format of DumpStillValid's EC-Council Digital Forensics Essentials (DFE) (112-57) exam dumps to prepare off-screen and on the go.

>> EC-COUNCIL 112-57 Reliable Test Objectives <<

Confirm Your Success With Free EC-COUNCIL 112-57 Exam Questions Updates & Demo

If you choose our 112-57 exam question for related learning and training, the system will automatically record your actions and analyze your learning effects. Many people want to get a 112-57 certification, but they worry about their ability. So please do not hesitate and join our study. Our 112-57 Exam Question will help you to get rid of your worries and help you achieve your wishes. So you will have more opportunities than others and get more confidence. Our 112-57 quiz guide is based on the actual situation of the customer.

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) Sample Questions (Q60-Q65):

NEW QUESTION # 60
Below is the syntax of a command-line utility that displays active TCP connections and ports on which the computer is listening.
netstat [-a] [-e] [-n] [-o] [-p Protocol] [-r] [-s] [Interval]
Identify the netstat parameter that displays active TCP connections and includes the process ID (PID) for each connection.

- A. [-o]
- B. [-a]
- C. [-n]
- D. [-s]

Answer: A

Explanation:
In Windows forensics and incident response, investigators often need to linknetwork activity(remote IPs, ports, connection states) to theresponsible processto determine whether traffic is legitimate or associated with malware, unauthorized tools, or data exfiltration. The Windowsnetstatutility can enumerate current TCP connections and listening ports, but the key flag that enables attribution to a running program is-o. The-o parameter instructs netstat to include theOwning Process ID (PID)with each connection or listening socket.
Once the PID is known, examiners can correlate it with process listings (e.g., Task Manager,tasklist, memory forensics output) to identify the executable name, path, user context, and parent process-critical steps in reconstructing attacker behavior and persistence.
The other options do not provide PID mapping:-nshows addresses and ports in numeric form (useful for speed and to avoid DNS lookups),-adisplays all connections and listening ports but without PID attribution by itself, and-sshows protocol statistics rather than per-connection ownership. Therefore, the parameter that shows active connectionsandincludes the PID for each is[-o](Option C).

NEW QUESTION # 61
Benoy, a security professional at an organization, extracted Apache access log entries to view critical information about all the operations performed on a web server. The Apache access log extracted by Benoy is given below:
"10.10.10.10 - Jason [17/Aug/2019:00:12:34 +0300] "GET /images/content/bg_body_1.jpg HTTP/1.0" 500 1458"
Identify the HTTP status code in the Apache access log entry above that indicates the response was successful.

- A. +0300
- B. 1.0
- C. 0
- D. 1

Answer: D

Explanation:
In the Apache Combined/Custom access log format, the value immediately after the quoted request (here," GET ... HTTP/1.0") is theHTTP status codereturned by the server. In the provided entry, that field is500.
From a forensic analysis standpoint, recognizing field positions matters because investigators correlate client IPs, timestamps, requested resources, and server outcomes to reconstruct attack timelines and identify failed exploitation attempts or misconfigurations.
It is important to note thatsuccessful HTTP responses are typically in the 2xx range, most commonly200 (OK), while3xxindicates redirects,4xxindicates client-side errors (such as 404 Not Found), and5xxindicates server-side failures. Specifically,500represents anInternal Server Error, meaning the server encountered an unexpected condition and could not fulfill the request successfully.
The other options are not HTTP status codes in this entry:+0300is the timezone offset in the timestamp,1.0is the HTTP protocol version, and2019is part of the date. Therefore, the only HTTP status code present-and the correct choice among the options-is500 (B), even though it reflects an error rather than success.

NEW QUESTION # 62
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. Artifact wiping
- B. Password cracking
- C. Steganography
- D. Program packer

Answer: C

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 # 63
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. Mac OS
- C. Windows
- D. Linux

Answer: D

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 # 64
Given below is a regex signature used by security professionals for detecting an XSS attack:
/((%3C)|<)[