EC-COUNCIL 112-57: EC-Council Digital Forensics Essentials (DFE) braindumps PDF & Testking echter Test

Die Ausbildungsmaterialien zur EC-COUNCIL 112-57 Zertifizierungsprüfung aus Fast2test sind nicht nur der Grundstein auf dem Weg zu Ihrem Erfolg, sie können Ihnen auch dabei helfen, Ihre Fähigkeiten in der IT-Branche effektiver zu entfalten. Nach mehrjährigen Bemühungen beträgt die Hit-Rate von EC-COUNCIL 112-57 Zertifizierungsprüfung von Fast2test bereits 100%. Wenn Sie die Zertifizierungsprüfung nicht bestehen, nachdem Sie unsere Fragenpool gekauft haben, werden wir alle Ihre bezahlten Summe zurückgeben.

EC-COUNCIL 112-57 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• 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.
Thema 2	• 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.
Thema 3	• Network Forensics: This module introduces network forensic concepts, including event correlation, analyzing network logs, identifying indicators of compromise, and investigating network traffic.
Thema 4	• 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.
Thema 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.
Thema 6	• Malware Forensics: This module introduces malware investigation techniques, including static and dynamic analysis, and examining system and network behavior to understand malicious activity.

EC-COUNCIL 112-57 Deutsche, 112-57 Zertifikatsdemo

Die EC-COUNCIL 112-57 Dumps von Fast2test haben die sagenhafte Hit-Rate. Diese Dumps beinhalten alle mögliche Fragen in den aktuellen Prüfungen. Deshalb können Sie EC-COUNCIL 112-57 Prüfungen sehr leicht bestehen, wenn Sie diese Dumps ernst lernen. Als eine sehr wichtige EC-COUNCIL 112-57 Prüfung Zertifizierung spielt heute eine übergreifende Rolle. Deswegen können Sie die Chance nicht verlieren, die Prüfung zu bestehen. Fast2test verspricht Ihnen volle Rückerstattung wenn durchgefallen. Informieren Sie bitte mehr an Fast2test, wenn Sie die 112-57 Zertifizierungsprüfung bestehen wollen.

EC-COUNCIL EC-Council Digital Forensics Essentials (DFE) 112-57 Prüfungsfragen mit Lösungen (Q70-Q75):

70. Frage
Andrew, a system administrator, is performing a UEFI boot process. The current phase of the UEFI boot process consists of the initialization code that the system executes after powering on the EFI system. This phase also manages platform reset events and sets up the system so that it can find, validate, install, and run the PEI.
Which of the following UEFI boot phases is the process currently in?

- A. Boot device selection phase
- B. Pre-EFI initialization phase
- C. Driver execution environment phase
- D. Security phase

Antwort: D

Begründung:
In the UEFI/PI boot architecture, the phase that runsimmediately after power-on or resetis theSEC (Security) phase. Digital forensics references include UEFI phases because firmware-level activity can affect the trustworthiness of the platform (e.g., bootkits, persistence, and measured boot artifacts). The SEC phase is responsible for executing the earliest initialization instructions, handlingplatform reset events, and establishing a minimal, controlled execution environment. Critically, SEC prepares the system so it canlocate, verify, and hand off controlto the next stage-PEI (Pre-EFI Initialization)-by setting up temporary memory and foundational CPU/chipset state required for PEI modules to execute.
The wording in the question precisely matches SEC responsibilities: "initialization code executed after powering on," "manages platform reset events," and "sets up the system so it can find, validate, install, and run the PEI." By contrast,PEIfocuses on discovering and initializing permanent memory and producing the Hand-Off Blocks for DXE;DXEloads drivers and boot services; andBDSselects and launches the boot option.
Therefore, the phase described is theSecurity phase (SEC), which corresponds to optionD.

71. Frage
Which of the following standards and criteria version of SWGDE mandates that any action with the potential to alter, damage, or destroy any aspect of original evidence must be performed by qualified persons in a forensically sound manner?

- A. Standards and Criteria 1.1
- B. Standards and Criteria 1.7
- C. Standards and Criteria 1.3
- D. Standards and Criteria 1.5

Antwort: B

Begründung:
The statement in the question matchesSWGDE Principle 1, Standards and Criteria 1.7, which explicitly requires thatany action that could alter, damage, or destroy original digital evidence must be performed by qualified personnel in a forensically sound manner. In digital forensics doctrine, this requirement exists because digital evidence is highly fragile: routine interactions (booting a system, opening a file, connecting storage, running commands) can change timestamps, overwrite unallocated space, modify logs, or trigger encryption/key rotation. SWGDE's emphasis on "qualified persons" and "forensically sound manner" aligns with core evidentiary expectations: minimizing changes to original media, using controlled and repeatable methods (e.g., write-blocking, validated imaging, documented procedures), and ensuring actions are defensible under scrutiny.
Options 1.1, 1.3, and 1.5 relate to broader quality and procedural requirements (quality systems, SOP review, appropriate tools), but they do not contain the specific mandate about potentially altering original evidence.
The exact phrasing about alteration/damage/destruction and qualified handling is associated withStandards and Criteria 1.7, makingBthe correct choice.

72. Frage
An organization decided to strengthen the security of its network by studying and analyzing the behavior of attackers. For this purpose, Steven, a security analyst, was instructed to deploy a device to bait attackers.
Steven selected a solution that appears to contain very useful information to lure attackers and find their locations and techniques.
Identify the type of device deployed by Steven in the above scenario.

- A. Intrusion detection system
- B. Firewall
- C. Router
- D. Honeypot

Antwort: D

Begründung:
Ahoneypotis a deliberately deployed decoy system or service designed toattract attackersby appearing valuable or vulnerable, thereby enabling defenders to observe malicious behavior in a controlled manner.
Digital forensics and incident response references describe honeypots as tools forthreat intelligence and evidence collection, because they can record interaction details such as connection sources, exploited services, commands executed, malware dropped, and attempted privilege escalation. This directly matches the scenario: Steven deployed something that "appears to contain very useful information" tolure attackersand help identify theirlocations and techniques. Honeypots are typically instrumented with extensive logging and monitoring, making them especially useful for building timelines, extracting indicators of compromise, and understanding adversary tactics, techniques, and procedures.
The other options do not align with the "bait attackers" goal. AnIDSprimarily detects and alerts on suspicious activity but is not intended to impersonate a valuable target. Afirewallenforces access control rules to block
/allow traffic, not entice attackers. Arouterforwards packets and provides network connectivity; it is not a deception platform.
Therefore, the device type described is aHoneypot (C).

73. Frage
Bob, a security specialist at an organization, extracted the following IIS log from a Windows-based server:
"2019-12-12
06:11:41 192.168.0.10 GET /images/content/bg_body1.jpg - 80 - 192.168.0.27 Mozilla/5.0+(Windows+NT+6.
3;+WOW64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/48.0.2564.103+Safari/537.36
http://www.moviescope.com/css/style.css 200 0 0 365"
Identify the element in the above IIS log entry that indicates the request was fulfilled without error.

- A. 0
- B. 1
- C. 2
- D. 3

Antwort: A

Begründung:
In Microsoft IIS (W3C Extended) logging, each request line records multiple standardized fields that help investigators reconstruct what was accessed, by whom, and with what outcome. Among these fields, the most direct indicator of whether the server successfully handled the request is theHTTP status codecaptured in thesc-statusfield. A status code of200means"OK", indicating the server located the requested resource (here,
/images/content/bg_body1.jpg) and returned it successfully to the client without application-level failure.
Other numbers in the entry represent different attributes:80is the server port used for the HTTP request,
192values appear as part of IP addressing (client/server addresses), and537is embedded in the user-agent string (AppleWebKit build number), not a success indicator. IIS often logs additional substatus and Win32 status values (e.g.,sc-substatusandsc-win32-status) to refine the outcome; in the shown line, those follow the
200 as "200 0 0 ...", reinforcing that no substatus error or OS-level error occurred. Therefore,200is the element confirming the request was fulfilled without error.

74. Frage
Michael, a forensic expert, was assigned to investigate an incident that involved unauthorized intrusion attempts. In this process, Michael identified all the open ports on a system and disabled them because these open ports can allow attackers to install malicious services and compromise the security of the system or network.

Which of the following commands assisted Michael in identifying open ports in the above scenario?

- A. ifconfig <interface> -promisc
- B. netstat -i
- C. nmap -sT localhost
- D. netstat -rn

Antwort: C

Begründung:
To identifyopen ports, investigators need a method that actively checks which TCP/UDP ports on a host are accepting connections. The commandnmap -sT localhostperforms aTCP Connect scanagainst the local system. In a connect scan, Nmap uses the operating system's normal networking API to attempt a full TCP three-way handshake to each targeted port. If the handshake completes, the port is reported asopen; if it is refused, it isclosed; and if filtered by firewall rules, it may appearfiltered. This directly supports Michael's objective of enumerating open ports so they can be reviewed and disabled to reduce the attack surface and prevent malicious services from being installed.
The other options do not enumerate open ports in the same way.netstat -ishows interface-level statistics (packets, errors) rather than listing listening services.netstat -rndisplays the routing table (routes and gateways), which helps understand network paths but not which ports are open.ifconfig <interface> -promisc relates to enabling/disabling promiscuous mode on an interface for packet capture, not port discovery.
Therefore, the command that assisted in identifying open ports isnmap -sT localhost (C).

75. Frage
.....

- 112-57 German □ 112-57 Zertifikatsdemo □ 112-57 Simulationsfragen □ Suchen Sie jetzt auf 【 www.zertpruefung.ch 】 nach ☀ 112-57 □☀□ und laden Sie es kostenlos herunter □112-57 German
- denismscu724005.blogsumer.com, bookmarkblast.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, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, 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, www.stes.tyc.edu.tw, myfirstbookmark.com, www.stes.tyc.edu.tw, Disposable vapes