312-49v11 Unterlagen mit echte Prüfungsfragen der EC-COUNCIL Zertifizierung

2026 Die neuesten ZertPruefung 312-49v11 PDF-Versionen Prüfungsfragen und 312-49v11 Fragen und Antworten sind kostenlos verfügbar: https://drive.google.com/open?id=1AQ_UaL3st2u-y1v4XXa92_UTNj1RWvL8

Sie können Prüfungsfragen und Antworten zur EC-COUNCIL 312-49v11 Zertifizierungsprüfung teilweise umsonst als Probe herunterladen. Sobald Sie ZertPruefung wählen, würden wir alles tun, um Ihnen bei der Prüfung zu helfen. Wenn Sie später finden, dass die von uns gebotenen EC-COUNCIL 312-49v11 Prüfungsfragen und Antworten den echten Prüfungsfragen und Antworten nicht entsprechen und Sie somit die Prüfung nicht bestehen, dann erstatten wir Ihnen die an uns geleisteten Zahlung.

EC-COUNCIL 312-49v11 Prüfungsplan:

Thema	Einzelheiten
Thema 1	• Dark Web Forensics: This domain addresses dark web investigation focusing on Tor browser artifact identification, memory dump analysis, and extracting evidence of dark web activities.
Thema 2	• Linux and Mac Forensics: This domain addresses forensic methodologies for Linux and macOS systems including data collection, memory forensics, log analysis, APFS examination, and platform-specific investigation tools.
Thema 3	• Cloud Forensics: This domain covers cloud platform forensics (AWS, Azure, Google Cloud) including data storage, logging, forensic acquisition of virtual machines, and investigation of cloud security incidents.
Thema 4	• Windows Forensics: This domain covers Windows-specific investigation techniques including volatile and non-volatile data collection, memory and registry analysis, web browser forensics, metadata examination, and analysis of Windows artifacts like ShellBags, LNK files, and event logs.
Thema 5	• Computer Forensics Investigation Process: This domain addresses the structured investigation phases including first response procedures, lab setup, evidence preservation, data acquisition, case analysis, documentation, reporting, and expert witness testimony.
Thema 6	• Investigating Web Attacks: This domain covers web application forensics including IIS and Apache log analysis, OWASP Top 10 risks, and investigation of attacks like XSS, SQL injection, path traversal, command injection, and brute-force attempts.
Thema 7	• IoT Forensics: This domain addresses IoT device investigation including architecture, OWASP IoT threats, forensic processes, wearable and smart device analysis, hardware-level techniques (JTAG, chip-off), and drone data extraction.
Thema 8	• Mobile Forensics: This domain covers Android and iOS forensics including device architecture, forensics processes, cellular data investigation, file system acquisition, lock bypassing, rooting • jailbreaking, and mobile application analysis.

Thema 9	• Network Forensics: This domain covers network incident investigation through traffic and log analysis, event correlation, indicators of compromise identification, SIEM usage, and wireless network attack detection and examination.
Thema 10	• Computer Forensics in Today's World: This domain covers fundamentals of computer forensics including cybercrime types, investigation procedures, digital evidence handling, forensic readiness, investigator roles and responsibilities, industry standards, and legal compliance requirements.
Thema 11	• Defeating Anti-Forensics Techniques: This domain teaches methods to overcome evidence hiding techniques including data recovery, file carving, partition recovery, password cracking, steganography detection, encryption handling, and program unpacking.
Thema 12	• Malware Forensics: This domain addresses malware investigation including controlled lab setup, static analysis, system and network behavior analysis, suspicious document examination, and ransomware investigation techniques.
Thema 13	• Email and Social Media Forensics: This domain addresses email crime investigation including message analysis, U.S. email laws, social media activity tracking, footage extraction, and social network graph analysis.
Thema 14	• Understanding Hard Disks and File Systems: This domain covers storage media characteristics, disk logical structures, operating system boot processes (Windows, Linux, macOS), file systems analysis, encoding standards, and examination of common file formats.

Neueste 312-49v11 Pass Guide & neue Prüfung 312-49v11 braindumps & 100% Erfolgsquote

Wenn Sie Ihre IT-Fähigkeiten erhöhen und die EC-COUNCIL 312-49v11 Zertifizierungsprüfung einmalig bestehen möchten, können Sie auf ZertPruefung vertrauen. Denn ZertPruefung kann Ihnen helfen, das Prüfungszertifikat zu bekommen, indem wir Ihnen die zutreffendesten und genauesten Fragenkataloge zur EC-COUNCIL 312-49v11 Zertifizierungsprüfung anbieten. Wenn Sie mit dem Kaufen noch zögern, können Sie die Demo auf unserer Webseite ZertPruefung herunterladen. Wir sind sicher, dass Sie nicht enttäuscht sein werden.

EC-COUNCIL Computer Hacking Forensic Investigator (CHFI-v11) 312-49v11 Prüfungsfragen mit Lösungen (Q181-Q186):

181. Frage
In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

- A. RESTART packets to the affected router to get it to power back up
- B. STOP packets to all other routers warning of where the attack originated
- C. The change in the routing fabric to bypass the affected router
- D. More RESET packets to the affected router to get it to power back up

Antwort: C

182. Frage
You should always work with original evidence

- A. True

- B. False

Antwort: B

183. Frage
Which layer in the loT architecture is comprised of hardware parts such as sensors, RFID tags, and devices that play an important role in data collection?

- A. Edge technology layer
- B. Access gateway layer
- C. Application layer
- D. Middleware layer

Antwort: A

184. Frage
You're a cybersecurity analyst tasked with understanding the functionality of a Web Application Firewall (WAF) and its role in protecting web applications from various attacks. You need to grasp the benefits and limitations of WAFs and learn how to analyze log files generated by WAF tools like ModSecurity to detect web-based attacks.
What is the primary function of a Web Application Firewall (WAF)?

- A. Encrypting web traffic to ensure confidentiality
- B. Monitoring and analyzing system logs for suspicious activities
- C. Protecting network infrastructure from DDoS attacks
- D. Inspecting and filtering incoming and outgoing HTTP traffic for web applications

Antwort: D

Begründung:
According to theCHFI v11 Web Application Forensics and WAF module, the primary function of aWeb Application Firewall (WAF)is toinspect, monitor, and filter HTTP/HTTPS trafficbetween a web application and its users. Unlike traditional network firewalls, which operate at the network or transport layer, WAFs function at theapplication layer (Layer 7)and are specifically designed to protect web applications from attacks such asSQL injection, Cross-Site Scripting (XSS), command injection, file inclusion, parameter tampering, and cookie poisoning.
WAFs such asModSecurityanalyze web requests and responses usingrule-based logic, signatures, anomaly detection, and behavioral analysis. CHFI v11 emphasizes that WAF logs are critical forensic artifacts, as they record blocked requests, rule violations, payload details, source IP addresses, timestamps, and attack patterns. These logs allow investigators to detect, reconstruct, and attribute web-based attacks during forensic investigations.
The other options do not describe the primary function of a WAF.Encryption of web trafficis handled by SSL/TLS, not WAFs.DDoS protectionis typically managed by network-level or cloud-based mitigation systems, although some WAFs may offer limited support.System log monitoringis the role of SIEM solutions, not WAFs.
Therefore, as defined in CHFI v11, the core purpose of a Web Application Firewall isinspecting and filtering HTTP traffic to protect web applications, makingOption Athe correct and verified answer.

185. Frage
You're a digital forensic analyst tasked with analyzing a Portable Document Format (PDF) file to extract information about its structure and contents. Understanding the PDF file structure is essential for conducting a thorough analysis. What is the component of a PDF file that enables random access to objects, includes links to all objects within the file, and aids in tracking updates made to the PDF file?

- A. Cross-reference table (xref table)
- B. Body
- C. Footer
- D. Header

Antwort: A

Begründung:

According to the CHFI v11 objectives under File Type Analysis and Malware Forensics, understanding the internal structure of a PDF file is critical when investigating malicious documents. A standard PDF file consists of four main components: Header, Body, Cross- reference table (xref), and Trailer (Footer). Among these, the cross-reference table (xref table) plays a pivotal forensic role. The xref table contains byte offsets for every object stored in the PDF file, allowing the PDF reader--and forensic investigators--to locate objects directly without reading the entire file sequentially. This enables random access to objects such as text streams, images, embedded files, JavaScript, and form objects. Additionally, the xref table supports incremental updates, a mechanism frequently abused by attackers to append malicious content to a legitimate PDF without altering the original data. By analyzing multiple xref sections, investigators can identify document revisions, hidden objects, and malicious insertions.

186. Frage

.....