New 312-49v11 Test Answers | 312-49v11 Latest Test Practice

BTW, DOWNLOAD part of BraindumpsVCE 312-49v11 dumps from Cloud Storage: https://drive.google.com/open?id=1Qc0GoQQb9QZS0qNDndoi1p9ElxfS7lwN

These EC-COUNCIL 312-49v11 updated dumps are launched in the market after suggestions from experienced professionals. Therefore, this EC-COUNCIL 312-49v11 exam study material is kept to the point and concise. The EC-COUNCIL 312-49v11 practice material for Exams. Choice are essential for your successful learning. Often applicants for the exam run on a tight daily schedule before the final EC-COUNCIL 312-49v11 Exam, so actual Computer Hacking Forensic Investigator (CHFI-v11) exam questions are fruitful to prepare successfully on the first try.

EC-COUNCIL 312-49v11 Exam Syllabus Topics:

Topic	Details
Topic 1	• 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.
Topic 2	• 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.
Topic 3	• Data Acquisition and Duplication: This domain addresses live and dead acquisition techniques, eDiscovery methodologies, data acquisition formats, validation procedures, write protection, and forensic image preparation for examination.
Topic 4	• 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.

Topic 5	• 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.
Topic 6	• 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.
Topic 7	• 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.
Topic 8	• 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.

Quiz Accurate 312-49v11 - New Computer Hacking Forensic Investigator (CHFI-v11) Test Answers

We often receive news feeds and what well-known entrepreneurs have done to young people. The achievements of these entrepreneurs are the goals we strive for and we must value their opinions. And you may don't know that they were also benefited from our 312-49v11 study braindumps. We have engaged in this career for over ten years and helped numerous enterpreneurs achieved their 312-49v11 certifications toward their success. Just buy our 312-49v11 learning materials and you will become a big man as them.

EC-COUNCIL Computer Hacking Forensic Investigator (CHFI-v11) Sample Questions (Q77-Q82):

NEW QUESTION # 77
During an ongoing cybercrime investigation, a non-expert witness, who is an employee of the organization, testifies to observing unusual computer activity. Simultaneously, an expert witness introduces a record of the regularly conducted activity of the organization. The record was kept near the incident's time adept as part of the regular activity. It reveals a similar observation as the non-expert witness. How would the Federal Rules of Evidence classify and treat these testimonies in this scenario?

- A. The lay witness testimony is admissible under Rule 701, but the record is inadmissible hearsay under Rule 803(6)
- B. Both testimonies are admissible; the lay witness testimony is under Rule 701, and the record is under Rule 803(6)
- C. The lay witness testimony is inadmissible hearsay under Rule 801. but the record is admissible under Rule 803(6)
- D. Both testimonies are inadmissible; the lay witness testimony is hearsay under Rule 801, and the record is hearsay under Rule 803(6)

Answer: B

NEW QUESTION # 78
Robert needs to copy an OS disk snapshot of a compromised VM to a storage account in different region for further investigation. Which of the following should he use in this scenario?

- A. Azure Portal
- B. Azure Monitor
- C. Azure Active Directory
- D. Azure CLI

Answer: A

NEW QUESTION # 79
In a multinational corporation, there have been increasing reports of system crashes and data leaks from the intranet. Forensic investigators discovered a highly polymorphic worm propagating across the network. The worm quickly changes its structure, making it difficult to analyze its behavior and create signatures. Susan, a cybersecurity analyst, needs to conduct a behavioral analysis of the worm in a secure and controlled environment. Which of the following tools should she use for this purpose?

- A. Wireshark
- B. IDA Pro
- C. Cuckoo Sandbox
- D. Process Monitor

Answer: C

Explanation:
Option B. Cuckoo Sandbox is the best answer because CHFI v11 explicitly includes Malware Analysis:
Static and Dynamic , the Prominence of Setting up a Controlled Malware Analysis Lab , Preparing Testbed for Malware Analysis , and Tools to Perform Static and Dynamic Malware Analysis . The question specifically asks for behavioral analysis in a secure and controlled environment , which is the hallmark of sandbox-based dynamic malware analysis.
A polymorphic worm that changes structure rapidly is difficult to analyze with signature-based approaches alone, so observing its behavior in a sandbox is the most effective next step. Cuckoo Sandbox is designed for this type of controlled execution and can reveal process activity, file changes, registry modifications, network communications, and persistence behavior without exposing the production environment. Wireshark only captures network traffic. IDA Pro is a reverse engineering tool for code analysis. Process Monitor is useful for local system monitoring but does not provide the same isolated malware-analysis lab capability.
Therefore, under CHFI malware-forensics objectives, Cuckoo Sandbox is the strongest answer for secure behavioral analysis of the worm.

NEW QUESTION # 80
A Computer Hacking Forensic Investigator is acquiring volatile data from a Linux-based suspect machine that they cannot physically access. They need to obtain a dump of the system's RAM remotely. Which of the following sequences of commands and tools should be utilized for a forensically sound extraction?

- A. On the forensic workstation: insmod lime-.ko "path= format=lime"; on the suspect machine: nc : > filename.mem
- B. On the suspect machine: dd if=/dev/fmem of= bs=lMB; on the forensic workstation: nc -1 > filename.dd
- C. On the forensic workstation: nc -1 > filename.dd; on the suspect machine: dd if=/dev/fmem bs=l024 | nc
- D. On the suspect machine: insmod lime-.ko "path=tcp: format=lime": on the forensics workstation: nc : > filename.mem

Answer: D

NEW QUESTION # 81
A sophisticated cyber-attack has targeted an organization, and the forensic team is called upon for incident response. Their assets are largely hosted on AWS, particularly using S3 and EC2 instances. As a forensic investigator, your first step to retaining valuable evidence in the EC2 instances is:

- A. Encrypt all the data present in the EC2 instances to avoid further unauthorized access
- B. Immediately isolate the affected EC2 instances from the network to avoid data corruption
- C. Create a snapshot of the EBS volume in the affected EC2 instance and share it with the forensic team for analysis
- D. Retrieve and analyze log data from the affected EC2 instances

Answer: C

NEW QUESTION # 82
.....

In today's society, everyone wants to find a good job and gain a higher social status. As we all know, the internationally recognized 312-49v11 certification means that you have a good grasp of knowledge of certain areas and it can demonstrate your ability. This is

a fair principle. But obtaining this 312-49v11 certificate is not an easy task, especially for those who are busy every day. We do not charge extra service fees, but the service quality is high. Your satisfaction is the greatest affirmation for us and we sincerely serve you. Our 312-49v11 Exam Guide deliver the most important information in a simple, easy-to-understand language that you can learn efficiently learn with high quality. Whether you are a student or an in-service person, our 312-49v11 exam torrent can adapt to your needs.

312-49v11 Latest Test Practice: https://www.braindumpsvce.com/312-49v11_exam-dumps-torrent.html

DOWNLOAD the newest BraindumpsVCE 312-49v11 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=1Qc0GoQQb9QZS0qNDndoi1p9ElxfS7lwN