EC-COUNCIL 312-49v11考題套裝 - 312-49v11考試

從Google Drive中免費下載最新的Testpdf 312-49v11 PDF版考試題庫：https://drive.google.com/open?id=1rMj6JLc2ATWNziNMDN9mOMkWTWX95JBH

獲得 EC-COUNCIL EC-COUNCIL 認證對於考生而言有很多好處，相對于考生尋找工作而言，一張 EC-COUNCIL 的 312-49v11 認證會讓你倍受青睞的企業信任狀，帶來更好的工作機會。要想通過此認證學習過程中要注意方法，最重要的是需要毅力，如果有相關的工作經驗，學起來可能輕鬆一點，否則的話，你需要付出更多的勞動。EC-COUNCIL 的 312-49v11 證照作為全球IT領域專家 EC-COUNCIL 證照之一，是許多大中IT企業選擇人才標準的必備條件。

IT行業中很多雄心勃勃的專業人士為了在IT行業中能更上一層樓，離IT頂峰更近一步，都會選擇EC-COUNCIL 312-49v11這個難度較高的認證考試來獲取通認證證書從而獲得行業認可。EC-COUNCIL 312-49v11 的難度比較高所以通過率也比較低。但是報名參加EC-COUNCIL 312-49v11 認證考試是個明智的選擇，因為在如今競爭激烈的IT行業應該要不斷的提升自己。但是您可以選擇很多方式幫你通過考試。

>> EC-COUNCIL 312-49v11考題套裝 <<

312-49v11考試 & 312-49v11考古題推薦

312-49v11 擬真試題含蓋真實的考試指南，保證考生順利通過 312-49v11 考試。考生需要在一定的時間內完成所有

的 EC-COUNCIL 312-49v11 考試測驗題，該考試隸屬于EC-COUNCIL 認證助理認證體系。考生可以先到考試中心去打聽這科考試的有關的情況。了解考試的流程，考試的注意事項。預約一個合適的時間去報名參加 312-49v11 考試即可。

最新的 Certified Ethical Hacker 312-49v11 免費考試真題 (Q399-Q404):

問題 #399
You are a forensic analyst working on a case of a possible cyber-attack on a bank ' s network. You have been provided an image of the suspected machine for examination. To ensure a thorough investigation, you decided to use Autopsy for file system analysis. However, the image is huge, and manually sifting through the data could take weeks. What Autopsy feature can be utilized to expedite the analysis process?

- A. Image mounting
- B. Keyword search
- C. File carving
- D. Timeline analysis

答案：B

解題說明：
Option B. Keyword search is the best answer because the problem is the large volume of data and the need to expedite analysis . In CHFI v11, investigators are expected to use forensic tools efficiently to narrow evidence and find relevant artifacts quickly rather than reviewing everything manually. Keyword search is one of the most direct ways to locate names, account identifiers, project terms, malicious filenames, URLs, commands, or other case-relevant strings across a large disk image.
File carving helps recover deleted files, timeline analysis helps reconstruct activity order, and image mounting simply makes the image accessible. None of those is as immediately useful as keyword searching when the main challenge is reducing the workload of manual review in a huge dataset.
Because the question emphasizes speed and efficiency in analyzing a large image with Autopsy, the feature that most directly supports that goal is keyword search . It allows the examiner to focus quickly on relevant evidence and is consistent with CHFI's broader approach to efficient digital evidence analysis.

問題 #400
An investigator has found certain details after analysis of a mobile device. What can reveal the manufacturer information?

- A. Electronic Serial Number (ESN)
- B. International mobile subscriber identity (IMSI)
- C. Equipment Identity Register (EIR)
- D. Integrated circuit card identifier (ICCID)

答案：A

問題 #401
An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.

- A. Anti-Magnetic
- B. Logical
- C. Magnetic
- D. Optical

答案：D

問題 #402
Dariel, a forensic investigator, has been assigned to investigate a recent security incident that occurred within the organization's network. As part of the investigation, Dariel installs a command-line interface packet sniffer on a Unix-based system to monitor and capture network traffic, looking for signs of unauthorized access or malicious activity. The captured data will help Dariel identify the

sources of the security breach and trace the attacker's actions through the network. The tool used must be efficient for analyzing real-time network traffic and capable of running on a Unix-based operating system. Which of the following tools did Dariel employ in the above scenario?

- A. Metashield Analyzer
- B. tcpdump
- C. Billboard
- D. Timestomp

答案：B

解題說明：
According to the CHFI v11 curriculum underNetwork Forensics, investigators must be proficient in using packet sniffing tools to capture and analyze live network traffic.tcpdumpis a widely usedcommand-line packet analyzerthat runs natively on Unix, Linux, and BSD-based systems. It allows investigators to capture packets in real time, apply powerful filters, and save traffic inPCAP formatfor further offline analysis using tools such as Wireshark.
In forensic investigations, tcpdump is especially valuable because it provides low-level visibility into network communications, including source and destination IP addresses, ports, protocols, TCP flags, and payload data.
This enables investigators to detect suspicious behaviors such as unauthorized connections, port scans, malware command-and-control traffic, data exfiltration attempts, and denial-of-service activities. CHFI v11 specifically highlightstcpdumpas a core tool fornetwork traffic investigation and evidence gatheringin Unix-based environments.
The other options are incorrect. Metashield Analyzer is used for file-based threat analysis, Timestomp is an anti-forensics tool used to manipulate file timestamps, and Billboard is not a recognized network forensic or packet sniffing tool.
The CHFI Exam Blueprint v4 emphasizes the importance ofreal-time packet capture toolsfor network investigations, makingtcpdumpthe correct, forensically sound, and exam-aligned answer

問題 #403
A cybersecurity investigator is analyzing a suspected dark web transaction involving illegal activities. However, the investigator struggles to find conclusive data due to Tor's onion routing and encryption. What is a specific feature of the Tor network that might help explain why the original source of this transaction is hard to trace?

- A. The Tor network only includes the entry/guard relay, hence making the data origin untraceable
- B. The exit relay of the Tor network is perceived to be the origin of the data by the destination server
- C. The Tor network uses the hidden service protocol, allowing users to host websites anonymously
- D. Tor relay nodes are not publicly available, thereby preventing data origin identification

答案：B

問題 #404
.....

Computer Hacking Forensic Investigator (CHFI-v11)

現在馬上去網站下載免費試用版本，你就會相信自己的選擇不會錯，我們完全保312-49v11障客戶隱私，尊重用戶個人隱私是Testpdf的基本政策，我們不會在未經合法用戶授權公開、編輯或透露其註冊資料及保存在本網站中的非公開信息。