212-89시험대비덤프문제, 212-89적중율높은시험대비덤프

그리고 ITDumpsKR 212-89 시험 문제집의 전체 버전을 클라우드 저장소에서 다운로드할 수 있습니다: https://drive.google.com/open?id=14-YCRfznIapQl1Y3Ch4nvyOOLgvsBJ_0

EC-COUNCIL 212-89인증덤프는 최근 출제된 실제시험문제를 바탕으로 만들어진 공부자료입니다. EC-COUNCIL 212-89 시험문제가 변경되면 제일 빠른 시일내에 덤프를 업데이트하여 최신버전 덤프자료를EC-COUNCIL 212-89 덤프를 구매한 분들께 보내드립니다. 시험탈락시 덤프비용 전액환불을 약속해드리기에 안심하시고 구매하셔도 됩니다.

ECIH 인증 시험은 사고 관리 프로세스, 위험 평가 방법론, 사고 대응 프레임 워크 등을 포함한 광범위한 주제를 다룹니다. 맬웨어 공격, 네트워크 침입 및 데이터 유출을 포함한 다양한 유형의 보안 사고를 식별, 평가 및 대응하는 후보자의 숙련도를 테스트하도록 설계되었습니다. 인증은 업계에서 높은 존경을 받고 있으며, 전 세계 고용주들이 사고 대응 및 취급의 우수성으로 인정 받고 있습니다.

>> 212-89시험대비 덤프문제 <<

EC-COUNCIL 212-89적중율 높은 시험대비덤프, 212-89최신 업데이트버전 덤프문제공부

비스를 제공해드려 아무런 걱정없이 212-89시험에 도전하도록 힘이 되어드립니다. ITDumpsKR덤프를 사용하여 시

험에서 통과하신 분이 전해주신 희소식이 ITDumpsKR 덤프품질을 증명해드립니다.

최신 ECIH Certification 212-89 무료샘플문제 (Q198-Q203):

질문 # 198
Which of the following is not called volatile data?

- A. Creation dates of files
- B. The dale a no Lime of the system
- C. State of the network interface
- D. Open sockets er open ports

정답：A

설명：
Volatile data refers to information that is stored temporarily and is lost when a computer is turned off or restarted, such as RAM contents, including open sockets and open ports, the date and time of the system, and the state of the network interface. The creation dates of files, however, are considered non-volatile data because they are preserved on the hard drive and remain available after the system is restarted or turned off.
Non-volatile data is stored on persistent storage mediums like hard drives, SSDs, and magnetic tapes, where it remains until it is deleted or overwritten.References:The Incident Handler (ECIH v3) certification emphasizes the distinction between volatile and non-volatile data in the context of digital forensics and incident response, highlighting the importance of understanding what data may be lost upon system shutdown and what data persists.

질문 # 199
Which of the following techniques against insider threats identifies events that are related to suspicious activity?

- A. Normalization
- B. Correlation
- C. Anomaly detection
- D. Pattern discovery

정답：C

질문 # 200
Farheen is an incident responder at reputed IT Firm based in Florida. Farheen was asked to investigate a recent cybercrime faced by the organization. As part of this process, she collected static data from a victim system. She used DD tool command to perform forensic duplication to obtain an NTFS image of the original disk. She created a sector-by-sector mirror imaging of the disk and saved the output image file as image.dd.
Identify the static data collection process step performed by Farheen while collecting static data.

- A. Physical presentatio
- B. Comparison
- C. System preservation
- D. Administrative consideration

정답：C

설명：
Farheen's activity of using the DD tool to create a sector-by-sector mirror image of the original disk is an example of system preservation. This process is crucial in digital forensics for creating an exact copy of a storage device to ensure that the original data remains unchanged during the investigation. By making a forensic duplication, or image, of the disk, Farheen ensures that the static data on the disk is preserved in its current state for thorough analysis, without altering the original evidence. This step allows investigators to work with a precise replica of the data, protecting the integrity of the original evidence.
References:The Incident Handler (ECIH v3) certification materials discuss various methods and tools for data acquisition and preservation, highlighting the importance of system preservation in the initial stages of forensic analysis.

질문 # 201
Drake is an incident handler at Dark Cloud Inc. He is tasked with performing log analysis to detect traces of malicious activities within the network infrastructure.
Which of the following tools should Drake employ to view logs in real time and identify malware propagation within the network?

- A. Splunk
- B. HULK
- C. Hydra
- D. LOIC

정답：A

질문 # 202
Alexis works as an incident responder at XYZ organization. She was asked to identify and attributethe actors behind an attack that occurred recently. For this purpose, she is performing a type of threat attribution that deals with the identification of a specific person, society, or country sponsoring a well-planned and executed intrusion or attack on its target. Which of the following types of threat attributions is Alexis performing?

- A. Campaign attribution
- B. Intrusion set attribution
- C. Nation-state attribution
- D. True attribution

정답：C

설명：
Nation-state attribution involves identifying a specific country or government as the sponsor behind a cyber-attack or intrusion. This type of threat attribution is focused on determining the involvement of state actors in cyber operations against specific targets, which often involves sophisticated, well-planned, and executed cyber campaigns. Alexis's efforts to identify and attribute the actors behind the attack to a specific nation-state fall under this category, as she seeks to uncover the geopolitical motives and the extent of state sponsorship behind the incident. Nation-state attribution requires analyzing a variety of indicators, including technical evidence, tactics, techniques, and procedures (TTPs), and contextual intelligence. This is distinct from campaign attribution, which focuses on linking attacks to a specific campaign or operation, true attribution, which aims at identifying the actual individuals behind an attack, and intrusion set attribution, which involves attributing a set of malicious activities to a particular threat actor or group.References:The Incident Handler (ECIH v3) certification program includes discussions on various types of threat attributions, highlighting the challenges and methodologies involved in attributing cyber-attacks to specific actors, including nation-states.

질문 # 203
.....

212-89시험대비 덤프문제 100% 유효한 덤프

212-89인증시험을 어떻게 패스할지 고민하고 계시나요, EC-COUNCIL인증 212-89시험준비중이신 분들은EC-COUNCIL인증 212-89시험통과가 많이 어렵다는것을 알고 있을것입니다, ITDumpsKR의 인지도는212-89고객님께서 상상하는것보다 훨씬 높습니다.많은 분들이ITDumpsKR의 덤프공부가이드로 IT자격증 취득의 꿈을 이루었습니다.

ITDumpsKR는 여러분이 EC-COUNCIL인증212-89시험 패스와 추후사업에 모두 도움이 되겠습니다.ITDumpsKR제품을 선택함으로 여러분은 시간과 돈을 절약하는 일석이조의 득을 얻을수 있습니다.

- 212-89시험대비 덤프문제 시험대비 덤프공부자료 □ □ www.pass4test.net □웹사이트를 열고➡ 212-89 □□□를 검색하여 무료 다운로드212-89시험패스 가능 덤프문제
- 212-89합격보장 가능 인증덤프 □ 212-89시험패스 가능한 인증덤프자료 □ 212-89높은 통과율 인기 덤프문제 □ “ www.itdumpskr.com ”을 통해 쉽게⇛ 212-89 ⇚무료 다운로드 받기212-89높은 통과율 인기 덤프문제
- 212-89합격보장 가능 인증덤프 □ 212-89시험준비자료 □ 212-89시험준비자료 □ □ kr.fast2test.com □을(를) 열고「 212-89 」를 검색하여 시험 자료를 무료로 다운로드하십시오212-89최신버전 공부자료
- 212-89시험대비 덤프문제 시험대비 덤프공부자료 □ ➤ www.itdumpskr.com □에서▹ 212-89 ◃를 검색하고 무료 다운로드 받기212-89최고품질 덤프자료
- 212-89인기자격증 시험덤프 □ 212-89유효한 덤프문제 □ 212-89유효한 덤프문제 □ □ www.koreadumps.com □에서➥ 212-89 □를 검색하고 무료 다운로드 받기212-89높은 통과율 인기 덤프문제
- 212-89최신버전 덤프자료 □ 212-89최신버전 공부자료 □ 212-89완벽한 공부자료 □ 「 www.itdumpskr.com 」에서 검색만 하면⇛ 212-89 ⇚를 무료로 다운로드할 수 있습니다212-89최고패스자료
- 212-89유효한 덤프문제 □ 212-89퍼펙트 최신 덤프자료 □ 212-89시험준비자료 □ 지금➽ www.koreadumps.com □을(를) 열고 무료 다운로드를 위해《 212-89 》를 검색하십시오212-89최신버전 시험덤프문제
- 212-89높은 통과율 시험대비자료 □ 212-89높은 통과율 인기 덤프문제 □ 212-89완벽한 공부자료 □ ➠ www.itdumpskr.com □에서➡ 212-89 □□□를 검색하고 무료로 다운로드하세요212-89최신 업데이트 시험공부자료
- 최신 업데이트된 212-89시험대비 덤프문제 시험공부자료 □ □ www.itdumpskr.com □을 통해 쉽게「 212-89 」무료 다운로드 받기212-89최고품질 덤프자료
- 212-89시험대비 덤프문제 시험준비에 가장 좋은 인기 인증시험자료 □ ➽ www.itdumpskr.com □을(를) 열고 ▸ 212-89 ◂를 검색하여 시험 자료를 무료로 다운로드하십시오212-89높은 통과율 시험대비자료
- 212-89최신 업데이트 시험공부자료 □ 212-89최신버전 덤프자료 🤚 212-89최고패스자료 □ 무료 다운로드를 위해➡ 212-89 □를 검색하려면☀ www.exampassdump.com □☀□을(를) 입력하십시오212-89최고품질 덤프자료
- sjbdirectory.com, andrewyywb508079.elbloglibre.com, socialmediaentry.com, deannartdy524947.59bloggers.com, letsbookmarkit.com, imogenoekc248421.tokka-blog.com, adreagofr486761.salesmanwiki.com, chiaranfkj631266.daneblogger.com, donnanbep960517.wikitelevisions.com, esocialmall.com, Disposable vapes

BONUS!!! ITDumpsKR 212-89 시험 문제집 전체 버전을 무료로 다운로드하세요: https://drive.google.com/open?id=14-YCRfznIapQl1Y3Ch4nvyOOLgvsBJ_0