212-89新版題庫上線，212-89證照考試

P.S. Testpdf在Google Drive上分享了免費的、最新的212-89考試題庫：https://drive.google.com/open?id=150L0Sgr6I5tPUpOOU6me41yTExaHXKOA

如果你想通過困難的212-89認證考試，那麼在準備考試時不使用相關考試資料是絕對不行的。如果你想找到適合你自己的優秀的資料，那麼你最應該來的地方就是Testpdf。Testpdf的知名度很高，擁有很多與IT認證相關的優秀的考試考古題。而且所有的考古題都免費提供demo。如果你想知道Testpdf的考古題是不是適合你，那麼先下載考古題的demo體驗一下吧。

EC Council Certified Incident Handler（ECIH v2）認證是一項入門級的网络安全認證，專注於事件處理和應對。該認證由 EC-Council 提供，EC-Council 是网络安全領域的一家領先國際組織。ECIH v2 認證旨在為個人提供識別、應對和解決网络安全事件所需的知識和技能。

ECIH v2認證考試是一個選擇題考試，共有100道題目。考試時間為四個小時，考生必須得分至少70%才能通過考試。該考試是基於計算機的，並在全球授權的測試中心進行。

EC-COUNCIL 212-89 認證考試涵蓋了許多與事件處理相關的主題，包括事件回應流程和程序、數位取證、網路安全基礎和漏洞管理。該考試由 100 道多選題組成，考生有兩個小時的時間完成。該考試是基於電腦的，可以在 EC-COUNCIL 授權的測試中心之一進行考試。

>> 212-89新版題庫上線 <<

212-89證照考試 - 212-89認證考試解析

作好充分的 212-89 考試準備，對考生取得 EC-COUNCIL 的證照很有幫助。在評估新的候選者或考量現有人員的專業能力時，雇主認同 212-89 認證的價值。這些認證提供了要在您的職涯中出類拔萃所需的認可，並且提供雇主驗證您的技能。Testpdf 212-89 考試測試引擎試用，讓您可以模擬真實的考試情景，可以快速讓您掌握並應用。保證考生一次性通過考試！

最新的 ECIH Certification 212-89 免費考試真題 (Q260-Q265):

問題 #260
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. Comparison
- B. System preservation
- C. Administrative consideration
- D. Physical presentatio

答案：B

解題說明：

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.

問題 #261
Investigator Ian gives you a drive image to investigate. What type of analysis are you performing?

- A. Live
- B. Real-time
- C. Dynamic
- D. Static

答案：D

問題 #262
Marley was asked by his incident handing and response (IH&R) team lead to collect volatile data such as system information and network information present in the registries, cache, and RAM of victim's system.
Identify the data acquisition method Marley must employ to collect volatile data.

- A. Validate data acquisition
- B. Static data acquisition
- C. Remote data acquisition
- D. Live data acquisition

答案：D

問題 #263
Eve's is an incident handler in ABC organization. One day, she got a complaint about email hacking incident from one of the employees of the organization. As a part of incident handling and response process, she must follow many recovery steps in order to recover from incident impact to maintain business continuity.
What is the first step that she must do to secure employee account?

- A. Enable two-factor authentication
- B. Disabling automatic file sharing between the systems
- C. Restore the email services and change the password
- D. Enable scanning of links and attachments in all the emails

答案：C

解題說明：
The first step in securing an employee's account following an email hacking incident involves restoring access to the email services if necessary and immediately changing the password to prevent unauthorized access.
This action ensures that the attacker is locked out of the account as quickly as possible. While enabling two- factor authentication, scanning links and attachments, and disabling automatic file sharing are important security measures, they come into play after ensuring that the compromised account is first secured by changing its password to halt any ongoing unauthorized access.
References:The ECIH v3 certification materials cover the initial steps to be taken when responding to incidents involving compromised accounts, emphasizing the importance of quickly changing passwords to secure the accounts against further unauthorized access.

問題 #264
Authorized users with privileged access who misuse the corporate informational assets and directly affects the confidentiality, integrity, and availability of the assets are known as:

- A. Outsider threats
- B. Social Engineers
- C. Insider threats
- D. Zombies

答案：C

問題 #265

.....

有很多網站提供資訊EC-COUNCIL的212-89考試，為你提供 EC-COUNCIL的212-89考試認證和其他的培訓資料，Testpdf是唯一的網站，為你提供優質的EC-COUNCIL的212-89考試認證資料，在Testpdf指導和幫助下，你完全可以通過你的第一次EC-COUNCIL的212-89考試，我們Testpdf提供的試題及答案是由現代和充滿活力的資訊技術專家利用他們的豐富的知識和不斷積累的經驗，為你的未來在IT行業更上一層樓。

212-89證照考試: https://www.testpdf.net/212-89.html

- 最新212-89題庫資源 □ 212-89題庫資料 □ 212-89考古題分享 □ 立即在➥ www.newdumpspdf.com □上搜尋“212-89 ”並免費下載212-89題庫下載
- 212-89考題寶典 ➡□ 212-89最新題庫 □ 212-89考試題庫 □ 透過【 www.newdumpspdf.com 】輕鬆獲取⇒ 212-89 ⇐免費下載212-89題庫下載
- 真正全新的212-89考古題 - 順利通過EC Council Certified Incident Handler (ECIH v3) - 212-89考試 □ { www.pdfexamdumps.com }上的《 212-89 》免費下載只需搜尋212-89考古題更新
- 真實的EC-COUNCIL 212-89：EC Council Certified Incident Handler (ECIH v3)新版題庫上線 - 完美的Newdumpspdf 212-89證照考試 □ ➠ www.newdumpspdf.com □上的□ 212-89 □免費下載只需搜尋212-89考試資訊
- 212-89熱門考古題 □ 最新212-89題庫資源 □ 212-89在線考題 □ 到「 www.newdumpspdf.com 」搜尋⇒ 212-89 ⇐以獲取免費下載考試資料212-89資訊
- 使用真實的EC-COUNCIL 212-89新版題庫上線準備您的EC-COUNCIL 212-89考試，輕松通過 □ 複製網址 ✔ www.newdumpspdf.com □✔□打開並搜索“212-89 ”免費下載212-89在線考題
- 212-89考古題更新 □ 新版212-89題庫上線 □ 212-89 PDF題庫 □ ➤ www.vcesoft.com □是獲取[212-89]免費下載的最佳網站212-89考古題更新
- 212-89最新題庫 □ 212-89考試指南 □ 212-89資訊 □ 打開網站➽ www.newdumpspdf.com □搜索[212-89]免費下載212-89在線考題
- 最新更新的212-89新版題庫上線和資格考試的領導者與專業的212-89：EC Council Certified Incident Handler (ECIH v3) □ 立即到[www.newdumpspdf.com]上搜索《 212-89 》以獲取免費下載212-89考題寶典
- 212-89在線題庫 □ 212-89考試指南 □ 212-89考古題分享 □ 透過➥ www.newdumpspdf.com □輕鬆獲取{ 212-89 }免費下載最新212-89題庫
- 優秀的212-89新版題庫上線和資格考試中的領先材料供應商＆最熱門的212-89證照考試 □ 請在□ www.newdumpspdf.com □網站上免費下載✔ 212-89 □✔□題庫212-89題庫下載
- 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, myportal.utt.edu.tt, www.stes.tyc.edu.tw, 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, animentor.in, 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, myportal.utt.edu.tt, Disposable vapes

從Google Drive中免費下載最新的Testpdf 212-89 PDF版考試題庫：https://drive.google.com/open?id=150L0Sgr6I5tPUpOOU6me41yTExaHXKOA