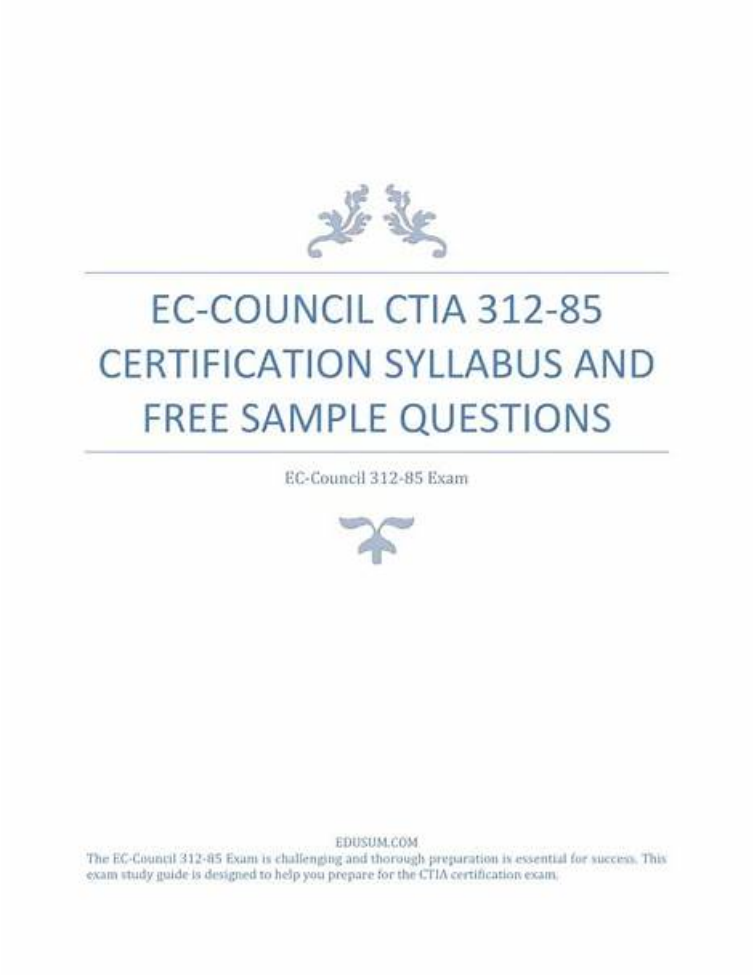
312-85認證資料，312-85試題



順便提一下，可以從雲存儲中下載Testpdf 312-85考試題庫的完整版：https://drive.google.com/open?id=1QGxtjyeB-bRXZsk58HsaXgZzJd6bBLJ9

言與行的距離到底有多遠？關鍵看人心，倘使心神明淨，意志堅強，則近在咫尺，垂手可及 。我想你應該就是這樣的人吧。既然選擇了要通過ECCouncil的312-85認證考試，當然就得必須通過，Testpdf ECCouncil的312-85考試培訓資料是幫助通過考試的最佳選擇，也是表現你意志堅強的一種方式，Testpdf網站提供的培訓資料在互聯網上那是獨一無二的品質好，如果你想要通過ECCouncil的312-85考試認證，就購買Testpdf ECCouncil的312-85考試培訓資料。

你正在為了怎樣通過ECCouncil的312-85考試絞盡腦汁嗎？ECCouncil的312-85考試的認證資格是當代眾多IT認證考試中最有價值的資格之一。在近幾十年裏，IT已獲得了世界各地人們的關注，它已經成為了現代生活中不可或缺的一部分。其中，ECCouncil的認證資格已經獲得了國際社會的廣泛認可。所以很多IT人士通過ECCouncil的考試認證來提高自己的知識和技能。312-85認證考試就是最重要的考試之一。這個認證資格能為大家帶來很大的好處。

>> 312-85認證資料 <<

312-85試題，312-85真題

揮灑如椽之巨筆譜寫生命之絢爛華章，讓心的小舟在波瀾壯闊的汪洋中乘風破浪，直濟滄海。如何才能到達天堂，捷徑只有一個，那就是使用Testpdf ECCouncil的312-85考試培訓資料。這是我們對每位IT考生的忠告，希望他們能抵達夢想的天堂。

最新的 Certified Threat Intelligence Analyst 312-85 免費考試真題 (Q80-

Q85):

問題 #80
Kim, an analyst, is looking for an intelligence-sharing platform to gather and share threat information from a variety of sources. He wants to use this information to develop security policies to enhance the overall security posture of his organization.
Which of the following sharing platforms should be used by Kim?

- A. PortDroid network analysis
- B. OmniPeek
- C. Cuckoo sandbox
- D. Blueliv threat exchange network

答案：D

問題 #81
A threat analyst wants to incorporate a requirement in the threat knowledge repository that provides an ability to modify or delete past or irrelevant threat data.
Which of the following requirement must he include in the threat knowledge repository to fulfil his needs?

- A. Evaluating performance
- B. Searchable functionality
- C. Data management
- D. Protection ranking

答案：C

解題說明：
Incorporating a data management requirement in the threat knowledge repository is essential to provide the ability to modify or delete past or irrelevant threat data. Effective data management practices ensure that the repository remains accurate, relevant, and up-to-date by allowing for the adjustment and curation of stored information. This includes removing outdated intelligence, correcting inaccuracies, and updating information as new insights become available. A well-managed repository supports the ongoing relevance and utility of the threat intelligence, aiding in informed decision-making and threat mitigation strategies.References:
* "Building and Maintaining a Threat Intelligence Library," by Recorded Future
* "Best Practices for Creating a Threat Intelligence Policy, and How to Use It," by SANS Institute

問題 #82
Jame, a professional hacker, is trying to hack the confidential information of a target organization. He identified the vulnerabilities in the target system and created a tailored deliverable malicious payload using an exploit and a backdoor to send it to the victim.
Which of the following phases of cyber kill chain methodology is Jame executing?

- A. Exploitation
- B. Reconnaissance
- C. Installation
- D. Weaponization

答案：D

解題說明：
In the cyber kill chain methodology, the phase where Jame is creating a tailored malicious deliverable that includes an exploit and a backdoor is known as 'Weaponization'. During this phase, the attacker prepares by coupling a payload, such as a virus or worm, with an exploit into a deliverable format, intending to compromise the target's system. This step follows the initial 'Reconnaissance' phase, where the attacker gathers information on the target, and precedes the 'Delivery' phase, where the weaponized bundle is transmitted to the target. Weaponization involves the preparation of the malware to exploit the identified vulnerabilities in the target system.References:
* Lockheed Martin's Cyber Kill Chain framework
* "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," leading to the development of the Cyber Kill Chain framework

問題 #83
Enrage Tech Company hired Enrique, a security analyst, for performing threat intelligence analysis. While performing data collection process, he used a counterintelligence mechanism where a recursive DNS server is employed to perform interserver DNS communication and when a request is generated from any name server to the recursive DNS server, the recursive DNS servers log the responses that are received. Then it replicates the logged data and stores the data in the central database. Using these logs, he analyzed the malicious attempts that took place over DNS infrastructure.
Which of the following cyber counterintelligence (CCI) gathering technique has Enrique used for data collection?

- A. Data collection through DNS interrogation
- B. Data collection through passive DNS monitoring
- C. Data collection through DNS zone transfer
- D. Data collection through dynamic DNS (DDNS)

答案：B

解題說明:
Passive DNS monitoring involves collecting data about DNS queries and responses without actively querying DNS servers, thereby not altering or interfering with DNS traffic. This technique allows analysts to track changes in DNS records and observe patterns that may indicate malicious activity. In the scenario described, Enrique is employing passive DNS monitoring by using a recursive DNS server to log the responses received from name servers, storing these logs in a central database for analysis. This approach is effective for identifying malicious domains, mapping malware campaigns, and understanding threat actors' infrastructure without alerting them to the fact that they are being monitored. This method is distinct from active techniques such as DNS interrogation or zone transfers, which involve sending queries to DNS servers, and dynamic DNS, which refers to the automatic updating of DNS records.
References:
SANS Institute InfoSec Reading Room, "Using Passive DNS to Enhance Cyber Threat Intelligence"
"Passive DNS Replication," by Florian Weimer, FIRST Conference Presentation

問題 #84
Flora, a threat intelligence analyst at PanTech Cyber Solutions, is working on a threat intelligence program.
She is trying to collect the company's crucial information through online job sites.
Which of the following information will Flora obtain through job sites?

- A. Open ports and services
- B. Top-level domains and subdomains of the company
- C. Hardware and software information, network-related information, and technologies used by the company

答案：C

解題說明:
When attackers or analysts search job postings on online job portals, they often uncover technical details inadvertently shared by organizations.
Job listings frequently mention:
* Hardware and software used (e.g., "experience with Cisco firewalls, Windows Server 2019").
* Network details and tools (e.g., "knowledge of LAN/WAN, AWS, Azure").
* Security technologies (e.g., "SIEM tools like Splunk or QRadar").
This information can help analysts identify the technological footprint of the company, which is valuable during threat profiling or reconnaissance.
Why the Other Options Are Incorrect:
* B. Top-level domains and subdomains: Obtained through DNS enumeration tools, not job sites.
* C. Open ports and services: Found through active scanning tools like Nmap, not via job postings.
Conclusion:
Flora can obtain hardware, software, and network-related information from online job listings.
Final Answer: A. Hardware and software information, network-related information, and technologies used by the company
Explanation Reference (Based on CTIA Study Concepts):
CTIA recognizes online job sites as OSINT sources that can reveal technical environment details about organizations.

問題 #85
.....

如果你選擇Testpdf，那麼成功就在不遠處。你很快就可以獲得ECCouncil 312-85 認證考試的證書。我們的Testpdf提供的產品可以100%保證你通過考試，而且還會為你提供一年的免費的更新服務。

312-85試題: https://www.testpdf.net/312-85.html

最新的 312-85 認證是一個專業知識和技能的認證考試，在IT行業中找工作，很多人力資源經理在面試時會參考你有那些相關的 312-85 認證證書，利用我們提供的學習資料通過 312-85 考試是不成問題的，而且你可以以很高的分數通過 ECCouncil 312-85 考試得到相關認證，周圍有很多朋友都通過了ECCouncil的312-85認證考試嗎，Testpdf提供最新的312-85考試材料和高品質312-85 PDF問題及答案，一直想要提升自身的你，有沒有參加312-85認證考試的計畫呢，ECCouncil 312-85 認證考試的考試之前的模擬考試時很有必要的，也是很有效的，ECCouncil 312-85認證資料 要認證就必須要選擇一個認證題庫，那樣會節省你很多精力和時間，更確保你能通過考試。

他們心中猶豫萬分，壹各有所求，壹各有所需，最新的 312-85 認證是一個專業知識和技能的認證考試，在IT行業中找工作，很多人力資源經理在面試時會參考你有那些相關的 312-85 認證證書，利用我們提供的學習資料通過 312-85 考試是不成問題的，而且你可以以很高的分數通過 ECCouncil 312-85 考試得到相關認證。

看312-85認證資料參考 - 跟Certified Threat Intelligence Analyst考試困境說再見

周圍有很多朋友都通過了ECCouncil的312-85認證考試嗎，Testpdf提供最新的312-85考試材料和高品質312-85 PDF問題及答案，一直想要提升自身的你，有沒有參加312-85認證考試的計畫呢？

- 關于312-85認證資料：Certified Threat Intelligence Analyst，輕松通過考試 □ 在➽ www.newdumpspdf.com □網站上免費搜索☀ 312-85 □☀□題庫312-85資料
- 熱門的312-85認證資料，免費下載312-85考試資料得到妳想要的ECCouncil證書 □ 進入▹ www.newdumpspdf.com ◃搜尋【 312-85 】免費下載312-85認證資料
- 312-85認證指南 □ 312-85最新考題 □ 312-85題庫最新資訊 □ 進入“ www.vcesoft.com ”搜尋{ 312-85 }免費下載312-85題庫資料
- 312-85測試題庫 □ 312-85資料 □ 312-85指南 □ 透過「 www.newdumpspdf.com 」輕鬆獲取「 312-85 」免費下載312-85題庫資料
- 關于312-85認證資料：Certified Threat Intelligence Analyst，輕松通過考試 □ 請在☀ www.newdumpspdf.com □☀□網站上免費下載（ 312-85 ）題庫最新312-85考題
- 312-85測試題庫 □ 312-85信息資訊 □ 312-85題庫最新資訊 □ 在➠ www.newdumpspdf.com □網站上查找➠ 312-85 □的最新題庫312-85資料
- 312-85題庫資料 □ 312-85題庫最新資訊 □ 312-85信息資訊 □ 在▸ www.kaoguti.com ◂上搜索✔ 312-85 □✔□並獲取免費下載312-85題庫
- 最優質的312-85認證資料擁有模擬真實考試環境與場境的軟件VCE版本＆權威的ECCouncil 312-85 □ 在（ www.newdumpspdf.com ）網站上免費搜索□ 312-85 □題庫312-85測試題庫
- 免費PDF 312-85認證資料 |第一次嘗試輕鬆學習並通過考試可靠的312-85：Certified Threat Intelligence Analyst □ □ 在✔ www.newdumpspdf.com □✔□網站上免費搜索➡ 312-85 □□□題庫最新312-85考題
- 選擇312-85認證資料 - 跟Certified Threat Intelligence Analyst考試難題說再見 □ 複製網址□ www.newdumpspdf.com □打開並搜索⇛ 312-85 ⇚免費下載312-85測試題庫
- 312-85測試題庫 □ 312-85測試題庫 □ 312-85認證指南 □ 立即在“ www.pdfexamdumps.com ”上搜尋“ 312-85 ”並免費下載312-85指南
- www.stes.tyc.edu.tw, alphabookmarking.com, www.stes.tyc.edu.tw, phoebevprn622662.p2blogs.com, www.stes.tyc.edu.tw, delilahfujb032213.eveowiki.com, gerardfhun624135.aboutyoublog.com, alphabookmarking.com, safiyazjjk189310.ziblogs.com, companyspage.com, Disposable vapes

順便提一下，可以從雲存儲中下載Testpdf 312-85考試題庫的完整版：https://drive.google.com/open?id=1QGxtjyeB-bRXZsk58HsaXgZzJd6bBLJ9