ECCouncil 312-50v13熱門考題 & 312-50v13證照資訊

P.S. VCESoft在Google Drive上分享了免費的2025 ECCouncil 312-50v13考試題庫：https://drive.google.com/open?id=1pOUBBoYNIf-_pFDpGn0owey2pEFD89f8

彰顯一個人在某一領域是否成功往往體現在他所獲得的資格證書上，在IT行業也不外如是。所以現在很多人都選擇參加312-50v13資格認證考試來證明自己的實力。但是要想通過312-50v13資格認證卻不是一件簡單的事。不過只要你找對了捷徑，通過考試也就變得容易許多了。這就不得不推薦VCESoft的考試考古題了，它可以讓你少走許多彎路，節省時間幫助你考試合格。

IT專業技術認證是進入IT行業的“敲門磚”。由國際著名IT企業頒發的職業證書，證明了你具有某種專業IT技能，為國際承認並通用。這些國際著名 IT企業為：Microsoft、Oracle、Cisco、Amazon、IBM、Oracle等。312-50v13 考試就是其中一個流行的 ECCouncil 認證。許多考生對這門考試沒有什麼信心，其實，312-50v13 最新的擬真試題是用最快和最聰明的的方式來傳遞您的考試，並幫助您獲得 ECCouncil 312-50v13 認證。

>> ECCouncil 312-50v13熱門考題 <<

優秀的312-50v13熱門考題和資格考試中的領先供應商和快速下載 ECCouncil Certified Ethical Hacker Exam (CEHv13)

VCESoft提供有保證的題庫資料，以提高您的ECCouncil 312-50v13考試的通過率，您可以認識到我們產品的真正價值。如果您想參加312-50v13考試，請選擇我們最新的312-50v13題庫資料，該題庫資料具有針對性，不僅品質是最高的，而且內容是最全面的。對于那些沒有充分的時間準備考試的考生來說，ECCouncil 312-50v13考古題就是您唯一的、也是最好的選擇，這是一個高效率的學習資料，312-50v13可以讓您在短時間內為考試做好充分的準備。

最新的 CEH v13 312-50v13 免費考試真題 (Q48-Q53):

問題 #48
Tremp is an IT Security Manager planning to deploy an IDS. He needs a solution that:
Verifies success/failure of an attack
Monitors system activities
Detects local (host-based) attacks
Provides near real-time detection
Doesn't require additional hardware
Has a lower entry cost
Which type of IDS is best suited for Tremp's requirements?

- A. Host-based IDS
- B. Network-based IDS
- C. Gateway-based IDS

- D. Open source-based

答案： A

解題說明：
Comprehensive and Detailed Explanation:
Host-based Intrusion Detection Systems (HIDS) run on individual hosts and monitor activities like file access, processes, and system logs. HIDS:
Detects attacks missed by NIDS (e.g., insider threats, encrypted traffic) Monitors integrity of system files Works in near real-time Requires no additional network hardware Can be implemented at low cost From CEH v13 Courseware:
Module 13: IDS, Firewalls and Honeypots # Types of IDS (HIDS vs. NIDS)
Reference:CEH v13 Study Guide - Host-Based IDS Capabilities

問題 #49
A large e-commerce organization is planning to implement a vulnerability assessment solution to enhance its security posture. They require a solution that imitates the outside view of attackers, performs well-organized inference-based testing, scans automatically against continuously updated databases, and supports multiple networks. Given these requirements, which type of vulnerability assessment solution would be most appropriate?

- A. Product-based solution installed on a private network
- B. Service-based solution offered by an auditing firm
- C. Inference-based assessment solution
- D. Tree-based assessment approach

答案： B

解題說明：
A service-based solution offered by an auditing firm would be the most appropriate type of vulnerability assessment solution for the large e-commerce organization, given their requirements. A service-based solution is a type of vulnerability assessment that is performed by external experts who have the skills, tools, and experience to conduct a thorough and comprehensive analysis of the target system or network. A service- based solution can imitate the outside view of attackers, as the experts are not familiar with the internal details or configurations of the organization. A service-based solution can also perform well-organized inference- based testing, which is a type of testing that uses logical reasoning and deduction to identify and exploit vulnerabilities based on the information gathered from the target. A service-based solution can scan automatically against continuously updated databases, as the experts have access to the latest security intelligence and threat feeds. A service-based solution can also support multiple networks, as the experts can use different techniques and tools to scan different types of networks, such as wired, wireless, cloud, or hybrid12.
The other options are not as appropriate as option B for the following reasons:
* A. Inference-based assessment solution: This option is not a type of vulnerability assessment solution, but a type of testing method that can be used by any solution. Inference-based testing is a testing method that uses logical reasoning and deduction to identify and exploit vulnerabilities based on the information gathered from the target. Inference-based testing can be performed by service-based, product-based, or tree-based solutions, depending on the scope, objectives, and resources of the assessment3.
* C. Tree-based assessment approach: This option is not a type of vulnerability assessment solution, but a type of testing method that can be used by any solution. Tree-based testing is a testing method that uses a hierarchical structure to organize and prioritize the vulnerabilities based on their severity, impact, and exploitability. Tree-based testing can be performed by service-based, product-based, or inference-based solutions, depending on the scope, objectives, and resources of the assessment4.
* D. Product-based solution installed on a private network: This option is a type of vulnerability assessment solution, but it may not meet all the requirements of the large e-commerce organization. A product-based solution is a type of vulnerability assessment that is performed by using software or hardware tools that are installed on the organization's own network. A product-based solution can scan automatically against continuously updated databases, as the tools can be configured to download and apply the latest security updates and patches. However, a product-based solution may not imitate the outside view of attackers, as the tools may have limited access or visibility to the external network or the internet. A product-based solution may also not perform well-organized inference-based testing, as the tools may rely on predefined rules or signatures to detect and report vulnerabilities, rather than using logical reasoning and deduction. A product-based solution may also not support multiple networks, as the tools may be designed or optimized for a specific type of network, such as wired, wireless, cloud, or hybrid .
References:
* 1: Vulnerability Assessment Services | Rapid7
* 2: Vulnerability Assessment Services | IBM
* 3: Inference-Based Vulnerability Testing of Firewall Policies - IEEE Conference Publication
* 4: A Tree-Based Approach for Vulnerability Assessment - IEEE Conference Publication
* : Vulnerability Assessment Tools | OWASP Foundation

* : Vulnerability Assessment Solutions: Why You Need One and How to Choose | Defensible

問題 #50
An AWS security operations team receives an alert regarding abnormal outbound traffic from an EC2 instance. The instance begins transmitting encrypted data packets to an external domain that resolves to a Dropbox account not associated with the organization. Further analysis reveals that a malicious executable silently modified the Dropbox sync configuration to use the attacker's access token, allowing automatic synchronization of internal files to the attacker's cloud storage. What type of attack has likely occurred?

- A. Side-channel attack exploiting CPU cache
- B. Man-in-the-Cloud (MITC) attack
- C. Cryptojacking using Coin Hive scripts
- D. Cloud Snooper attack leveraging port masquerading

答案：B

解題說明：
Man-in-the-Cloud (MITC) attacks target cloud synchronization services such as Dropbox, Google Drive, and OneDrive by manipulating authentication tokens instead of user passwords. CEH courseware explains that cloud storage clients rely heavily on sync tokens stored locally, which authorize access without user interaction. If an attacker replaces or injects a malicious token, they can hijack the victim's cloud account or redirect synced data to attacker-controlled locations. In this scenario, the EC2 instance continues to operate normally, but its Dropbox client silently synchronizes data to an external account using the attacker's token. This bypasses traditional defenses such as perimeter firewalls, credential monitoring, or user behavior analytics, because the synchronization process appears legitimate and authenticated. MITC attacks are uniquely stealthy, as they require no further compromise once the sync token is stolen or replaced. Other choices, such as Cloud Snooper or cryptojacking, do not match the described behavior. Therefore, this attack clearly aligns with a Man-in-the-Cloud attack.

問題 #51
Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate data. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?

- A. Port 23
- B. Port 53
- C. Port 50
- D. Port 80

答案：B

解題說明：
DNS uses Ports 53 which is almost always open on systems, firewalls, and clients to transmit DNS queries.
instead of the more familiar Transmission Control Protocol (TCP) these queries use User Datagram Protocol (UDP) due to its low-latency, bandwidth and resource usage compared TCP-equivalent queries. UDP has no error or flow-control capabilities, nor does it have any integrity checking to make sure the info arrived intact.
How is internet use (browsing, apps, chat etc) so reliable then? If the UDP DNS query fails (it's a best-effort protocol after all) within the first instance, most systems will retry variety of times and only after multiple failures, potentially switch to TCP before trying again; TCP is additionally used if the DNS query exceeds the restrictions of the UDP datagram size - typically 512 bytes for DNS but can depend upon system settings.
Figure 1 below illustrates the essential process of how DNS operates: the client sends a question string (for example, mail.google[.]com during this case) with a particular type - typically A for a number address. I've skipped the part whereby intermediate DNS systems may need to establish where '.com' exists, before checking out where 'google[.]com' are often found, and so on.

Many worms and scanners are created to seek out and exploit systems running telnet. Given these facts, it's really no surprise that telnet is usually seen on the highest Ten Target Ports list. Several of the vulnerabilities of telnet are fixed. They require only an

upgrade to the foremost current version of the telnet Daemon or OS upgrade. As is usually the case, this upgrade has not been performed on variety of devices. this might flow from to the very fact that a lot of systems administrators and users don't fully understand the risks involved using telnet. Unfortunately, the sole solution for a few of telnets vulnerabilities is to completely discontinue its use. the well-liked method of mitigating all of telnets vulnerabilities is replacing it with alternate protocols like ssh. Ssh is capable of providing many of an equivalent functions as telnet and a number of other additional services typical handled by other protocols like FTP and Xwindows. Ssh does still have several drawbacks to beat before it can completely replace telnet. it's typically only supported on newer equipment. It requires processor and memory resources to perform the info encryption and decryption. It also requires greater bandwidth than telnet thanks to the encryption of the info . This paper was written to assist clarify how dangerous the utilization of telnet are often and to supply solutions to alleviate the main known threats so as to enhance the general security of the web Once a reputation is resolved to an IP caching also helps: the resolved name-to-IP is usually cached on the local system (and possibly on intermediate DNS servers) for a period of your time . Subsequent queries for an equivalent name from an equivalent client then don't leave the local system until said cache expires. Of course, once the IP address of the remote service is understood , applications can use that information to enable other TCP-based protocols, like HTTP, to try to to their actual work, for instance ensuring internet cat GIFs are often reliably shared together with your colleagues.So, beat all, a couple of dozen extra UDP DNS queries from an organization's network would be fairly inconspicuous and will leave a malicious payload to beacon bent an adversary; commands could even be received to the requesting application for processing with little difficulty.

問題 #52
Mary found a high vulnerability during a vulnerability scan and notified her server team. After analysis, they sent her proof that a fix to that issue had already been applied. The vulnerability that Marry found is called what?

- A. Backdoor
- B. False-positive
- C. False-negative
- D. Brute force attack

答案： B

解題說明：
https://www.infocyte.com/blog/2019/02/16/cybersecurity-101-what-you-need-to-know-about-false-positives- and-false-negatives/
False positives are mislabeled security alerts, indicating there is a threat when in actuality, there isn't. These false/non-malicious alerts (SIEM events) increase noise for already over-worked security teams and can include software bugs, poorly written software, or unrecognized network traffic.
False negatives are uncaught cyber threats - overlooked by security tooling because they're dormant, highly sophisticated (i.e. file-less or capable of lateral movement) or the security infrastructure in place lacks the technological ability to detect these attacks.

問題 #53
.....

最好的312-50v13熱門考題，提前為Certified Ethical Hacker Exam (CEHv13) 312-50v13考試做好準備

如果您購買我們的312-50v13學習資料後，發現我們的產品存在嚴重質量問題或者對您的學習沒起到幫助作用，我們將退還您購買學習資料費用，絕對保證您的利益不受到任何的損失，專業IT認證題庫供應商_提供Cisco,Microsoft,IBM,Oracle等國際IT認證題庫_VCESoft。

將 ECCouncil Certified Ethical Hacker Exam (CEHv13) - 312-50v13 題庫產品加入購物車吧！

- 最新的312-50v13認證考古題 □ 到⇒ tw.fast2test.com ⇐搜尋□ 312-50v13 □以獲取免費下載考試資料312-50v13熱門題庫
- 312-50v13熱門考題和資格考試中的領先提供商和312-50v13證照資訊 □ 立即到➡ www.newdumpspdf.com □□□上搜索➠ 312-50v13 □以獲取免費下載312-50v13認證指南
- 312-50v13考題免費下載 □ 312-50v13考題套裝 □ 312-50v13真題 □ 免費下載➠ 312-50v13 □只需進入⇛ tw.fast2test.com ⇐網站312-50v13新版題庫上線
- 最新312-50v13考證 □ 312-50v13套裝 □ 312-50v13考試證照 □ 到{ www.newdumpspdf.com }搜尋▶ 312-50v13 ◀以獲取免費下載考試資料312-50v13考題免費下載
- 312-50v13新版題庫上線 □ 312-50v13認證指南 □ 312-50v13真題 □ 在{ www.vcesoft.com }搜索最新的{ 312-50v13 }題庫312-50v13題庫分享
- 高通過率的312-50v13熱門考題，高質量的考試指南幫助妳快速通過312-50v13考試 □ 立即在「 www.newdumpspdf.com 」上搜尋⇛ 312-50v13 ⇚並免費下載312-50v13題庫更新資訊
- 最新的312-50v13熱門考題和資格考試中的領先提供商和最近更新的312-50v13證照資訊 □ 在「 www.vcesoft.com 」上搜索➠ 312-50v13 □並獲取免費下載312-50v13最新考題
- 熱門的312-50v13熱門考題，全面覆蓋312-50v13考試知識點 □ 透過➤ www.newdumpspdf.com □搜索➥ 312-50v13 □免費下載考試資料312-50v13考題免費下載
- 312-50v13測試題庫 □ 312-50v13認證指南 □ 312-50v13題庫更新資訊 □ 複製網址▶ tw.fast2test.com ◀打開並搜索（ 312-50v13 ）免費下載312-50v13熱門題庫
- 精心準備的ECCouncil 312-50v13熱門考題是行業領先材料＆準確的312-50v13：Certified Ethical Hacker Exam (CEHv13) □ 立即到《 www.newdumpspdf.com 》上搜索➡ 312-50v13 □□□以獲取免費下載312-50v13熱門題庫
- 312-50v13題庫更新資訊 □ 312-50v13新版題庫上線 □ 312-50v13考題免費下載♪「 www.pdfexamdumps.com 」網站搜索➡ 312-50v13 □□□並免費下載312-50v13套裝
- myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, telegra.ph, thescholarsakademy.com, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

從Google Drive中免費下載最新的VCESoft 312-50v13 PDF版考試題庫：https://drive.google.com/open?id=1pOUBBoYNIf-_pFDpGn0owey2pEFD89f8