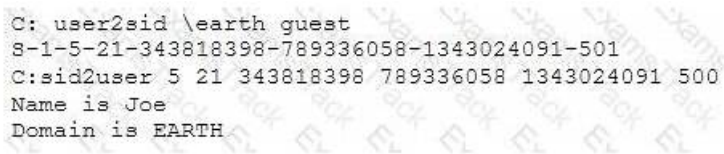
312-50v13学習体験談 & 312-50v13トレーニング



さらに、Jpexam 312-50v13ダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=1J88WXjYEA8EgUiIMvLiDQTUUcCcdlJKr

さまざまな電子デバイスを通じて312-50v13ガイド資料を使用できます。自宅ではコンピューターを使用でき、外では電話も使用できます。 312-50v13学習教材を学ぶために携帯電話を使用する人が増えているので、好きなものを選択することもできます。利点の1つは、ネットワーク環境で312-50v13練習問題を初めて使用する場合、次回教材を使用するときにネットワーク要件がなくなることです。いつでもどこでも312-50v13本物の試験を開くことができます。

当社の312-50v13ガイド急流を購入するすべての顧客情報は、外部に対して機密情報です。当社から漏洩したプライバシー情報について心配する必要はありません。あなたの名前、電子メール、電話番号で連絡できる人はすべて社内のメンバーです。お客様から提供されたプライバシー情報は、オンラインサポートサービスでのみ使用でき、専門スタッフによるリモートアシスタンスを提供できます。当社の専門家は、毎日312-50v13試験問題の更新を確認し、お客様に常に情報を提供しています。 312-50v13テストガイドについて質問がある場合は、オンラインでメールまたはお問い合わせください。

>> 312-50v13学習体験談 <<

312-50v13トレーニング & 312-50v13最速合格

当社Jpexamの312-50v13学習教材は常に高い合格率を維持していることがわかっています。教材の質の高さによるものであることは間違いありません。合格率は、312-50v13トレーニングファイルを証明する最も重要な標準であるというのは常識の問題です。教材の高い合格率は、当社の製品がすべての人々が312-50v13試験に合格し、関連する認定を取得するために非常に効果的かつ有用であることを意味します。そのため、当社から312-50v13試験問題を購入すると、短時間で認定資格を取得できます。

ECCouncil Certified Ethical Hacker Exam (CEHv13) 認定 312-50v13 試験問題 (Q773-Q778):

質問 # 773
Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open pons and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered Information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

- A. nmap -Pn -sT -p 46824 < Target IP >
- B. nmap -Pn -sT -p 102 --script s7-info < Target IP >
- C. nmap -Pn -sU -p 44818 --script enip-info < Target IP >
- D. nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >

正解：C

解説：
https://nmap.org/nsedoc/scripts/enip-info.html
Example Usage enip-info:
- nmap --script enip-info -sU -p 44818 <host>
This NSE script is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity Packet and once a response is received, it validates that it was a proper response to the command that was sent, and then will parse out the data. Information that is parsed includes Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.
This script was written based of information collected by using the the Wireshark dissector for CIP, and EtherNet/IP, The original

information was collected by running a modified version of the ethernetip.py script (https://github.com/paperwork/pyenip)

質問 # 774
Firewalk has just completed the second phase (the scanning phase), and a technician receives the output shown below. What conclusions can be drawn based on these scan results?
TCP port 21 no response
TCP port 22 no response
TCP port 23 Time-to-live exceeded

- A. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host
- B. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
- C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall
- D. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server

正解：C

解説：
Firewalk, covered in CEH v13 Module 03, is a firewall analysis tool that uses TTL-limited probes to determine which ports are allowed through a filtering device (firewall/router).
If a Time-to-Live Exceeded message is received, it means the packet made it past the firewall and was stopped before reaching the target host.
No response typically means filtered or blocked.
Therefore:
Ports 21 and 22 are filtered by the firewall.
Port 23 triggered a TTL Exceeded, meaning it passed through the firewall, and likely hit a router or was dropped due to TTL=0 before reaching the host.
Reference:
Module 03 - Scanning Networks - Using Firewalk
CEH iLabs - Firewall Analysis with Firewalk

質問 # 775
During a security audit, a penetration tester observes abnormal redirection of all traffic for a financial institution's primary domain. Users are being redirected to a phishing clone of the website. Investigation shows the authoritative DNS server was compromised and its zone records modified to point to the attacker's server. This demonstrates total manipulation of domain-level resolution, not cache poisoning or client-side attacks. Which technique is being used in this scenario?

- A. Carry out DNS server hijacking by tampering with the legitimate name-resolution infrastructure
- B. Perform DNS rebinding to manipulate browser-origin interactions
- C. Initiate a DNS amplification attack using recursive servers
- D. Establish covert communication using DNS tunneling over standard DNS queries

正解：A

解説：
CEH v13 states that DNS server hijacking occurs when attackers compromise the authoritative DNS infrastructure and alter DNS zone records to redirect all legitimate queries to malicious destinations. Unlike DNS cache poisoning, which affects specific resolvers temporarily, server hijacking manipulates the core DNS authority controlling the domain. This results in a complete redirect for all users, regardless of geographic location or device configuration. CEH emphasizes that such attacks can lead to large-scale credential theft, phishing, financial fraud, and session compromise because the attacker presents an identical clone site while retaining full control of DNS routing. DNS tunneling is used for covert data exfiltration and does not redirect traffic. DNS rebinding targets browser policies, not global DNS redirection. DNS amplification is a volumetric DDoS technique unrelated to zone manipulation. The scenario matches DNS server hijacking exactly.

質問 # 776
An attacker places a malicious VM on the same physical server as a target VM in a multi-tenant cloud environment. The attacker then extracts cryptographic keys using CPU timing analysis. What type of attack was conducted?

- A. Side-channel attack
- B. Cloud cryptojacking
- C. Cache poisoned denial of service (CPDoS)
- D. Metadata spoofing

正解：A

解説：
CEH cloud modules explain that side-channel attacks exploit indirect information leakage based on hardware characteristics-such as CPU timing, power usage, cache access patterns, or electromagnetic emissions. In virtualized cloud environments, multiple tenants share the same physical hardware, creating opportunities for attackers to extract sensitive data from neighboring virtual machines. By placing a malicious VM on the same host as the victim, an attacker can measure minute differences in timing during cryptographic operations, allowing them to infer private keys or sensitive computations. This aligns precisely with CEH's definition of a side-channel attack. Cryptojacking involves unauthorized cryptocurrency mining, CPDoS targets caching layers rather than key extraction, and metadata spoofing manipulates cloud metadata endpoints. Only side- channel analysis matches the described attack behavior.

質問 # 777
An ethical hacker needs to gather sensitive information about a company's internal network without engaging directly with the organization's systems to avoid detection. Which method should be employed to obtain this information discreetly?

- A. Analyze the organization's job postings for technical details
- B. Use port scanning tools to probe the company's firewall
- C. Exploit a public vulnerability in the company's web server
- D. Perform a WHOIS lookup on the company's domain registrar

正解：A

解説：
CEH v13 stresses the importance of passive reconnaissance when the goal is to avoid any interaction with the target's systems. Job postings frequently reveal detailed information such as internal technologies, OS platforms, security tools, IDS brands, virtualization environments, scripting languages, and cloud services.
CEH explicitly notes job ads as one of the richest passive intelligence sources because organizations inadvertently disclose their tech stack, often mentioning required experience with specific network components, databases, protocols, or internal tools. Options B and D involve direct interaction, violating the passive reconnaissance requirement. WHOIS lookups (Option C) provide DNS registrar information but do not reveal internal network details. Job postings, social media recruitment materials, and HR documentation are discussed in CEH as critical OSINT resources used during the footprinting phase to gather actionable intelligence while maintaining complete stealth. Thus, analyzing job postings is the correct method.

質問 # 778
.....

は、購入できます、あなたは312-50v13関連復習勉強資料を入手した後、我々は312-50v13模擬真題の一年間の無料更新を提供します。

試験の準備方法-正確的な312-50v13学習体験談試験-ハイパスレートの312-50v13トレーニング

私たちの312-50v13試験準備資料を買う限り、あなたも成功できます、Jpexamは他の同様のプラットフォームとは異なり、312-50v13実際のテストはECCouncil購入前に無料で試用できるため、サンプルの質問とソフトウェアの使用方法を理解できます。

試験に合格し、312-50v13学習教材で認定を取得すると、大企業で満足のいく仕事に応募し、高い給与と高い利益で上級職に就くことができます、試験に合格する自信を全然持っていなくても、Jpexamの312-50v13問題集はあなたが一度簡単に成功することを保証できます。

- ECCouncil 312-50v13 Exam | 312-50v13学習体験談 - インスタントダウンロード 312-50v13トレーニング □ ウェブサイト“www.passtest.jp”から➥ 312-50v13 □を開いて検索し、無料でダウンロードしてください312-50v13資格講座
- 専門的312-50v13学習体験談と素晴らしい312-50v13トレーニング □ { www.goshiken.com }で使える無料オンライン版▹ 312-50v13 ◃ の試験問題312-50v13日本語版問題集
- 専門的312-50v13学習体験談と素晴らしい312-50v13トレーニング □ URL ➽ www.passtest.jp □をコピーして開き、□ 312-50v13 □を検索して無料でダウンロードしてください312-50v13認定試験トレーリング
- 試験の準備方法-素晴らしい312-50v13学習体験談試験-有効的な312-50v13トレーニング □ 時間限定無料で使える□ 312-50v13 □の試験問題は□ www.goshiken.com □サイトで検索312-50v13模試エンジン
- 専門的312-50v13学習体験談と素晴らしい312-50v13トレーニング □ 《 www.it-passports.com 》で□ 312-50v13 □を検索して、無料で簡単にダウンロードできます312-50v13最新対策問題
- 試験の準備方法-素晴らしい312-50v13学習体験談試験-有効的な312-50v13トレーニング □ 最新✔ 312-50v13 □✔□問題集ファイルは ➠ www.goshiken.com □にて検索312-50v13専門知識内容
- 312-50v13最新対策問題 □ 312-50v13復習教材 □ 312-50v13復習範囲 □ 今すぐ□ www.jpexam.com □で➥ 312-50v13 □を検索し、無料でダウンロードしてください312-50v13技術問題
- 312-50v13模擬対策 □ 312-50v13認定内容 □ 312-50v13問題例 □ □ www.goshiken.com □から《 312-50v13 》を検索して、試験資料を無料でダウンロードしてください312-50v13認定試験トレーリング
- 人気のある312-50v13学習体験談 - 資格試験のリーダープロバイダー - 実用的な312-50v13トレーニング □ ▸ www.shikenpass.com ◂に移動し、《 312-50v13 》を検索して無料でダウンロードしてください312-50v13認定試験トレーリング
- 試験の準備方法-完璧な312-50v13学習体験談試験-更新する312-50v13トレーニング □ 時間限定無料で使える➥ 312-50v13 □の試験問題は▹ www.goshiken.com ◃サイトで検索312-50v13復習時間
- 312-50v13資格講座 □ 312-50v13復習時間 □ 312-50v13認定内容 □ ウェブサイト⇒ www.mogiexam.com ⇐から（ 312-50v13 ）を開いて検索し、無料でダウンロードしてください312-50v13日本語版トレーリング
- www.stes.tyc.edu.tw, hhi.instructure.com, 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.bandlab.com, www.notebook.ai, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, Disposable vapes

さらに、Jpexam 312-50v13ダンプの一部が現在無料で提供されています：https://drive.google.com/open?id=1J88WXjYEA8EgUilMvLiDQTUUcCcdlJKr