312-50v13 Reliable Test Forum, 312-50v13 Valid Exam Testking

What's more, part of that Exam4Docs 312-50v13 dumps now are free: https://drive.google.com/open?id=1oyTgrwU6kv_37LTkIHOp1RBMWjCkG8p0

You just need to get Exam4Docs's ECCouncil Certification 312-50v13 Exam exercises and answers to do simulation test, you can pass the ECCouncil certification 312-50v13 exam successfully. If you have a ECCouncil 312-50v13 the authentication certificate, your professional level will be higher than many people, and you can get a good opportunity of promoting job. Add Exam4Docs's products to cart right now! Exam4Docs can provide you with 24 hours online customer service.

ECCouncil 312-50v13 Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Cryptography and Post-Exploitation	13%	- Cryptography Concepts • 1. Cryptography Tools • 2. Encryption Fundamentals • 3. Public Key Infrastructure (PKI) • 4. Cryptography Countermeasures • 5. Hashing and Digital Signatures • 6. Code Signing and Email Encryption • 7. Disk Encryption and Cryptanalysis • 8. Encryption Algorithms (Symmetric and Asymmetric) - Post-Exploitation Techniques • 1. Advanced Persistent Threat (APT) • 2. Reporting and Documentation • 3. Post-Exploitation Concepts • 4. Lateral Movement and Tunneling • 5. Covering Tracks and Maintaining Access

Topic 2: Information Security and Ethical Hacking Overview	6%	- Ethical Hacking Overview • 1. Need for Ethical Hackers • 2. Security Testing Methodologies • 3. Skills and Mindset of an Ethical Hacker • 4. What is Ethical Hacking? • 5. Governance and Compliance - Information Security Overview • 1. Information Security Threats and Attack Vectors • 2. Understanding Information Security Controls • 3. Understanding Information Security • 4. Understanding Information Security Laws and Standards • 5. Proactive Cyber Defense
Topic 3: Vulnerability Analysis	7%	- Vulnerability Assessment Concepts • 1. Vulnerability Assessment Solutions • 2. Vulnerability Scoring Systems • 3. Vulnerability Assessment Tools and Software
Topic 4: System Hacking	17%	- System Hacking Tools and Countermeasures • 1. Password Recovery Tools • 2. Covering Tracks Countermeasures • 3. Steganography • 4. Rootkits • 5. Keyloggers and Spyware • 6. Ports and Log Files - System Hacking Methodologies • 1. Cracking Passwords • 2. Gaining Access • 3. Executing Applications • 4. Hiding Files • 5. Covering Tracks • 6. Escalating Privileges
Topic 5: Web Application Attacks	19%	- Web Application Concepts and Attacks • 1. Web Application Scanning and Testing Tools • 2. Authentication and Session Management Attacks • 3. OWASP Top 10 Vulnerabilities • 4. Injection Attacks • 5. Web Application Password Cracking and Clickjacking • 6. Web Application Architecture • 7. Web Application Countermeasures • 8. Cross-Site Scripting (XSS) and Request Forgery - Hacking Web Servers and Web Applications • 1. Web Server and Web Application Countermeasures • 2. Web Server Attack Methodology • 3. Web Server Attacks

Topic 6: Mobile Platform and IoT Attacks	7%	- Mobile Platform Attack Vectors • 1. Mobile Device Management (MDM) • 2. Mobile Malware and Mobile Spyware • 3. Mobile Security Tools and Countermeasures • 4. Mobile Attack Surfaces and Vulnerabilities • 5. Mobile Attack Techniques • 6. Mobile Platform Overview - IoT and OT Attacks • 1. IoT Hacking Methodology • 2. IoT Vulnerabilities and Threats • 3. IoT Concepts and Architecture • 4. OT Concepts and Attacks • 5. IoT Attack Tools and Countermeasures
Topic 7: Reconnaissance Techniques	21%	- Footprinting and Reconnaissance • 1. Footprinting through Search Engines • 2. Footprinting Countermeasures • 3. Footprinting Tools • 4. Website Footprinting • 5. Email Footprinting • 6. Competitive Intelligence Gathering • 7. AWS Cloud Footprinting • 8. DNS Footprinting • 9. Network Footprinting • 10. Footprinting through Social Networking Sites • 11. Footprinting through Web Services - Scanning Networks • 1. Port Scanning Techniques • 2. Drawing Network Diagrams • 3. Detecting Live Systems • 4. Banner Grabbing • 5. Proxy Servers and Anonymizers • 6. Scanning Tools • 7. Scan for Vulnerabilities • 8. Scanning Countermeasures • 9. Masscan • 10. Nmap and Zenmap • 11. Hping2 and Hping3 • 12. NIDS, NIPS, and Firewall Evasion Techniques • 13. Network Scanning Concepts

Topic 8: Sniffing and Evasion	10%	- Network Evasion • 1. Denial of Service Attacks • 2. Firewalls and Intrusion Detection/Prevention Systems • 3. Evasion Techniques • 4. IDS/Firewall Evasion Tools - Social Engineering • 1. Insider Threats and Identity Theft • 2. Social Engineering Tools and Countermeasures • 3. Social Engineering Concepts • 4. Social Engineering Techniques - Network Sniffing • 1. Sniffing Concepts • 2. MAC Flooding and Switch Port Stealing • 3. STP Attacks and DNS Poisoning • 4. Sniffing Tools • 5. ARP Spoofing • 6. VLAN Hopping and DHCP Starvation • 7. Sniffing Detection and Countermeasures
Topic 9: Wireless Network Attacks	9%	- Wireless Hacking Methodology • 1. Wireless Network Countermeasures • 2. Wireless Network Hacking Tools • 3. Wireless Sniffing and Wardriving • 4. Cracking WPA/WPA2 and WEP Encryption • 5. Bluetooth and RFID Attacks - Wireless Network Concepts • 1. Wireless Network Topology and Threats • 2. Wireless Terminology and Standards • 3. Wireless Encryption and Security
Topic 10: Cloud and Container Attacks	10%	- Cloud Attacks and Security • 1. Container Security Tools and Countermeasures • 2. Cloud Security Tools and Best Practices • 3. Cloud Penetration Testing • 4. Cloud Security Threats and Attacks - Cloud Computing Concepts • 1. Cloud Architecture and Deployment Models • 2. Cloud Service Models (IaaS, PaaS, SaaS) • 3. Serverless Architecture • 4. Container Technology

Topic 11: Malware Threats	8%	- Malware Analysis and Distribution • 1. Malware Analysis Techniques • 2. Malware Detection Methods • 3. Malware Countermeasures - Malware and Its Types • 1. APT and Futuristic Malware • 2. Types of Malware • 3. APT Concepts • 4. Malware Fundamentals
Topic 12: Enumeration	15%	- Enumeration Process • 1. NTP Enumeration • 2. VoIP Enumeration • 3. RPC and NFS Enumeration • 4. LDAP Enumeration • 5. Mail Server Enumeration • 6. NetBIOS Enumeration • 7. SNMP Enumeration • 8. SMB and SAMBA Enumeration • 9. Enumeration Countermeasures - Enumeration Concepts • 1. Enumeration Techniques • 2. Enumeration Fundamentals

100% Free 312-50v13 – 100% Free Reliable Test Forum | Certified Ethical Hacker Exam (CEHv13) Valid Exam Testking

Desktop ECCouncil 312-50v13 Practice Exam Software is a one-of-a-kind and very effective software developed to assist applicants in preparing for the ECCouncil 312-50v13 certification test. The Desktop ECCouncil 312-50v13 Practice Exam Software that we provide includes a self-assessment feature that enables you to test your knowledge by taking simulated tests and evaluating the results.

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q544-Q549):

NEW QUESTION # 544
Which information CANNOT be directly obtained from DNS interrogation?

- A. Server geolocation (via IPs)
- B. IP addresses of mail servers
- C. Usernames and passwords
- D. Subdomains of the organization

Answer: C

Explanation:
DNS interrogation is a core passive and semi-active reconnaissance technique described in CEH v13 Reconnaissance Techniques. It allows ethical hackers to gather publicly available information about a target' s domain infrastructure.
Through DNS queries, testers can retrieve:
* Subdomains (via zone transfers, brute force, or DNS records)
* Mail server IP addresses (via MX records)

* Server IP addresses, which can then be mapped to approximate geographic locations However, DNS does not store authentication credentials such as usernames and passwords. That information resides in authentication systems like Active Directory, LDAP, or application databases, not DNS.
Therefore, Option A is the only choice that cannot be obtained via DNS interrogation. CEH v13 clearly distinguishes between naming infrastructure data and credential-based information, reinforcing why DNS enumeration cannot reveal user credentials.
Thus, Option A is correct.

NEW QUESTION # 545
User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

- A. Session
- B. Presentation
- C. Application
- D. Transport

Answer: B

Explanation:
https://en.wikipedia.org/wiki/Presentation_layer
In the seven-layer OSI model of computer networking, the presentation layer is layer 6 and serves as the data translator for the network. It is sometimes called the syntax layer. The presentation layer is responsible for the formatting and delivery of information to the application layer for further processing or display.
Encryption is typically done at this level too, although it can be done on the application, session, transport, or network layers, each having its own advantages and disadvantages. Decryption is also handled at the presentation layer. For example, when logging on to bank account sites the presentation layer will decrypt the data as it is received.

NEW QUESTION # 546
You perform a network scan using ICMP Echo Requests and observe that certain IP addresses do not return Echo Replies, while other network services remain functional. How should this situation be interpreted?

- A. The lack of replies indicates a major breach
- B. The scanned IPs are unused and available for expansion
- C. A firewall or security control is blocking ICMP Echo Requests
- D. The non-responsive IPs indicate severe congestion

Answer: C

Explanation:
According to CEH v13 Network Scanning and Enumeration, ICMP Echo Requests (ping) are commonly filtered by firewalls and intrusion prevention systems to reduce network reconnaissance exposure. When ICMP Echo Replies are not returned but other services remain operational, the most likely explanation is ICMP filtering rather than host unavailability or compromise.
CEH v13 explicitly states that many organizations configure firewalls to block ICMP Echo Requests while allowing other ICMP types or higher-layer protocols. This practice helps prevent attackers from easily mapping live hosts during the reconnaissance phase.
The other options are incorrect because:
* Unused IPs would not necessarily have active services.
* A breach would typically present additional symptoms.
* Network congestion would affect multiple protocols, not just ICMP.
Thus, blocked ICMP is the correct interpretation.

NEW QUESTION # 547
OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?

- A. openssl s_client -site www.website.com:443

- B. openssl_client -connect www.website.com:443
- C. openssl_client -site www.website.com:443
- D. openssl s_client -connect www.website.com:443

Answer: D

NEW QUESTION # 548
Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

- A. 44EFCE164AB921CQAAD3B435B51404EE
- B. 0182BD0BD4444BF836077A718CCDF409
- C. CEC52EB9C8E3455DC2265B23734E0DAC
- D. BA810DBA98995F1817306D272A9441BB
- E. B757BF5C0D87772FAAD3B435B51404EE
- F. E52CAC67419A9A224A3B108F3FA6CB6D

Answer: A,E

Explanation:
LM hashes are split into two 16-character halves (each representing 7-character blocks). If the original password is less than 8 characters, the second half of the LM hash will always be a constant:
"AAD3B435B51404EE"
This known value is used to pad the second half of the password, and it signals that the original password was
7 characters or fewer.
In the options:
B). 44EFCE164AB921CQAAD3B435B51404EE # ends with AAD3B435B51404EE # < 8 chars E).
B757BF5C0D87772FAAD3B435B51404EE # also ends with AAD3B435B51404EE # < 8 chars From CEH v13 Official Courseware:
Module 6: Malware Threats # LM Hash Weaknesses
Reference:CEH v13 Study Guide - Module 6: Password Cracking # LM Hash Structure and Indicators
═══

NEW QUESTION # 549
.....

Our 312-50v13 exam prep is subservient to your development. And our experts generalize the knowledge of the 312-50v13 exam into our products showing in three versions. PDF version of 312-50v13 learning quiz can support customers' printing request and Software version can support simulation test system. App/online version of 312-50v13 Training Materials can be suitable to all kinds of equipment or digital devices. You can choose your most desirable way to practice on the daily basis.

➠ www.pdfvce.com □ open and search for ➤ 312-50v13 □ to download for free □Reliable 312-50v13 Practice Materials

- Free PDF Quiz ECCouncil - Updated 312-50v13 Reliable Test Forum □ Easily obtain （ 312-50v13 ） for free download through ➥ www.verifieddumps.com □ □312-50v13 Practice Test Engine
- Pass Guaranteed 2026 312-50v13: Certified Ethical Hacker Exam (CEHv13) –Authoritative Reliable Test Forum □ Search for ➥ 312-50v13 □ on 【 www.pdfvce.com 】 immediately to obtain a free download □Reliable 312-50v13 Braindumps Book
- www.easy4engine.com: Your Solution to Ace the ECCouncil 312-50v13 Exam □ Easily obtain free download of " 312-50v13 " by searching on 「 www.easy4engine.com 」 □312-50v13 Certification Dumps
- 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, freestyler.ws, 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, scalar.usc.edu, scalar.usc.edu, 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, fortunetelleroracle.com, www.stes.tyc.edu.tw, fortunetelleroracle.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, myportal.utt.edu.tt, Disposable vapes

P.S. Free 2026 ECCouncil 312-50v13 dumps are available on Google Drive shared by Exam4Docs: https://drive.google.com/open?id=1oyTgrwU6kv_37LTkIHOp1RBMWjCkG8p0