

Pass Leader 312-50v13 Dumps & 312-50v13 Test Sample Online

312-50v13 Dumps Questions

9. Attacker Rony Installed a rogue access point within an organization's perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack.

What is the type of vulnerability assessment performed by Johnson in the above scenario?

- A. Distributed assessment
- B. Wireless network assessment
- C. Host-based assessment
- D. Application assessment

Answer: B

P.S. Free 2026 ECCouncil 312-50v13 dumps are available on Google Drive shared by VCEdumps:
<https://drive.google.com/open?id=1KktMC9cyLbbZL6Xna-VeCTXaFBiEWk81>

For candidates who are preparing for the 312-50v13 exam, passing the 312-50v13 exam is a long-cherished wish. So if you want to pass the 312-50v13 exam, you should choose the product of our company. Since our company is a leading team of the business, we have lots of experienced experts to compile the practice materials of the 312-50v13 exam, and the practice materials also provide the detailed answers. And the pass rate of the 312-50v13 Exam is 98%. If you failure to pass the 312-50v13 exam after purchasing the product, money back is guaranteed. What's more, our product is quite cheaper compared with other product, you just need to spent some money to buy and practiceit, then a certificate of the 312-50v13 will be gotten, which can add your competitive ability in the job market.

All these three ECCouncil 312-50v13 exam questions formats are easy to use and compatible with all devices, operating systems, and browsers. You can install and run these three 312-50v13 exam practice test questions easily and start ECCouncil 312-50v13 Exam Preparation without wasting further time. The 312-50v13 exam practice questions will ace your Certified Ethical Hacker Exam (CEHv13) 312-50v13 exam preparation and prepare you for the final 312-50v13 exam.

>> Pass Leader 312-50v13 Dumps <<

312-50v13 Test Sample Online | Valid 312-50v13 Exam Discount

In the world of industry, 312-50v13 certification is the key to a successful career. If you have achieved credential such as 312-50v13 then it means a bright future is waiting for you. Avail the opportunity of 312-50v13 dump at VCEdumps.com that helps you in achieving good scores in the exam. Due to these innovative methodologies students get help online. The 312-50v13 Exam Questions Answers PDF is very effective and greatly helpful in increasing the skills of students. They can easily cover the exam topics with more practice due to the unique set of 312-50v13 exam dump. The 312-50v13 certification learning is getting popular with the passage of time.

ECCouncil Certified Ethical Hacker Exam (CEHv13) Sample Questions (Q40-Q45):

NEW QUESTION # 40

Which system consists of a publicly available set of databases that contain domain name registration contact information?

- A. CAPTCHA
- B. IANA
- C. IETF
- D. WHOIS

Answer: D

NEW QUESTION # 41

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

- A. 0
- B. 1
- C. 2
- D. 3
- E. 4
- F. 5

Answer: A,C,F

Explanation:

To block NetBIOS and related Windows networking traffic from traversing a firewall (especially from external sources), you should block the following ports:

- * Port 135 (TCP/UDP): Microsoft RPC endpoint mapper (DCOM/RPC)
- * Port 139 (TCP): NetBIOS Session Service
- * Port 445 (TCP): Direct-hosted SMB over TCP/IP (Windows 2000+)

These ports are commonly used for:

- * File sharing
- * RPC-based communication
- * Windows network services

From CEH v13 Official Courseware:

- * Module 3: Scanning Networks
- * Module 4: Enumeration

CEH v13 Study Guide states:

"To prevent external enumeration, remote file sharing, and NetBIOS attacks, administrators should block inbound access to ports 135, 139, and 445 on the firewall." Incorrect Options:

- * A (110): POP3 mail service
- * D (161): SNMP
- * F (1024): High ephemeral port; not specific to NetBIOS

Reference:CEH v13 Study Guide - Module 4: Enumeration # NetBIOS Enumeration PreventionMicrosoft Security Best Practices - Block SMB Ports (135-139, 445)

NEW QUESTION # 42

During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.

What is this type of DNS configuration commonly called?

- A. DNSSEC
- B. DynDNS
- C. Split DNS
- D. DNS Scheme

Answer: C

Explanation:

Split DNS (also known as Split-Horizon DNS) is a configuration where internal users and external users receive different DNS responses. Typically, one DNS server resides in the DMZ for public access, and another is inside the network for internal name resolution.

Reference - CEH v13 Official Study Guide, Module 9: System Hacking / Perimeter Security

"Split DNS allows different DNS records to be presented based on whether the requester is from inside or outside the organization's network."

Incorrect options:

- A). DynDNS is a dynamic DNS provider.
- B). DNS Scheme is a non-standard term
- C). DNSSEC is a security extension for DNS, not a deployment model.

NEW QUESTION # 43

What would be the purpose of running "wget 192.168.0.15 -q -S" against a web server?

- A. Performing content enumeration on the web server to discover hidden folders
- B. Flooding the web server with requests to perform a DoS attack
- C. Downloading all the contents of the web page locally for further examination
- **D. Using wget to perform banner grabbing on the web server**

Answer: D

Explanation:

The command in question:

```
wget 192.168.0.15 -q -S
```

* wget is a command-line utility used to retrieve files via HTTP, HTTPS, or FTP.

* -q (quiet mode): Suppresses output, except for errors.

* -S: Displays the server response headers (even in quiet mode).

In this case, wget is being used to connect to the specified web server (192.168.0.15) and retrieve the HTTP response headers - such as the Server field (e.g., Apache, Nginx), HTTP status codes, and other metadata.

This is a classic example of banner grabbing - the process of capturing metadata (often from headers) to identify the software, version, or configuration of a service.

Incorrect Options:

* A. Content enumeration would require directory brute-forcing tools like DirBuster or Gobuster.

* C. DoS attacks require high volumes of traffic or specially crafted packets; wget with a single request does not perform flooding.

* D. Downloading full site contents would involve options like -r (recursive) or --mirror, which are not used in this command.

Reference - CEH v13 Official Courseware:

Module 03: Scanning Networks

Section: "Banner Grabbing"

Tool Reference: wget, netcat, telnet, curl for banner enumeration

NEW QUESTION # 44

A skilled ethical hacker was assigned to perform a thorough OS discovery on a potential target. They decided to adopt an advanced fingerprinting technique and sent a TCP packet to an open TCP port with specific flags enabled. Upon receiving the reply, they noticed the flags were SYN and ECN-Echo. Which test did the ethical hacker conduct and why was this specific approach adopted?

- **A. Qrest 1: The test was conducted because SYN and ECN-Echo flags enabled to allow the hacker to probe the nature of the response and subsequently determine the OS fingerprint**
- B. Test 2: This test was chosen because a TCP packet with no flags enabled is known as a NULL packet and this would allow the hacker to assess the OS of the target
- C. Test 6: The hacker selected this test because a TCP packet with the ACK flag enabled sent to a closed TCP port would yield more information about the OS
- D. Test 3: The test was executed to observe the response of the target system when a packet with URG, PSH, SYN, and FIN flags was sent, thereby identifying the OS

Answer: A

Explanation:

The ethical hacker conducted Test 1, which is a TCP/IP stack fingerprinting technique that uses the SYN and ECN-Echo flags to determine the OS of the target system. The SYN flag is used to initiate a TCP connection, and the ECN-Echo flag is used to indicate that the sender supports Explicit Congestion Notification (ECN), which is a mechanism to reduce network congestion. Different OSes have different implementations and responses to these flags, which can reveal their identity. For example, Windows XP and 2000 will reply with SYN and ECN-Echo flags set, while Linux will reply with only SYN flag set. By sending a TCP packet with these flags enabled to an open TCP port and observing the reply, the ethical hacker can probe the nature of the response and subsequently determine the OS fingerprint.

The ethical hacker adopted this specific approach because it is an advanced and stealthy technique that can evade some firewalls and intrusion detection systems (IDS) that may block or alert other types of packets, such as NULL, FIN, or Xmas packets.

Moreover, this technique can provide more accurate and reliable results than other techniques, such as banner grabbing or passive analysis, that may depend on the availability or validity of the information provided by the target system.

The other options are not correct, as they describe different tests and reasons. Test 3 is a TCP/IP stack fingerprinting technique that

uses the URG, PSH, SYN, and FIN flags to determine the OS of the target system. Test 2 is a TCP/IP stack fingerprinting technique that uses a NULL packet, which is a TCP packet with no flags enabled, to determine the OS of the target system. Test 6 is a TCP/IP stack fingerprinting technique that uses the ACK flag, which is used to acknowledge the receipt of a TCP segment, to determine the OS of the target system. References:

- * OS and Application Fingerprinting | SANS Institute
- * Operating System Fingerprinting | SpringerLink
- * OS and Application Fingerprinting - community.akamai.com
- * What is OS Fingerprinting and Techniques - Zerosuniverse

NEW QUESTION # 45

.....

What 312-50v13 study materials can give you is far more than just a piece of information. First of all, 312-50v13 study materials can save you time and money. As a saying goes, to sensible men, every day is a day of reckoning. Every minute 312-50v13 study material saves for you may make you a huge profit. Secondly, 312-50v13 Study Materials will also help you to master a lot of very useful professional knowledge in the process of helping you pass the exam. The 312-50v13 study materials are valuable, but knowledge is priceless.

312-50v13 Test Sample Online: <https://www.vcedumps.com/312-50v13-examcollection.html>

ECCouncil Pass Leader 312-50v13 Dumps As we all know that these real tests are hard to pass many examinees may fail one or more times before clearing one exam, All these three ECCouncil 312-50v13 exam questions features are designed to help you in ECCouncil 312-50v13 exam preparation and enable you to pass the final ECCouncil 312-50v13 certification exam easily, ECCouncil Pass Leader 312-50v13 Dumps They are professional practice material under warranty.

A set of large and small logo images to be displayed on the 312-50v13 Start Screen, After the system verifies the information, the account appears in the Accounts list and you're done.

As we all know that these real tests are hard to pass many examinees may fail one or more times before clearing one exam, All these three ECCouncil 312-50v13 Exam Questions features are designed to help you in ECCouncil 312-50v13 exam preparation and enable you to pass the final ECCouncil 312-50v13 certification exam easily.

Pass Leader 312-50v13 Dumps offer you accurate Test Sample Online to pass Certified Ethical Hacker Exam (CEHv13) exam

They are professional practice material under warranty, For the convenience of users, our 312-50v13 learn materials will be timely updated information associated with the qualification of the home page.

With customizable exams and a real exam environment, our Valid 312-50v13 Exam Discount practice tests are the perfect way to prepare for the test pressure you will face during the final exam.

- 312-50v13 Valid Vce Dumps Valid 312-50v13 Exam Duration 312-50v13 Latest Exam Duration Download 312-50v13 for free by simply searching on www.prep4away.com 312-50v13 Reliable Test Syllabus
- 2026 ECCouncil 312-50v13: Certified Ethical Hacker Exam (CEHv13) Latest Pass Leader Dumps Copy URL www.pdfvce.com open and search for **【 312-50v13 】** to download for free 312-50v13 Latest Exam Pass4sure
- 100% Pass Rate with ECCouncil 312-50v13 PDF Dumps Simply search for \Rightarrow 312-50v13 \Leftarrow for free download on www.practicevce.com Exam Dumps 312-50v13 Free
- 2026 ECCouncil 312-50v13: Certified Ethical Hacker Exam (CEHv13) Latest Pass Leader Dumps Open website www.pdfvce.com and search for **《 312-50v13 》** for free download Best 312-50v13 Practice
- Pass Leader 312-50v13 Dumps | Useful Certified Ethical Hacker Exam (CEHv13) 100% Free Test Sample Online The page for free download of \Rightarrow 312-50v13 on www.pass4test.com will open immediately 312-50v13 Valid Exam Discount
- 312-50v13 Latest Exam Pass4sure 312-50v13 Valid Exam Discount New Braindumps 312-50v13 Book Search for 312-50v13 and download it for free on “ www.pdfvce.com ” website Exam Dumps 312-50v13 Pdf
- 312-50v13 Exams New Braindumps 312-50v13 Book 312-50v13 Reliable Test Sample Easily obtain 312-50v13 for free download through \Rightarrow www.prep4sures.top 312-50v13 Reliable Test Sample
- 100% Pass Rate with ECCouncil 312-50v13 PDF Dumps Search for [312-50v13] and download exam materials for free through [www.pdfvce.com] \rightarrow 312-50v13 Valid Braindumps
- Take ECCouncil 312-50v13 Web-Based Practice Test on Popular Browsers Open website \Rightarrow www.examcollectionpass.com and search for **【 312-50v13 】** for free download 312-50v13 Mock Test

