



# 312-50V9<sup>Q&As</sup>

Certified Ethical Hacker Exam V9

**Pass EC-COUNCIL 312-50V9 Exam with 100% Guarantee**

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/312-50v9.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by EC-COUNCIL Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers





### QUESTION 1

Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test.

While conducting a port scan she notices open ports in the range of 135 to 139.

What protocol is most likely to be listening on those ports?

- A. Finger
- B. FTP C. Samba
- D. SMB

Correct Answer: D Section: (none)

---

### QUESTION 2

To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

- A. Vulnerability scanner
- B. Protocol analyzer
- C. Port scanner
- D. Intrusion Detection System

Correct Answer: A Section: (none)

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses. They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized access.

References: [https://en.wikipedia.org/wiki/Vulnerability\\_scanner](https://en.wikipedia.org/wiki/Vulnerability_scanner)

---

### QUESTION 3

The security concept of "separation of duties" is most similar to the operation of which type of security device?

- A. Firewall
- B. Bastion host
- C. Intrusion Detection System
- D. Honeypot



Correct Answer: A Section: (none)

In most enterprises the engineer making a firewall change is also the one reviewing the firewall metrics for unauthorized changes. What if the firewall administrator wanted to hide something? How would anyone ever find out? This is where the separation of duties comes in to focus on the responsibilities of tasks within security.

References: <http://searchsecurity.techtarget.com/tip/Modern-security-management-strategy-requiressecurity-separation-of-duties>

---

#### QUESTION 4

In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

- A. Full Blown
- B. Thorough
- C. Hybrid
- D. BruteDics

Correct Answer: C Section: (none)

---

#### QUESTION 5

A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

- A. white box
- B. grey box
- C. red box
- D. black box

Correct Answer: D Section: (none)

[Latest 312-50V9 Dumps](#)

[312-50V9 PDF Dumps](#)

[312-50V9 Study Guide](#)