



312-50V11^{Q&As}

Certified Ethical Hacker v11 Exam

Pass EC-COUNCIL 312-50V11 Exam with 100% Guarantee

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

<https://www.geekcert.com/312-50v11.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

Fingerprinting an Operating System helps a cracker because:

- A. It defines exactly what software you have installed
- B. It opens a security-delayed window based on the port being scanned
- C. It doesn't depend on the patches that have been applied to fix existing security holes
- D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Correct Answer: D

QUESTION 2

Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session ID to the target employee. The session ID links the target employee to Boney's account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boney's account. What is the attack performed by Boney in the above scenario?

- A. Session donation attack
- B. Session fixation attack
- C. Forbidden attack
- D. CRIME attack

Correct Answer: B

QUESTION 3

As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

- A. Use the same machines for DNS and other applications
- B. Harden DNS servers
- C. Use split-horizon operation for DNS servers
- D. Restrict Zone transfers
- E. Have subnet diversity between DNS servers

Correct Answer: BCDE

QUESTION 4



From the following table, identify the wrong answer in terms of Range (ft). Standard Range (ft) 802.11a 150-150
802.11b 150-150 802.11g 150-150

802.16 (WiMax) 30 miles

- A. 802.16 (WiMax)
- B. 802.11g
- C. 802.11b
- D. 802.11a

Correct Answer: A

QUESTION 5

Which is the first step followed by Vulnerability Scanners for scanning a network?

- A. OS Detection
- B. Firewall detection
- C. TCP/UDP Port scanning
- D. Checking if the remote host is alive

Correct Answer: D

[Latest 312-50V11 Dumps](#)

[312-50V11 PDF Dumps](#)

[312-50V11 Study Guide](#)