

312-50^{Q&As}

Ethical Hacker Certified

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

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

<https://www.pass2lead.com/312-50.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

Which is the Novell Netware Packet signature level used to sign all packets ?

- A. 0
- B. 1
- C. 2
- D. 3

Correct Answer: D

Level 0 is no signature, Level 3 is communication using signature only.

QUESTION 2

Exhibit:

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

- A. har.txt
- B. SAM file
- C. wwwroot
- D. Repair file

Correct Answer: B

He is actually trying to get the file har.txt but this file contains a copy of the SAM file.

QUESTION 3

A denial of Service (DoS) attack works on the following principle:

- A. MS-DOS and PC-DOS operating system utilize a weaknesses that can be compromised and permit them to launch an attack easily.
- B. All CLIENT systems have TCP/IP stack implementation weakness that can be compromised and permit them to lunch an attack easily.
- C. Overloaded buffer systems can easily address error conditions and respond appropriately.
- D. Host systems cannot respond to real traffic, if they have an overwhelming number of incomplete connections (SYN/RCVD State).
- E. A server stops accepting connections from certain networks one those network become flooded.

Correct Answer: D

Denial-of-service (often abbreviated as DoS) is a class of attacks in which an attacker attempts to prevent legitimate users from accessing an Internet service, such as a web site. This can be done by exercising a software bug that causes the software running the service to fail (such as the "Ping of Death" attack against Windows NT systems), sending enough data to consume all available network bandwidth (as in the May, 2001 attacks against Gibson Research), or sending data in such a way as to consume a particular resource needed by the service.

QUESTION 4

If an attacker's computer sends an IPID of 31400 to a zombie (Idle Scanning) computer on an open port, what will be the response?

- A. 31400
- B. 31402
- C. The zombie will not send a response
- D. 31401

Correct Answer: D

QUESTION 5

Access control is often implemented through the use of MAC address filtering on wireless Access Points. Why is this considered to be a very limited security measure?

- A. Vendors MAC address assignment is published on the Internet.
- B. The MAC address is not a real random number.
- C. The MAC address is broadcasted and can be captured by a sniffer.
- D. The MAC address is used properly only on Macintosh computers.

Correct Answer: C

[Latest 312-50 Dumps](#)

[312-50 PDF Dumps](#)

[312-50 Study Guide](#)