



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

Ethical Hacker Certified

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

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

<https://www.pass4itsure.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**

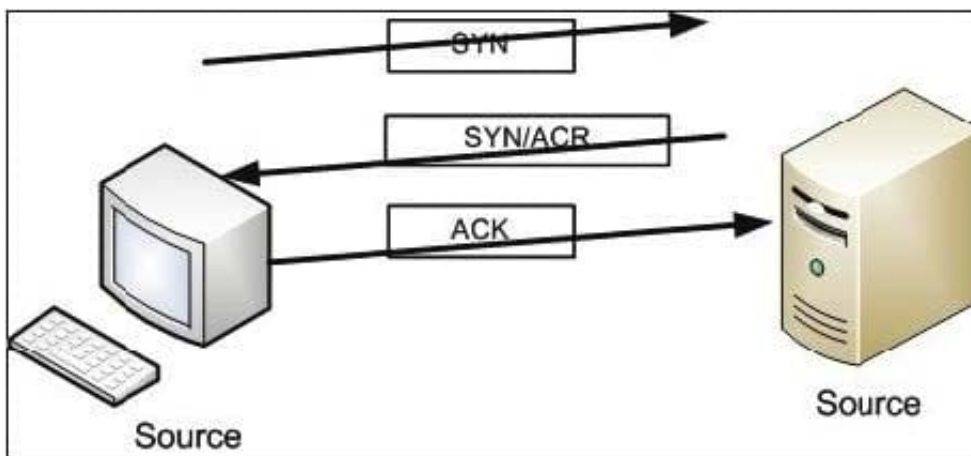
Yancey is a network security administrator for a large electric company. This company provides power for over 100,000 people in Las Vegas. Yancey has worked for his company for over 15 years and has become very successful. One day, Yancey comes in to work and finds out that the company will be downsizing and he will be out of a job in two weeks. Yancey is very angry and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. Yancey does not care if his actions land him in jail for 30 or more years, he just wants the company to pay for what they are doing to him. What would Yancey be considered?

- A. Yancey would be considered a Suicide Hacker
- B. Since he does not care about going to jail, he would be considered a Black Hat
- C. Because Yancey works for the company currently; he would be a White Hat
- D. Yancey is a Hacktivist Hacker since he is standing up to a company that is downsizing

Correct Answer: A

**QUESTION 2**

Exhibit:



Please study the exhibit carefully.

Which Protocol maintains the communication on that way?

- A. UDP
- B. IP
- C. TCP
- D. ARP
- E. RARP



Correct Answer: C

A TCP connection is always initiated with the 3-way handshake, which establishes and negotiates the actual connection over which data will be sent.

---

### QUESTION 3

Exhibit: \* Missing\*

Jason's Web server was attacked by a trojan virus. He runs protocol analyzer and notices that the trojan communicates to a remote server on the Internet. Shown below is the standard "hexdump" representation of the network packet, before

being decoded. Jason wants to identify the trojan by looking at the destination port number and mapping to a trojan-port number database on the Internet. Identify the remote server's port number by decoding the packet?

- A. Port 1890 (Net-Devil Trojan)
- B. Port 1786 (Net-Devil Trojan)
- C. Port 1909 (Net-Devil Trojan)
- D. Port 6667 (Net-Devil Trojan)

Correct Answer: D

From trace, 0x1A0B is 6667, IRC Relay Chat, which is one port used. Other ports are in the 900's.

---

### QUESTION 4

Dan is conducting a penetration testing and has found a vulnerability in a Web Application which gave him the sessionID token via a cross site scripting vulnerability. Dan wants to replay this token. However, the session ID manager (on the

server) checks the originating IP address as well. Dan decides to spoof his IP address in order to replay the sessionID. Why do you think Dan might not be able to get an interactive session?

- A. Dan cannot spoof his IP address over TCP network
- B. The server will send replies back to the spoofed IP address
- C. Dan can establish an interactive session only if he uses a NAT
- D. The scenario is incorrect as Dan can spoof his IP and get responses

Correct Answer: B

Spoofing your IP address is only effective when there is no need to establish a two way connection as all traffic meant to go to the attacker will end up at the place of the spoofed address.

---

### QUESTION 5



You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

- A. MD4
- B. DES
- C. SHA
- D. SSL

Correct Answer: B

The LM hash is computed as follows. 1. The user's password as an OEM string is converted to uppercase. 2. This password is either null-padded or truncated to 14 bytes. 3. The "fixed-length" password is split into two 7-byte halves. 4. These values are used to create two DES keys, one from each 7-byte half. 5. Each of these keys is used to DES-encrypt the constant ASCII string "KGS!@#\$ %", resulting in two 8-byte ciphertext values. 6. These two ciphertext values are concatenated to form a 16-byte value, which is the LM hash.

[Latest 312-50 Dumps](#)

[312-50 Study Guide](#)

[312-50 Exam Questions](#)