



# 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.geekcert.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

What is the advantage in encrypting the communication between the agent and the monitor in an Intrusion Detection System?

- A. Encryption of agent communications will conceal the presence of the agents
- B. The monitor will know if counterfeit messages are being generated because they will not be encrypted
- C. Alerts are sent to the monitor when a potential intrusion is detected
- D. An intruder could intercept and delete data or alerts and the intrusion can go undetected

Correct Answer: B

---

### QUESTION 2

Bill has successfully executed a buffer overflow against a Windows IIS web server. He has been able to spawn an interactive shell and plans to deface the main web page. He first attempts to use the "Echo" command to simply overwrite index.html and remains unsuccessful. He then attempts to delete the page and achieves no progress. Finally, he tries to overwrite it with another page again in vain.

What is the probable cause of Bill's problem?

- A. The system is a honeypot.
- B. There is a problem with the shell and he needs to run the attack again.
- C. You cannot use a buffer overflow to deface a web page.
- D. The HTML file has permissions of read only.

Correct Answer: D

The question states that Bill had been able to spawn an interactive shell. By this statement we can tell that the buffer overflow and its corresponding code was enough to spawn a shell. Any shell should make it possible to change the webpage. So we either don't have sufficient privilege to change the webpage (answer D) or it's a honeypot (answer A). We think the preferred answer is D

---

### QUESTION 3

Lori is a Certified Ethical Hacker as well as a Certified Hacking Forensics Investigator working as an IT security consultant. Lori has been hired on by Kiley Innovators, a large marketing firm that recently underwent a string of thefts and corporate espionage incidents. Lori is told that a rival marketing company came out with an exact duplicate product right before Kiley Innovators was about to release it. The executive team believes that an employee is leaking information to the rival company. Lori questions all employees, reviews server logs, and firewall logs; after which she finds nothing. Lori is then given permission to search through the corporate email system. She searches by email being sent to and sent from the rival marketing company.

She finds one employee that appears to be sending very large email to this other marketing company, even though they should have no reason to be communicating with them. Lori tracks down the actual emails sent and upon opening them,



only finds picture files attached to them. These files seem perfectly harmless, usually containing some kind of joke. Lori decides to use some special software to further examine the pictures and finds that each one had hidden text that was stored in each picture.

What technique was used by the Kiley Innovators employee to send information to the rival marketing company?

- A. The Kiley Innovators employee used cryptography to hide the information in the emails sent
- B. The method used by the employee to hide the information was logical watermarking
- C. The employee used steganography to hide information in the picture attachments
- D. By using the pictures to hide information, the employee utilized picture fuzzing

Correct Answer: C

---

#### QUESTION 4

In order to attack a wireless network, you put up an access point and override the signal of the real access point. As users send authentication data, you are able to capture it. What kind of attack is this?

- A. Rouge access point attack
- B. Unauthorized access point attack
- C. War Chalking
- D. WEP attack

Correct Answer: A

The definition of a Rogue access point is: 1. A wireless access point (AP) installed by an employee without the consent of the IT department. Without the proper security configuration, users have exposed their company's network to the outside world. 2. An access point (AP) set up by an attacker outside a facility with a wireless network. Also called an "evil twin," the rogue AP picks up beacons (signals that advertise its presence) from the company's legitimate AP and transmits identical beacons, which some client machines inside the building associate with.

---

#### QUESTION 5

You are having problems while retrieving results after performing port scanning during internal testing. You verify that there are no security devices between you and the target system. When both stealth and connect scanning do not work, you decide to perform a NULL scan with NMAP. The first few systems scanned shows all ports open.

Which one of the following statements is probably true?

- A. The systems have all ports open.
- B. The systems are running a host based IDS.
- C. The systems are web servers.
- D. The systems are running Windows.



Correct Answer: D

The null scan turns off all flags, creating a lack of TCP flags that should never occur in the real world. If the port is closed, a RST frame should be returned and a null scan to an open port results in no response. Unfortunately Microsoft (like usual) decided to completely ignore the standard and do things their own way. Thus this scan type will not work against systems running Windows as they choose not to respond at all. This is a good way to distinguish that the system being scanned is running Microsoft Windows.

[Latest 312-50 Dumps](#)

[312-50 PDF Dumps](#)

[312-50 VCE Dumps](#)