



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

What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

- A. Copy the system files from a known good system
- B. Perform a trap and trace
- C. Delete the files and try to determine the source
- D. Reload from a previous backup
- E. Reload from known good media

Correct Answer: E

QUESTION 2

Ben purchased a new smartphone and received some updates on it through the OTA method. He received two messages: one with a PIN from the network operator and another asking him to enter the PIN received from the operator. As soon as he entered the PIN, the smartphone started functioning in an abnormal manner. What is the type of attack performed on Ben in the above scenario?

- A. Advanced SMS phishing
- B. Bypass SSL pinning
- C. Phishing
- D. Tap \n ghost attack

Correct Answer: A

QUESTION 3

You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are starting an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

- A. IDS log
- B. Event logs on domain controller
- C. Internet Firewall/Proxy log.
- D. Event logs on the PC

Correct Answer: C



QUESTION 4

CORRECT TEXT

Allen, a professional pen tester, was hired by xpertTech solutWns to perform an attack simulation on the organization\\'s network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. B/ enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.

identify the NetBIOS code used for obtaining the messenger service running for the logged- in user?

- A.
- B.
- C.
- D.

Correct Answer: C

Windows Messenger administrationCourier administration is an organization based framework notice Windows administration by Microsoft that was remembered for some prior forms of Microsoft Windows. This resigned innovation, despite the fact that it has a comparable name, isn\\'t connected in any capacity to the later, Internet-based Microsoft Messenger administration for texting or to Windows Messenger and Windows Live Messenger (earlier named MSN Messenger) customer programming. The Messenger Service was initially intended for use by framework managers to tell Windows clients about their networks.[1] It has been utilized malevolently to introduce spring up commercials to clients over the Internet (by utilizing mass- informing frameworks which sent an ideal message to a predetermined scope of IP addresses). Despite the fact that Windows XP incorporates a firewall, it isn\\'t empowered naturally. Along these lines, numerous clients got such messages. Because of this maltreatment, the Messenger Service has been debilitated as a matter of course in Windows XP Service Pack 2.

QUESTION 5

Mr. Omkar performed tool-based vulnerability assessment and found two vulnerabilities. During analysis, he found that these issues are not true vulnerabilities.

What will you call these issues?

- A. False positives
- B. True negatives
- C. True positives
- D. False negatives

Correct Answer: A

[312-50V11 Practice Test](#)

[312-50V11 Study Guide](#)

[312-50V11 Exam Questions](#)