



# ECSAV10<sup>Q&As</sup>

EC-Council Certified Security Analyst (ECSA) v10 : Penetration Testing

## Pass EC-COUNCIL ECSAV10 Exam with 100% Guarantee

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

<https://www.geekcert.com/ecsav10.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

Sandra, a wireless network auditor, discovered her client is using WEP. To prove the point that the WEP encryption is very weak, she wants to decrypt some WEP packets. She successfully captured the WEP data packets, but could not reach the content as the data is encrypted.

Which of the following will help Sandra decrypt the data packets without knowing the key?

- A. Fragmentation Attack
- B. Chopchop Attack
- C. ARP Poisoning Attack
- D. Packet injection Attack

Correct Answer: B

---

### QUESTION 2

After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts responds to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

- A. A switched network will not respond to packets sent to the broadcast address
- B. Only IBM AS/400 will reply to this scan
- C. Only Unix and Unix-like systems will reply to this scan
- D. Only Windows systems will reply to this scan

Correct Answer: C

---

### QUESTION 3

A chipset is a group of integrated circuits that are designed to work together and are usually marketed as a single product." It is generally the motherboard chips or the chips used on the expansion card. Which one of the following is well supported in most wireless applications?

- A. Orinoco chipsets
- B. Prism II chipsets
- C. Atheros Chipset
- D. Cisco chipset



---

Correct Answer: B

---

#### QUESTION 4

Sam was asked to conduct penetration tests on one of the client's internal networks. As part of the testing process, Sam performed enumeration to gain information about computers belonging to a domain, list of shares on the individual hosts in the network, policies and passwords.

Identify the enumeration technique.

- A. NTP Enumeration
- B. NetBIOS Enumeration
- C. DNS Enumeration
- D. SMTP Enumeration

Correct Answer: B

---

#### QUESTION 5

Which one of the following scans starts, but does not complete the TCP handshake sequence for each port selected, and it works well for direct scanning and often works well through firewalls?

- A. SYN Scan
- B. Connect() scan
- C. XMAS Scan
- D. Null Scan

Correct Answer: A

[Latest ECSAV10 Dumps](#)

[ECSAV10 Practice Test](#)

[ECSAV10 Exam Questions](#)