



# 412-79V8<sup>Q&As</sup>

EC-Council Certified Security Analyst (ECSA)

## Pass EC-COUNCIL 412-79V8 Exam with 100% Guarantee

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

<https://www.passapply.com/412-79v8.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 one of the following is a supporting tool for 802.11 (wireless) packet injections, it spoofs 802.11 packets to verify whether the access point is valid or not?

- A. Aircsnort
- B. Aircrack
- C. Aircrack-ng
- D. WEPCrack

Correct Answer: C

---

#### QUESTION 2

Which of the following protocols' traffic is captured by using the filter tcp.port==3389 in the Wireshark tool?

- A. Reverse Gossip Transport Protocol (RGTP)
- B. Real-time Transport Protocol (RTP)
- C. Remote Desktop Protocol (RDP)
- D. Session Initiation Protocol (SIP)

Correct Answer: C

---

#### QUESTION 3

Which one of the following is a command line tool used for capturing data from the live network and copying those packets to a file?

- A. Wireshark: Capinfos
- B. Wireshark: Tcpdump
- C. Wireshark: Text2pcap
- D. Wireshark: Dumpcap

Correct Answer: D

---

#### QUESTION 4

A man enters a PIN number at an ATM machine, being unaware that the person next to him was watching. Which of the following social engineering techniques refers to this type of information theft?



- A. Shoulder surfing
- B. Phishing
- C. Insider Accomplice
- D. Vishing

Correct Answer: A

---

#### QUESTION 5

A Demilitarized Zone (DMZ) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. Usage of a protocol within a DMZ environment is highly variable based on the specific needs of an organization. Privilege escalation, system is compromised when the code runs under root credentials, and DoS attacks are the basic weakness of which one of the following Protocol?

- A. Lightweight Directory Access Protocol (LDAP)
- B. Simple Network Management Protocol (SNMP)
- C. Telnet
- D. Secure Shell (SSH)

Correct Answer: D

[412-79V8 Practice Test](#)

[412-79V8 Study Guide](#)

[412-79V8 Braindumps](#)