



412-79^{Q&As}

EC-Council Certified Security Analyst (ECSA)

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

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

<https://www.geekcert.com/412-79.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

You are working as Computer Forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firms employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will.

What do you do?

- A. Inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned
- B. Inform the owner that conducting an investigation without a policy is a violation of the 4th amendment
- C. Inform the owner that conducting an investigation without a policy is a violation of the employees expectation of privacy
- D. Inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies

Correct Answer: C

QUESTION 2

Software firewalls work at which layer of the OSI model?

- A. Transport
- B. Application
- C. Network
- D. Data Link

Correct Answer: D

QUESTION 3

This organization maintains a database of hash signatures for known software:

- A. International Standards Organization
- B. Institute of Electrical and Electronics Engineers
- C. National Software Reference Library
- D. American National standards Institute

Correct Answer: C

**QUESTION 4**

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 respond 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 5

Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

- A. Application-level proxy firewall
- B. Data link layer firewall
- C. Packet filtering firewall
- D. Circuit-level proxy firewall

Correct Answer: A

[412-79 VCE Dumps](#)

[412-79 Study Guide](#)

[412-79 Braindumps](#)