

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

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.leads4pass.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**

Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?

- A. PDF passwords can easily be cracked by software brute force tools
- B. PDF passwords are not considered safe by Sarbanes-Oxley
- C. PDF passwords are converted to clear text when sent through E-mail
- D. When sent through E-mail, PDF passwords are stripped from the document completely

Correct Answer: A

---

**QUESTION 2**

A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its proper destination? A packet is sent to a router that does not have the packet destination address in its route table, how will the packet get to its proper destination?

- A. Root Internet servers
- B. Border Gateway Protocol
- C. Gateway of last resort
- D. Reverse DNS

Correct Answer: C

---

**QUESTION 3**

In General, \_\_\_\_\_ Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.

- A. Network Forensics
- B. Data Recovery
- C. Disaster Recovery
- D. Computer Forensics

Correct Answer: D

---

**QUESTION 4**

An Expert witness give an opinion if:

- A. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors
- B. To define the issues of the case for determination by the finder of fact
- C. To stimulate discussion between the consulting expert and the expert witness
- D. To deter the witness from expanding the scope of his or her investigation beyond the requirements of the case

Correct Answer: A

---

## QUESTION 5

Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?

- A. network-based IDS systems (NIDS)
- B. host-based IDS systems (HIDS)
- C. anomaly detection
- D. signature recognition

Correct Answer: B

[412-79 Practice Test](#)

[412-79 Study Guide](#)

[412-79 Braindumps](#)