



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.pass4itsure.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**

After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, statefull firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

- A. Statefull firewalls do not work with packet filtering firewalls
- B. NAT does not work with statefull firewalls
- C. NAT does not work with IPSEC
- D. IPSEC does not work with packet filtering firewalls

Correct Answer: C

QUESTION 2

You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers:

```
http://172.168.4.131/level/99/exec/show/config
```

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

- A. URL Obfuscation Arbitrary Administrative Access Vulnerability
- B. Cisco IOS Arbitrary Administrative Access Online Vulnerability
- C. HTTP Configuration Arbitrary Administrative Access Vulnerability
- D. HTML Configuration Arbitrary Administrative Access Vulnerability

Correct Answer: C

QUESTION 3

With Regard to using an Antivirus scanner during a computer forensics investigation, You should:

- A. Scan the suspect hard drive before beginning an investigation
- B. Never run a scan on your forensics workstation because it could change your systems configuration
- C. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation
- D. Scan your Forensics workstation before beginning an investigation

Correct Answer: D



QUESTION 4

One way to identify the presence of hidden partitions on a suspect s hard drive is to:

- A. Add up the total size of all known partitions and compare it to the total size of the hard drive
- B. Examine the FAT and identify hidden partitions by noting an H in the partition Type field
- C. Examine the LILO and note an H in the partition Type field
- D. It is not possible to have hidden partitions on a hard drive

Correct Answer: A

QUESTION 5

If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?

- A. The system files have been copied by a remote attacker
- B. The system administrator has created an incremental backup
- C. The system has been compromised using a t0rnrootkit
- D. Nothing in particular as these can be operational files

Correct Answer: D

[412-79 VCE Dumps](#)

[412-79 Exam Questions](#)

[412-79 Braindumps](#)