



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.passapply.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

Harold is a security analyst who has just run the `rdisk /s` command to grab the backup SAM file on a computer. Where should Harold navigate on the computer to find the file?

- A. `%systemroot%\system32\drivers\etc`
- B. `%systemroot%\repair`
- C. `%systemroot%\LSA`
- D. `%systemroot%\system32\LSA`

Correct Answer: B

QUESTION 2

When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

- A. Avoid cross talk
- B. Avoid over-saturation of wireless signals
- C. So that the access points will work on different frequencies
- D. Multiple access points can be set up on the same channel without any issues

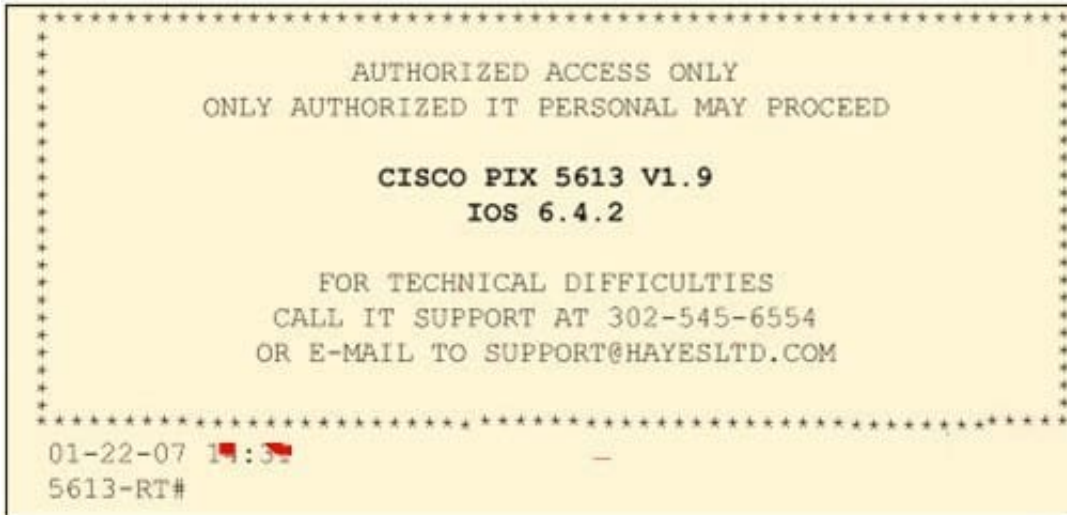
Correct Answer: A

QUESTION 3

Click on the Exhibit Button

Paulette works for an IT security consulting company that is currently performing an audit for the firm ACE Unlimited. Paulette's duties include logging on to all the company's network equipment to ensure IOS versions are up-to-date and all the other security settings are as stringent as possible. Paulette presents the following screenshot to her boss so he can inform the client about necessary changes need to be made. From the screenshot, what changes should the client company make?

Exhibit:



- A. The banner should not state "only authorized IT personnel may proceed"
- B. Remove any identifying numbers, names, or version information
- C. The banner should include the Cisco tech support contact information as well
- D. The banner should have more detail on the version numbers for the network equipment

Correct Answer: B

QUESTION 4

What is the advantage in encrypting the communication between the agent and the monitor in an Intrusion Detection System?

- A. Encryption of agent communications will conceal the presence of the agents
- B. Alerts are sent to the monitor when a potential intrusion is detected
- C. An intruder could intercept and delete data or alerts and the intrusion can go undetected
- D. The monitor will know if counterfeit messages are being generated because they will not be encrypted

Correct Answer: D

QUESTION 5

What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images?

- A. mcopy
- B. image
- C. MD5



D. dd

Correct Answer: D

[412-79 PDF Dumps](#)

[412-79 VCE Dumps](#)

[412-79 Braindumps](#)