EC1-349 Q&As

Computer Hacking Forensic Investigator Exam

Pass EC-COUNCIL EC1-349 Exam with 100% Guarantee

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

https://www.pass2lead.com/ec1-349.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

When monitoring for both intrusion and security events between multiple computers, it is essential that the computers\\' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

A. Time-Sync Protocol

B. SyncTime Service

C. Network Time Protocol

D. Universal Time Set

Correct Answer: C

QUESTION 2

When examining a file with a Hex Editor, what space does the file header occupy?

A. The first several bytes of the file

B. One byte at the beginning of the file

C. None, file headers are contained in the FAT

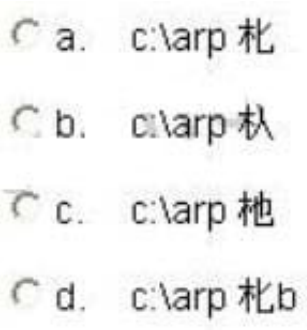
D. The last several bytes of the file

Correct Answer: A

QUESTION 3

The ARP table of a router comes in handy for Investigating network attacks, as the table contains IP addresses associated with the respective MAC addresses.

The ARP table can be accessed using the _____command in Windows 7.



A. Option A

B. Option B

C. Option C

D. Option D

Correct Answer: A

QUESTION 4

You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Oligomorhic

B. Transmorphic

C. Polymorphic

D. Metamorphic

Correct Answer: D

QUESTION 5

What does ICMP Type 3/Code 13 mean?

A. Administratively Blocked

B. Host Unreachable

C. Protocol Unreachable

D. Port Unreachable

Correct Answer: A