# CEH-001<sup>Q&As</sup>

Certified Ethical Hacker (CEH)

## Pass GAQM CEH-001 Exam with 100% Guarantee

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

**https://www.pass4itsure.com/ceh-001.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GAQM Official Exam Center

⚙ **Instant Download** After Purchase

⚙ **100% Money Back** Guarantee

⚙ **365 Days** Free Update

⚙ **800,000+** Satisfied Customers

**QUESTION 1**

What is the main advantage that a network-based IDS/IPS system has over a host-based solution?

A. They do not use host system resources.

B. They are placed at the boundary, allowing them to inspect all traffic.

C. They are easier to install and configure.

D. They will not interfere with user interfaces.

Correct Answer: A

**QUESTION 2**

What are common signs that a system has been compromised or hacked? (Choose three.)

A. Increased amount of failed logon events

B. Patterns in time gaps in system and/or event logs

C. New user accounts created

D. Consistency in usage baselines

E. Partitions are encrypted

F. Server hard drives become fragmented

Correct Answer: ABC

**QUESTION 3**

On a backdoored Linux box there is a possibility that legitimate programs are modified or trojaned. How is it possible to list processes and uids associated with them in a more reliable manner?

A. Use "ls"

B. Use "lsof"

C. Use "echo"

D. Use "netstat"

Correct Answer: B

**QUESTION 4**

Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

A. Penetration testing

B. Social engineering

C. Vulnerability scanning

D. Access control list reviews

Correct Answer: A

**QUESTION 5**

Neil is closely monitoring his firewall rules and logs on a regular basis. Some of the users have complained to Neil that there are a few employees who are visiting offensive web site during work hours, without any consideration for others. Neil knows that he has an up-to- date content filtering system and such access should not be authorized. What type of technique might be used by these offenders to access the Internet without restriction?

A. They are using UDP that is always authorized at the firewall

B. They are using an older version of Internet Explorer that allow them to bypass the proxy server

C. They have been able to compromise the firewall, modify the rules, and give themselves proper access

D. They are using tunneling software that allows them to communicate with protocols in a way it was not intended

Correct Answer: D