# CEH-001 Q&As

Certified Ethical Hacker (CEH)

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

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

**https://www.geekcert.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**

An IT security engineer notices that the company\\'s web server is currently being hacked. What should the engineer do next?

A. Unplug the network connection on the company\\'s web server.

B. Determine the origin of the attack and launch a counterattack.

C. Record as much information as possible from the attack.

D. Perform a system restart on the company\\'s web server.

Correct Answer: C

**QUESTION 2**

What are the three phases involved in security testing?

A. Reconnaissance, Conduct, Report

B. Reconnaissance, Scanning, Conclusion

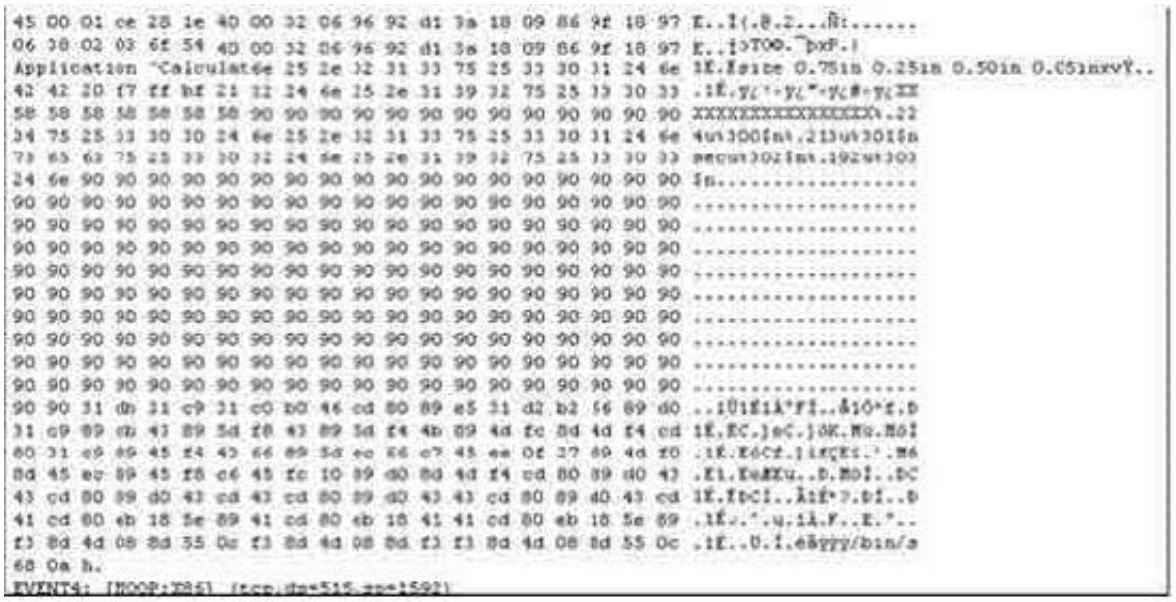
C. Preparation, Conduct, Conclusion

D. Preparation, Conduct, Billing

Correct Answer: C

**QUESTION 3**

Exhibit:




The following is an entry captured by a network IDS.You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a

buffer overflow attack. You also notice "/bin/sh" in the ASCII part of the output.

As an analyst what would you conclude about the attack?

A. The buffer overflow attack has been neutralized by the IDS

B. The attacker is creating a directory on the compromised machine

C. The attacker is attempting a buffer overflow attack and has succeeded

D. The attacker is attempting an exploit that launches a command-line shell

Correct Answer: D

**QUESTION 4**

Network Intrusion Detection systems can monitor traffic in real time on networks.

Which one of the following techniques can be very effective at avoiding proper detection?

A. Fragmentation of packets.

B. Use of only TCP based protocols.

C. Use of only UDP based protocols.

D. Use of fragmented ICMP traffic only.

Correct Answer: A

**QUESTION 5**

Susan has attached to her company\\'s network. She has managed to synchronize her boss\\'s sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory. What kind of attack is Susan carrying on?

A. A sniffing attack

B. A spoofing attack

C. A man in the middle attack

D. A denial of service attack

Correct Answer: C