

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.leads4pass.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

Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions?

- A. Firewall
- B. Honeypot
- C. Core server
- D. Layer 4 switch

Correct Answer: B

QUESTION 2

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's computer to update the router configuration. What type of an alert is this?

- A. False positive
- B. False negative
- C. True positive
- D. True negative

Correct Answer: A

QUESTION 3

On a default installation of Microsoft IIS web server, under which privilege does the web server software execute?

- A. Everyone
- B. Guest
- C. System
- D. Administrator

Correct Answer: C

QUESTION 4

Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site.

One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message
Hacker

Message: You are dead! Freaks!

From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact. No changes were apparent. Joseph called a friend of

his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site.

To help make sense of this problem, Joseph decided to access the Web site using his dial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith.

After his modem connected, he quickly typed `www.masonins.com` in his browser to reveal the following web page:

Hacker Mess@ge:

Y0u @re De@d! Fre@ks!

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every

system file and all the Web content on the server were intact.

How did the attacker accomplish this hack?

- A. ARP spoofing
- B. SQL injection
- C. DNS poisoning
- D. Routing table injection

Correct Answer: C

QUESTION 5

Most NIDS systems operate in layer 2 of the OSI model. These systems feed raw traffic into a detection engine and rely on the pattern matching and/or statistical analysis to determine what is malicious. Packets are not processed by the host's TCP/IP stack allowing the NIDS to analyze traffic the host would otherwise discard. Which of the following tools allows an attacker to intentionally craft packets to confuse pattern-matching NIDS systems, while still being correctly assembled by the host TCP/IP stack to render the attack payload?

- A. Defrag
- B. Tcpfrag
- C. Tcpdump

D. Fragroute

Correct Answer: D

[Latest CEH-001 Dumps](#)

[CEH-001 PDF Dumps](#)

[CEH-001 Study Guide](#)