

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.pass2lead.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 of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application?

- A. The victim user must open the malicious link with an Internet Explorer prior to version 8.
- B. The session cookies generated by the application do not have the HttpOnly flag set.
- C. The victim user must open the malicious link with a Firefox prior to version 3.
- D. The web application should not use random tokens.

Correct Answer: D

QUESTION 2

While attempting to discover the remote operating system on the target computer, you receive the following results from an nmap scan:

```
Starting nmap V. 3.10ALPHA9 ( www.insecure.org/nmap/ )
<http://www.insecure.org/nmap/> )
Interesting ports on 172.121.12.222:
(The 1592 ports scanned but not shown below are in state: filtered)
Port State Service
21/tcp open ftp
25/tcp open smtp
53/tcp closed domain
80/tcp open http
443/tcp open https
```

Remote operating system guess: Too many signatures match to reliably guess the OS.

Nmap run completed -- 1 IP address (1 host up) scanned in 277.483 seconds

What should be your next step to identify the OS?

- A. Perform a firewalk with that system as the target IP
- B. Perform a tcp traceroute to the system using port 53
- C. Run an nmap scan with the -v-v option to give a better output
- D. Connect to the active services and review the banner information

Correct Answer: D

QUESTION 3

The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

You are hired to conduct security testing on their network. You successfully brute-force the SNMP community string using a SNMP crack tool. The access-list configured at the router prevents you from establishing a successful connection.

You want to retrieve the Cisco configuration from the router. How would you proceed?

- A. Use the Cisco's TFTP default password to connect and download the configuration file
- B. Run a network sniffer and capture the returned traffic with the configuration file from the router
- C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address
- D. Send a customized SNMP set request with a spoofed source IP address in the range - 192.168.1.0

Correct Answer: BD

QUESTION 4

Bob wants to prevent attackers from sniffing his passwords on the wired network. Which of the following lists the best options?

- A. RSA, LSA, POP
- B. SSID, WEP, Kerberos
- C. SMB, SMTP, Smart card
- D. Kerberos, Smart card, Stanford SRP

Correct Answer: D

QUESTION 5

Password cracking programs reverse the hashing process to recover passwords.(True/False).

- A. True
- B. False

Correct Answer: B
