



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.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**

Stephanie works as senior security analyst for a manufacturing company in Detroit. Stephanie manages network security throughout the organization. Her colleague Jason told her in confidence that he was able to see confidential corporate information posted on the external website <http://www.jeansclothesman.com>. He tries random URLs on the company's website and finds confidential information leaked over the web. Jason says this happened about a month ago. Stephanie visits the said URLs, but she finds nothing. She is very concerned about this, since someone should be held accountable if there was sensitive information posted on the website.

Where can Stephanie go to see past versions and pages of a website?

- A. She should go to the web page [Sampspade.org](http://www.sampspade.org) to see web pages that might no longer be on the website
- B. If Stephanie navigates to [Search.com](http://www.search.com); she will see old versions of the company website
- C. Stephanie can go to [Archive.org](http://www.archive.org) to see past versions of the company website
- D. [AddressPast.com](http://www.addresspast.com) would have any web pages that are no longer hosted on the company's website

Correct Answer: C

QUESTION 2

After studying the following log entries, how many user IDs can you identify that the attacker has tampered with?

1.

```
mkdir -p /etc/X11/applnk/Internet/etc
```

2.

```
mkdir -p /etc/X11/applnk/Internet.etcpasswd
```

3.

```
touch -acmr /etc/passwd /etc/X11/applnk/Internet.etcpasswd
```

4.

```
touch -acmr /etc /etc/X11/applnk/Internet/etc
```

5.

```
passwd nobody -d
```

6.

```
/usr/sbin/adduser dns -d/bin -u 0 -g 0 -s/bin/bash
```

7.

```
passwd dns -d
```



8.

`touch -acmr /etc/X11/applnk/Internet/.etcpasswd /etc/passwd`

9.

`touch -acmr /etc/X11/applnk/Internet/.etc /etc`

A. IUSR_

B. acmr, dns

C. nobody, dns

D. nobody, IUSR_

Correct Answer: C

QUESTION 3

Blane is a network security analyst for his company. From an outside IP, Blane performs an XMAS scan using Nmap. Almost every port scanned does not illicit a response. What can he infer from this kind of response?

A. These ports are open because they do not illicit a response.

B. He can tell that these ports are in stealth mode.

C. If a port does not respond to an XMAS scan using NMAP, that port is closed.

D. The scan was not performed correctly using NMAP since all ports, no matter what their state, will illicit some sort of response from an XMAS scan.

Correct Answer: A

QUESTION 4

Which command line switch would be used in NMAP to perform operating system detection?

A. -OS

B. -sO

C. -sP

D. -O

Correct Answer: D

QUESTION 5

Hayden is the network security administrator for her company, a large finance firm based in Miami. Hayden just returned



from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. Hayden is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established she sends RST packets to those hosts to stop the session. She does this to see how her intrusion detection system will log the traffic. What type of scan is Hayden attempting here?

- A. Hayden is attempting to find live hosts on her company's network by using an XMAS scan
- B. She is utilizing a SYN scan to find live hosts that are listening on her network
- C. The type of scan, she is using is called a NULL scan
- D. Hayden is using a half-open scan to find live hosts on her network

Correct Answer: D

[Latest CEH-001 Dumps](#)

[CEH-001 VCE Dumps](#)

[CEH-001 Study Guide](#)