

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

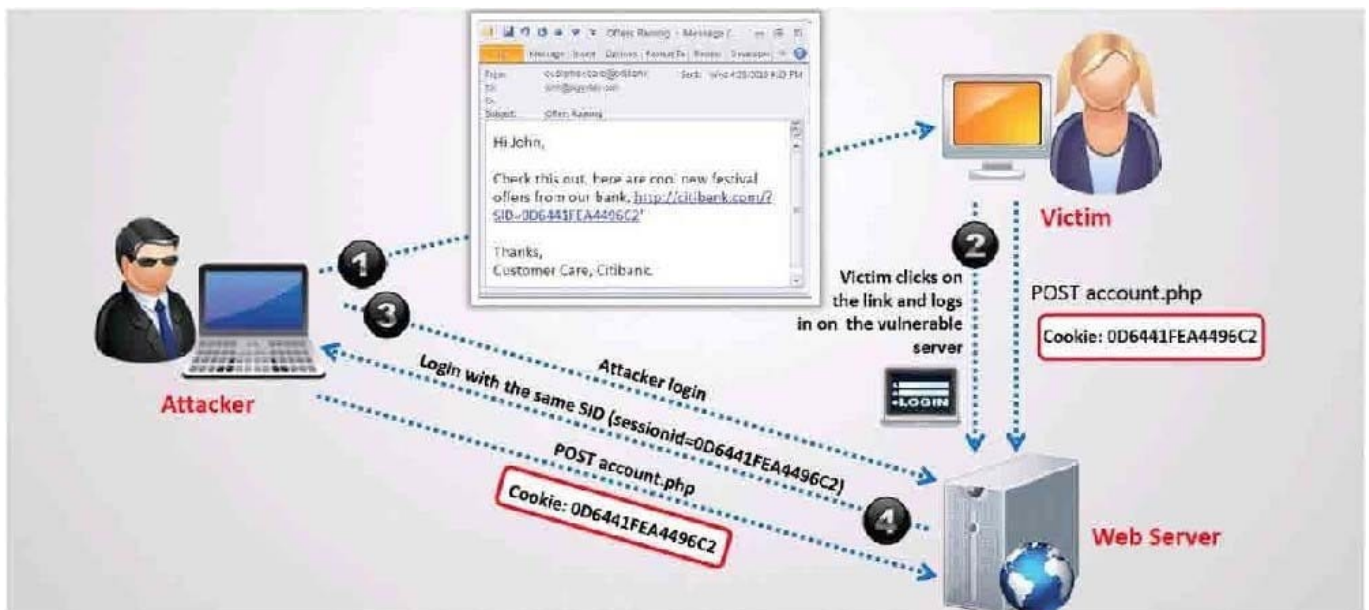
A Buffer Overflow attack involves:

- A. Using a trojan program to direct data traffic to the target host's memory stack
- B. Flooding the target network buffers with data traffic to reduce the bandwidth available to legitimate users
- C. Using a dictionary to crack password buffers by guessing user names and passwords
- D. Poorly written software that allows an attacker to execute arbitrary code on a target system

Correct Answer: D

QUESTION 2

What type of session hijacking attack is shown in the exhibit?



- A. Cross-site scripting Attack
- B. SQL Injection Attack
- C. Token sniffing Attack
- D. Session Fixation Attack

Correct Answer: D

QUESTION 3

You receive an email with the following message:

Hello Steve,

We are having technical difficulty in restoring user database record after the recent blackout. Your account data is corrupted. Please logon to the SuperEmailServices.com and change your password.

<http://www.supermailservices.com@0xde.0xad.0xbe.0xef/support/logon.htm>

If you do not reset your password within 7 days, your account will be permanently disabled locking you out from our e-mail services.

Sincerely,

Technical Support

SuperEmailServices

From this e-mail you suspect that this message was sent by some hacker since you have been using their e-mail services for the last 2 years and they have never sent out an e-mail such as this. You also observe the URL in the message and

confirm your suspicion about 0xde.0xad.0xbde.0xef which looks like hexadecimal numbers. You immediately enter the following at Windows 2000 command prompt:

Ping 0xde.0xad.0xbe.0xef

You get a response with a valid IP address.

What is the obstructed IP address in the e-mail URL?

- A. 222.173.190.239
- B. 233.34.45.64
- C. 54.23.56.55
- D. 199.223.23.45

Correct Answer: A

QUESTION 4

Finding tools to run dictionary and brute forcing attacks against FTP and Web servers is an easy task for hackers. They use tools such as arhontus or brutus to break into remote servers.

```
CEH# ./rpa
Remote Password Assassin V 1.0
Roses Labs / w00w00
Usage: ./rpa <host> (options)
Options:
-l : Login file to use.
-s : Use the same login.
-c : Password file to use.
-r : Attack FlowPoint Router.
-t : Attack Telnet Port.
-f : Attack FTP Port.
-p : Attack POP Port.
CEH# ./rpa 10.0.0.34 -t -f -c passwords.txt -s linksys
```

A command such as this, will attack a given 10.0.0.34 FTP and Telnet servers simultaneously with a list of passwords and a single login name. linksys. Many FTP- specific password-guessing tools are also available from major security sites.

What defensive measures will you take to protect your network from these attacks?

- A. Never leave a default password
- B. Never use a password that can be found in a dictionary
- C. Never use a password related to your hobbies, pets, relatives, or date of birth.
- D. Use a word that has more than 21 characters from a dictionary as the password
- E. Never use a password related to the hostname, domain name, or anything else that can be found with whois

Correct Answer: ABCE

QUESTION 5

Which of the following are advantages of adopting a Single Sign On (SSO) system? (Choose two.)

- A. A reduction in password fatigue for users because they do not need to know multiple passwords when accessing multiple applications
- B. A reduction in network and application monitoring since all recording will be completed at the SSO system
- C. A reduction in system administration overhead since any user login problems can be resolved at the SSO system
- D. A reduction in overall risk to the system since network and application attacks can only happen at the SSO point

Correct Answer: AC

[Latest CEH-001 Dumps](#)

[CEH-001 Practice Test](#)

[CEH-001 Exam Questions](#)