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 types of detection methods are employed by Network Intrusion Detection Systems (NIDS)? (Choose two.)

A. Signature

B. Anomaly

C. Passive

D. Reactive

Correct Answer: AB

QUESTION 2

In Linux, the three most common commands that hackers usually attempt to Trojan are:

A. car, xterm, grep

B. netstat, ps, top

C. vmware, sed, less

D. xterm, ps, nc

Correct Answer: B

QUESTION 3

Which one of the following attacks will pass through a network layer intrusion detection system undetected?

A. A teardrop attack

B. A SYN flood attack

C. A DNS spoofing attack

D. A test.cgi attack

Correct Answer: D

QUESTION 4

For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender\\'s public key

B. Receiver\\'s private key

C. Receiver\\'s public key

D. Sender\\'s private key

Correct Answer: D

QUESTION 5

Peter is a Network Admin. He is concerned that his network is vulnerable to a smurf attack.

What should Peter do to prevent a smurf attack?

Select the best answer.

A. He should disable unicast on all routers

B. Disable multicast on the router

C. Turn off fragmentation on his router

D. Make sure all anti-virus protection is updated on all systems

E. Make sure his router won\\'t take a directed broadcast

Correct Answer: E

QUESTION 6

John is the network administrator of XSECURITY systems. His network was recently compromised. He analyzes the log files to investigate the attack. Take a look at the following Linux log file snippet. The hacker compromised and "owned" a

Linux machine.

What is the hacker trying to accomplish here?

```
[root@apollo /]# rm rootkit.c
[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ; ps -aux | grep
portmap ; rm /sbin/portmap ; rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf
.bash* ; rm -rf /root/.bash_history ; rm -rf /usr/sbin/namedps -aux | grep
inetd ; ps -aux | grep portmap ; rm /sbin/por359 ? 00:00:00 inetd
359 ? 00:00:00 inetd
rm: cannot remove `/tmp/h': No such file or directory
rm: cannot remove `/usr/sbin/rpc.portmap': No such file or directory
[root@apollo /]# ps -aux | grep portmap
[root@apollo /]# [root@apollo /]# ps -aux | grep inetd ; ps -aux | grep
portmap ; rm /sbin/portmap ; rm /tmp/h ; rm /usr/sbin/rpc.portmap ; rm -rf
.bash* ; rm -rf /root/.bash_history ; rm -rf /usr/sbin/namedps -aux | grep
inetd ; ps -aux | grep portmap ; rm /sbin/por359 ? 00:00:00 inetd
rm: cannot remove `/sbin/portmap': No such file or directory
rm: cannot remove `/tmp/h': No such file or directory
rm: cannot remove `/usr/sbin/rpc.portmap': No such file or directory
[root@apollo /]# rm: cannot remove `/sbin/portmap': No such file or directory
```

A. The hacker is attempting to compromise more machines on the network

B. The hacker is planting a rootkit

C. The hacker is running a buffer overflow exploit to lock down the system

D. The hacker is trying to cover his tracks

Correct Answer: D

QUESTION 7

In the software security development life cyle process, threat modeling occurs in which phase?

A. Design

B. Requirements

C. Verification

D. Implementation

Correct Answer: A

QUESTION 8

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 9

A digital signature is simply a message that is encrypted with the public key instead of the private key.

A. true

B. false

Correct Answer: B

QUESTION 10

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 positve

D. True negative

Correct Answer: A

QUESTION 11

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

A. USER, NICK

B. LOGIN, NICK

C. USER, PASS

D. LOGIN, USER

Correct Answer: A

QUESTION 12

Doug is conducting a port scan of a target network. He knows that his client target network has a web server and that there is a mail server also which is up and running. Doug has been sweeping the network but has not been able to elicit

any response from the remote target. Which of the following could be the most likely cause behind this lack of response? Select 4.

A. UDP is filtered by a gateway

B. The packet TTL value is too low and cannot reach the target

C. The host might be down

D. The destination network might be down

E. The TCP windows size does not match

F. ICMP is filtered by a gateway

Correct Answer: ABCF

QUESTION 13

What type of encryption does WPA2 use?

A. DES 64 bit

B. AES-CCMP 128 bit

C. MD5 48 bit

D. SHA 160 bit

Correct Answer: B

QUESTION 14

Which of the following is the primary objective of a rootkit?

A. It opens a port to provide an unauthorized service

B. It creates a buffer overflow

C. It replaces legitimate programs

D. It provides an undocumented opening in a program

Correct Answer: C

QUESTION 15

E-mail scams and mail fraud are regulated by which of the following?

A. 18 U.S.C. par. 1030 Fraud and Related activity in connection with Computers

B. 18 U.S.C. par. 1029 Fraud and Related activity in connection with Access Devices

C. 18 U.S.C. par. 1362 Communication Lines, Stations, or Systems

D. 18 U.S.C. par. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Correct Answer: A