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.passapply.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

Steven the hacker realizes that the network administrator of XYZ is using syskey to protect organization resources in the Windows 2000 Server. Syskey independently encrypts the hashes so that physical access to the server, tapes, or ERDs is only first step to cracking the passwords. Steven must break through the encryption used by syskey before he can attempt to brute force dictionary attacks on the hashes. Steven runs a program called "SysCracker" targeting the Windows 2000 Server machine in attempting to crack the hash used by Syskey. He needs to configure the encryption level before he can launch attach.

How many bits does Syskey use for encryption?

A. 40 bit

B. 64 bit

C. 256 bit

D. 128 bit

Correct Answer: D

QUESTION 2

A XYZ security System Administrator is reviewing the network system log files.

He notes the following:

Network log files are at 5 MB at 12:00 noon. At 14:00 hours, the log files at 3 MB.

What should he assume has happened and what should he do about the situation?

A. He should contact the attacker\\'s ISP as soon as possible and have the connection disconnected.

B. He should log the event as suspicious activity, continue to investigate, and take further steps according to site security policy.

C. He should log the file size, and archive the information, because the router crashed.

D. He should run a file system check, because the Syslog server has a self correcting file system problem.

E. He should disconnect from the Internet discontinue any further unauthorized use, because an attack has taken place.

Correct Answer: B

QUESTION 3

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 4

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 5

Which statement best describes a server type under an N-tier architecture?

A. A group of servers at a specific layer

B. A single server with a specific role

C. A group of servers with a unique role

D. A single server at a specific layer

Correct Answer: C

QUESTION 6

This kind of attack will let you assume a users identity at a dynamically generated web page or site:

A. SQL Injection

B. Cross Site Scripting

C. Session Hijacking

D. Zone Transfer

Correct Answer: B

QUESTION 7

You are footprinting an organization and gathering competitive intelligence. You visit the company\\'s website for contact information and telephone numbers but do not find them listed there. You know they had the entire staff directory listed on their website 12 months ago but now it is not there. Is there any way you can retrieve information from a website that is outdated?

A. Visit Google\\'s search engine and view the cached copy

B. Crawl the entire website and store them into your computer

C. Visit Archive.org web site to retrieve the Internet archive of the company\\'s website

D. Visit the company\\'s partners and customers website for this information

Correct Answer: C

QUESTION 8

Eve decides to get her hands dirty and tries out a Denial of Service attack that is relatively new to her. This time she envisages using a different kind of method to attack Brownies Inc. Eve tries to forge the packets and uses the broadcast address. She launches an attack similar to that of fraggle. What is the technique that Eve used in the case above?

A. Smurf

B. Bubonic

C. SYN Flood

D. Ping of Death

Correct Answer: A

QUESTION 9

Tess King is making use of Digest Authentication for her Web site. Why is this considered to be more secure than Basic authentication?

A. Basic authentication is broken

B. The password is never sent in clear text over the network

C. The password sent in clear text over the network is never reused.

D. It is based on Kerberos authentication protocol

Correct Answer: B

QUESTION 10

Within the context of Computer Security, which of the following statements describes Social Engineering best?

A. Social Engineering is the act of publicly disclosing information

B. Social Engineering is the means put in place by human resource to perform time accounting

C. Social Engineering is the act of getting needed information from a person rather than breaking into a system

D. Social Engineering is a training program within sociology studies

Correct Answer: C

QUESTION 11

John wishes to install a new application onto his Windows 2000 server.

He wants to ensure that any application he uses has not been Trojaned.

What can he do to help ensure this?

A. Compare the file\\'s MD5 signature with the one published on the distribution media

B. Obtain the application via SSL

C. Compare the file\\'s virus signature with the one published on the distribution media

D. Obtain the application from a CD-ROM disc

Correct Answer: A

QUESTION 12

An Evil Cracker is attempting to penetrate your private network security. To do this, he must not be seen by your IDS, as it may take action to stop him. What tool might he use to bypass the IDS? Select the best answer.

A. Firewalk

B. Manhunt

C. Fragrouter

D. Fragids

Correct Answer: C

QUESTION 13

Joe the Hacker breaks into XYZ\\'s Linux system and plants a wiretap program in order to sniff passwords and user accounts off the wire. The wiretap program is embedded as a Trojan horse in one of the network utilities. Joe is worried that network administrator might detect the wiretap program by querying the interfaces to see if they are running in promiscuous mode.

Running "ifconfig –a" will produce the following:

```
# ifconfig –a

1o0: flags=848<UP, LOOPBACK, RUNNING, MULTICAST> mtu 8232
inet 127.0.0.1 netmask ff000000hme0:
flags=863<UP, BROADCAST, NOTRAILERS, RUNNING, PROMISC,
MULTICAST> mtu
1500
inet 192.0.2.99 netmask ffffff00 broadcast 134.5.2.255 ether
8:0:20:9c:a2:35
```

What can Joe do to hide the wiretap program from being detected by ifconfig command?

A. Block output to the console whenever the user runs ifconfig command by running screen capture utiliyu

B. Run the wiretap program in stealth mode from being detected by the ifconfig command.

C. Replace original ifconfig utility with the rootkit version of ifconfig hiding Promiscuous information being displayed on the console.

D. You cannot disable Promiscuous mode detection on Linux systems.

Correct Answer: C

QUESTION 14

What statement is true regarding LM hashes?

A. LM hashes consist in 48 hexadecimal characters.

B. LM hashes are based on AES128 cryptographic standard.

C. Uppercase characters in the password are converted to lowercase.

D. LM hashes are not generated when the password length exceeds 15 characters.

Correct Answer: D

QUESTION 15

Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?

A. Cross-site scripting

B. SQL injection

C. Missing patches

D. CRLF injection

Correct Answer: C