GCFA$^{\text{Q\&As}}$

GIAC Certified Forensics Analyst

Pass GIAC GCFA Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4itsure.com/gcfa.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by GIAC Official Exam Center

QUESTION 1

TCP FIN scanning is a type of stealth scanning through which the attacker sends a FIN packet to the target port. If the port is closed, the victim assumes that this packet was sent mistakenly by the attacker and sends the RST packet to the attacker. If the port is open, the FIN packet will be ignored and the port will drop the packet. Which of the following operating systems can be easily identified with the help of TCP FIN scanning?

A. Solaris

B. Red Hat

C. Knoppix

D. Windows

Correct Answer: D

QUESTION 2

Which of the following statements are true about Compact Disc (CD) and Digital Versatile Disk (DVD)? Each correct answer represents a complete solution. Choose all that apply.

A. CDs and DVDs are affected by EMP from nuclear detonations.

B. Data is encoded in the form of tiny pits on the surface of the CD and DVD.

C. CDs and DVDs are not affected by X-rays, and other sources of electromagnetic radiation.

D. It takes a small amount of energy to affect the data that written on CD and DVD.

Correct Answer: BD

QUESTION 3

Which of the following registry hives contains information about all users who have logged on to the system?

A. HKEY_CLASSES_ROOT

B. HKEY_CURRENT_USERS

C. HKEY_USERS

D. HKEY_CURRENT_CONFIG

Correct Answer: C

QUESTION 4

You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows or Cookie snooping attack. Which of the following logs will you review to accomplish the task?

Each correct answer represents a complete solution. Choose all that apply.

A. System logs

B. Event logs

C. Web server logs

D. Program logs

Correct Answer: ABD

QUESTION 5

Which of the following directories cannot be placed out of the root filesystem?

Each correct answer represents a complete solution. Choose all that apply.

A. /sbin

B. /etc

C. /var

D. /lib

Correct Answer: ABD

QUESTION 6

You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are creating a user account by using the USERADD command. Which of the following entries cannot be used for specifying a user ID?

Each correct answer represents a complete solution. Choose all that apply.

A. 0

B. 99

C. 100 D. -1

Correct Answer: ABD

QUESTION 7

Which of the following directories contains administrative commands on a UNIX computer?

A. /usr/local

B. /sbin

C. /bin

D. /export

Correct Answer: B

QUESTION 8

Which of the following is the process of overwriting all addressable locations on a disk?

A. Drive wiping

B. Spoofing

C. Sanitization

D. Authentication

Correct Answer: A

QUESTION 9

A firewall is a combination of hardware and software, used to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Which of the following tools works as a firewall for the Linux 2.4 kernel?

A. OpenSSH

B. IPTables

C. IPChains

D. Stunnel

Correct Answer: B

QUESTION 10

What is the name of the group of blocks which contains information used by the operating system in Linux system?

A. logblock

B. Systemblock

C. Bootblock

D. Superblock

Correct Answer: D

QUESTION 11

John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for personal reasons. He wants to send out some secret information of the company. To do so, he takes an image file and simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez, and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is unable to filter this mail. Which of the following techniques is he performing to accomplish his task?

A. Email spoofing

B. Social engineering

C. Steganography

D. Web ripping

Correct Answer: C

QUESTION 12

Which of the following Acts enacted in United States amends Civil Rights Act of 1964, providing technical changes affecting the length of time allowed to challenge unlawful seniority provisions, to sue the federal government for discrimination and to bring age discrimination claims?

A. Sexual Predators Act

B. Civil Rights Act of 1991

C. PROTECT Act

D. The USA Patriot Act of 2001

Correct Answer: B

QUESTION 13

Which of the following is a name, symbol, or slogan with which a product is identified?

A. Trade secret

B. Patent

C. Copyright

D. Trademark

Correct Answer: D

QUESTION 14

Which of the following tools works by using standard set of MS-DOS commands and can create an MD5 hash of an entire drive, partition, or selected files?

A. DriveSpy

B. Ontrack

C. Forensic Sorter

D. Device Seizure

Correct Answer: A

QUESTION 15

The incident response team has turned the evidence over to the forensic team. Now, it is the time to begin looking for the ways to improve the incident response process for next time. What are the typical areas for improvement? Each correct answer represents a complete solution. Choose all that apply.

A. Information dissemination policy

B. Additional personnel security controls

C. Incident response plan

D. Electronic monitoring statement

Correct Answer: ABCD