GCFA Q&As

GIAC Certified Forensics Analyst

Pass GIAC GCFA Exam with 100% Guarantee

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

QUESTION 1

Which of the following are the primary goals of the incident handling team?

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

A. Prevent any further damage.

B. Freeze the scene.

C. Repair any damage caused by an incident.

D. Inform higher authorities.

Correct Answer: ABC

QUESTION 2

You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are working as a root user on the Linux operating system. While performing some security investigation, you want to see the hostname and IP address from where users logged in.

Which of the following commands will you use to accomplish the task?

A. Dig

B. Netstat

C. Nslookup

D. Last

Correct Answer: D

QUESTION 3

Which of the following is used to store configuration settings and options on Microsoft Windows operating systems?

A. Windows Config file

B. Group policy editor

C. Windows setting

D. Windows Registry

Correct Answer: D

QUESTION 4

Which of the following statements are NOT true about volume boot record or Master Boot Record? Each correct answer represents a complete solution. Choose all that apply.

A. The end of MBR marker is h55CC.

B. The actual program can be 512 bytes long.

C. Volume boot sector is present at cylinder 0, head 0, and sector 1 of the default boot drive.

D. Four 16 bytes master partition records are present in MBR.

Correct Answer: AB

QUESTION 5

You are the Security Consultant working with a client who uses a lot of outdated systems. Many of their clients PC\\'s still have Windows 98. You are concerned about the security of passwords on a Windows 98 machine. What algorithm is used in Windows 98 to hash passwords?

A. DES

B. SHA

C. LANMAN

D. MD5

Correct Answer: C

QUESTION 6

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 7

Which of the following statements about the NTDETECT.COM file is true? Each correct answer represents a complete solution. Choose three.

A. It is used to gather information about currently installed hardware on the computer.

B. It is a startup file of the Windows NT/2000 operating system.

C. It is located in the root of the startup disk.

D. It is used to dual-boot a computer.

Correct Answer: ABC

QUESTION 8

Which of the following registry hives stores information about the file extensions that are mapped to their corresponding applications?

A. HKEY_CURRENT_USER

B. HKEY_USERS

C. HKEY_CLASSES_ROOT

D. HKEY_LOCAL_MACHINE

Correct Answer: C

QUESTION 9

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a multimedia enabled mobile phone, which is suspected to be used in a cyber crime. Adam uses a tool, with the help of which he can recover deleted text messages, photos, and call logs of the mobile phone. Which of the following tools is Adam using?

A. Galleta

B. FTK Imager

C. FAU

D. Device Seizure

Correct Answer: D

QUESTION 10

Which of the following is used to back up forensic evidences or data folders from the network or locally attached hard disk drives?

A. WinHex

B. Device Seizure

C. FAR system

D. Vedit

Correct Answer: C

QUESTION 11

You work as a Network Administrator for Tech Perfect Inc. The company has a Linux-based network. Users complain that they are unable to access resources on the network. However, there was no such problem the previous day. They are receiving the following error messages regularly:

Unable to resolve host name

As your primary step for resolving the issue, which of the following services will you verify whether it is running or not?

A. APACHE

B. BIND

C. SAMBA

D. SQUID

Correct Answer: B

QUESTION 12

Adam works as a professional Penetration tester. A project has been assigned to him to employ penetration testing on the network of Umbrella Inc. He is running the test from home and had downloaded every security scanner from the

Internet. Despite knowing the IP range of all of the systems, and the exact network configuration, Adam is unable to get any useful results.

Which of the following is the most like cause of this problem?

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

A. Security scanners are only as smart as their database and cannot find unpublished vulnerabilities.

B. Security scanners cannot perform vulnerability linkage.

C. Security scanners are smart as their database and can find unpublished vulnerabilities.

D. Security scanners are not designed to do testing through a firewall.

Correct Answer: ABD

QUESTION 13

You work as a Network Administrator for NetTech Inc. The company\\'s network is connected to the Internet. For security, you want to restrict unauthorized access to the network with minimum administrative effort. You want to implement a hardware-based solution. What will you do to accomplish this?

A. Connect a brouter to the network.

B. Implement firewall on the network.

C. Connect a router to the network.

D. Implement a proxy server on the network.

Correct Answer: B

QUESTION 14

Which of the following is used to detect the bad sectors in a hard disk under Linux environment?

A. Badblocks

B. CheckDisk

C. ScanDisk

D. CHKDSK

Correct Answer: A

QUESTION 15

Which of the following modules of OS X kernel (XNU) provides the primary system program interface?

A. BSD

B. LIBKERN

C. I/O Toolkit

D. Mach

Correct Answer: A