Demo Questions

GIAC GCFA Exam

GIAC Certified Forensic Analyst

Thank you for downloading GCFA Exam PDF

Question #1 *Topic 1*

Adam, a malicious hacker has successfully gained unauthorized access to the Linux system of Umbrella Inc. Web server of the company runs on Apache. He has downloaded sensitive documents and database files from the computer. After performing these malicious tasks, Adam finally runs the following command on the Linux command box before disconnecting. for ((i = 0;i<11;i++)); do dd if=/dev/random of=/dev/hda && dd if=/dev/zero of=/dev/hda done Which of the following actions does Adam want to perform by the above command?

- A. Making a bit stream copy of the entire hard disk for later download.
- B. Deleting all log files present on the system.
- C. Wiping the contents of the hard disk with zeros.
- D. Infecting the hard disk with polymorphic virus strings.

Correct Answer: *C*

Question #2*Topic 1*

Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company

does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?

- A. Trademark law
- B. Cyber law
- C. Copyright law
- D. Espionage law

Correct Answer: *A*

Question #3*Topic 1*

You work as a Network Administrator for Perfect Solutions Inc. You install Windows 98 on a computer. By default, which of the following folders does Windows 98 setup use to keep the registry tools?

- A. $SYSTEMROOT$REGISTRY
- B. $SYSTEMROOT$WINDOWS
- C. $SYSTEMROOT$WINDOWSREGISTRY
- D. $SYSTEMROOT$WINDOWSSYSTEM32

Correct Answer: *B*

Question #4*Topic 1*

Which of the following tools can be used to perform tasks such as Windows password cracking, Windows enumeration, and VoIP session sniffing?

- A. John the Ripper
- B. L0phtcrack
- C. Obiwan
- D. Cain

Correct Answer: *D*

Question #5*Topic 1*

Which of the following type of file systems is not supported by Linux kernel?

- A. vFAT
- B. NTFS
- C. HFS
- D. FAT32

Correct Answer: *D*

Question #6*Topic 1*

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*

Question #7*Topic 1*

You work as a Network Administrator for Blue Bell Inc. You want to install Windows XP Professional on your computer, which already has Windows Me installed.

You want to configure your computer to dual boot between Windows Me and Windows XP Professional. You have a single 40GB hard disk.

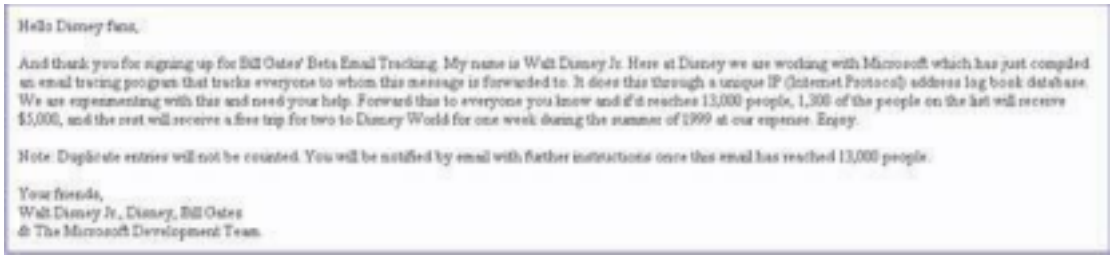
Which of the following file systems will you choose to dual-boot between the two operating systems?

- A. NTFS
- B. FAT32
- C. CDFS
- D. FAT

Correct Answer: *B*

Question #8*Topic 1*

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He receives the following e- mail:



Hello Disney fans,

And thank you for signing up for Bill Gates' Beta Email Tracking. My name is Walt Disney Jr. Here at Disney we are working with Microsoft which has just compiled an email tracing program that tracks everyone to whom this message is forwarded to. It does this through a unique IP (Internet Protocol) address log book database. We are experimenting with this and need your help. Forward this to everyone you know and if it reaches 13,000 people, 1,300 of the people on the list will receive $5,000, and the rest will receive a free trip for two to Disney World for one week during the summer of 1999 at our expense. Enjoy.

Note: Duplicate entries will not be counted. You will be notified by email with further instructions once this email has reached 13,000 people.

Your friends,
Walt Disney Jr., Disney, Bill Gates
& The Microsoft Development Team

The e-mail that John has received is an example of _____.

- A. Virus hoaxes
- B. Spambots
- C. Social engineering attacks
- D. Chain letters

Correct Answer: *D*