

GIAC

Exam GCFA

GIAC Certified Forensics Analyst

Version: 6.0

[Total Questions: 318]

Topic 1, Volume A**Question No : 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.

Answer: C

Question No : 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

Answer: A

Question No : 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

Answer: B

Question No : 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

Answer: D

Question No : 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

Answer: D

Question No : 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

Answer: A

Question No : 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

Answer: B

Question No : 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 tracking 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

Answer: D

Question No : 9 - (Topic 1)

Which of the following Acts enacted in United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?

- A. Wiretap Act
- B. Computer Fraud and Abuse Act
- C. Economic Espionage Act of 1996
- D. Electronic Communications Privacy Act of 1986

Answer: D

Question No : 10 - (Topic 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

Answer: D

Question No : 11 - (Topic 1)

Which of the following encryption methods uses AES technology?

- A. Dynamic WEP
- B. Static WEP
- C. TKIP
- D. CCMP

Answer: D

Question No : 12 - (Topic 1)

Mark works as a security manager for SofTech Inc. He is using a technique for monitoring what the employees are doing with corporate resources. Which of the following techniques is being used by Mark to gather evidence of an ongoing computer crime if a member of the staff is e-mailing company's secrets to an opponent?

- A. Electronic surveillance
- B. Civil investigation
- C. Physical surveillance
- D. Criminal investigation

Answer: A

Question No : 13 - (Topic 1)

Which of the following is the first computer virus that was used to infect the boot sector of storage media formatted with the DOS File Allocation Table (FAT) file system?

- A. Melissa
- B. Tequila
- C. Brain
- D. I love you

Answer: C

Question No : 14 - (Topic 1)

Which of the following attacks saturates network resources and disrupts services to a specific computer?

- A. Teardrop attack
- B. Polymorphic shell code attack
- C. Denial-of-Service (DoS) attack
- D. Replay attack

Answer: C

Question No : 15 - (Topic 1)

Peter works as a Technical Representative in a CSIRT for SecureEnet Inc. His team is called to investigate the computer of an employee, who is suspected for classified data theft. Suspect's computer runs on Windows operating system. Peter wants to collect data and evidences for further analysis. He knows that in Windows operating system, the data is searched in pre-defined steps for proper and efficient analysis. Which of the following is the correct order for searching data on a Windows based system?

- A. Volatile data, file slack, registry, memory dumps, file system, system state backup, internet traces
- B. Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps
- C. Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system
- D. Volatile data, file slack, file system, registry, memory dumps, system state backup, internet traces

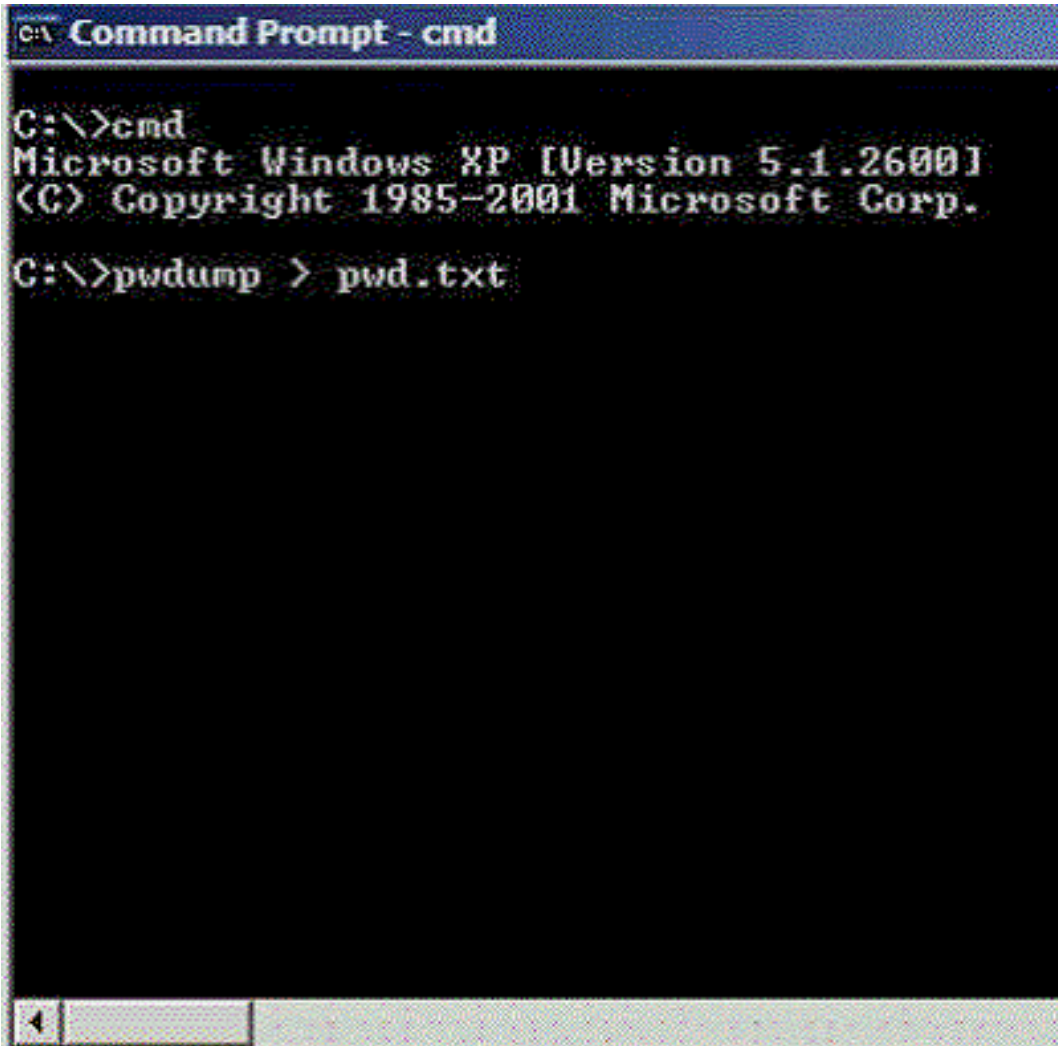
Answer: D

Question No : 16 - (Topic 1)

Adam works as a Security Administrator for Umbrella Inc. He is responsible for securing all 15 servers of the company. To successfully accomplish the task, he enables the hardware and software firewalls and disables all unnecessary services on all the servers. Sales manager of the company asks Adam to run emulation software on one of the servers that requires the telnet service to function properly. Adam is concerned about the security of the server, as telnet can be a very large security risk in an organization. Adam decides to perform some footprinting, scanning, and penetration testing on the server to checkon the server to check the security. Adam telnets into the server and writes the following command:

```
HEAD / HTTP/1.0
```

After pressing enter twice, Adam gets the following results:



```
C:\ Command Prompt - cmd

C:\>cmd
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>pwdump > pwd.txt
```

Which of the following tasks has Adam just accomplished?

- A. Poisoned the local DNS cache of the server.
- B. Submitted a remote command to crash the server.
- C. Grabbed the banner.
- D. Downloaded a file to his local computer.

Answer: C

Question No : 17 - (Topic 1)

The MBR of a hard disk is a collection of boot records that contain disk information such as disk architecture, cluster size, and so on. The main work of the MBR is to locate and run necessary operating system files that are required to run a hard disk. In the context of the operating system, MBR is also known as the boot loader. Which of the following viruses

can infect the MBR of a hard disk?

Each correct answer represents a complete solution. Choose two.

- A. Stealth
- B. Boot sector
- C. Multipartite
- D. File

Answer: B,C

Question No : 18 - (Topic 1)

You work as a professional Computer Hacking Forensic Investigator for DataEnet Inc. You want to investigate e-mail information of an employee of the company. The suspected employee is using an online e-mail system such as Hotmail or Yahoo. Which of the following folders on the local computer will you review to accomplish the task?

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

- A. History folder
- B. Temporary Internet Folder
- C. Download folder
- D. Cookies folder

Answer: A,B,D

Question No : 19 - (Topic 1)

Which of the following methods is used by forensic investigators to acquire an image over the network in a secure manner?

- A. DOS boot disk
- B. Linux Live CD
- C. Secure Authentication for EnCase (SAFE)
- D. EnCase with a hardware write blocker

Answer: C

Question No : 20 - (Topic 1)

You company suspects an employee of sending unauthorized emails to competitors. These emails are alleged to contain confidential company data. Which of the following is the most important step for you to take in preserving the chain of custody?

- A. Preserve the email server including all logs.
- B. Make copies of that employee's email.
- C. Seize the employee's PC.
- D. Place spyware on the employee's PC to confirm these activities.

Answer: A

Question No : 21 - (Topic 1)

Which of the following is the correct order of loading system files into the main memory of the system, when the computer is running on Microsoft's Windows XP operating system?

- A. NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe
- B. NTLDR, BOOT.ini, NTDETECT.com, HAL.dll, NTOSKRNL.exe
- C. NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe
- D. BOOT.ini, HAL.dll, NTDETECT.com, NTLDR, NTOSKRNL.exe

Answer: B

Question No : 22 - (Topic 1)

Fill in the blank with the appropriate name.

_____ is a list, which specifies the order of volatility of data in a Windows based system.

- A. RFC 3227

Answer: A

Question No : 23 - (Topic 1)