GIAC

Exam GCFA

GIAC Certified Forensics Analyst

Version: 6.0

[Total Questions: 318]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	98
Topic 2: Volume B	97
Topic 3: Volume C	123

Topic 1, Volume A

Question No : 1 - (Topic 1)

Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution. Which of the following data should be recorded in this documentation?

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

A. Names of the victims
B. Date and time of incident
C. Nature of harassment
D. Location of each incident

Answer: A,B,D

Question No : 2 - (Topic 1)

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.

Answer: A,B

Question No : 3 - (Topic 1)

You want to upgrade a partition in your computer's hard disk drive from FAT to NTFS. Which of the following DOS commands will you use to accomplish this?

A. FORMAT C: /s
B. CONVERT C: /fs:ntfs
C. SYS C:
D. FDISK /mbr

Answer: B

Question No : 4 - (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 : 5 - (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 : 6 - (Topic 1)

You are working with a team that will be bringing in new computers to a sales department at a company. The sales team would like to keep not only their old files, but system settings as well on the new PC's. What should you do?

A. Use the Disk Management tool to move everything to the new computer.
B. Copy the files and the Windows Registry to a removable media then copy it onto the new machines.
C. Do a system backup (complete) on each old machine, then restore it onto the new machines
D. Use the User State Migration tool to move the system settings and files to the new machines.

Answer: D

Question No : 7 - (Topic 1)

You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to fix partitions on a hard drive. Which of the following Unix commands can you use to accomplish the task?

A. fdformat
B. exportfs
C. fsck
D. fdisk

Answer: D

Question No : 8 - (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 : 9 - (Topic 1)

Which of the following is a type of intruder detection that involves logging network events to

a file for an administrator to review later?

A. Packet detection
B. Passive detection
C. Active detection
D. Event detection

Answer: B

Question No : 10 - (Topic 1)

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate the BlackBerry, which is suspected to be used to hide some important information. Which of the following is the first step taken to preserve the information in forensic investigation of the BlackBerry?

A. Keep BlackBerry in 'ON' state.
B. Remove the storage media.
C. Eliminate the ability of the device to receive the push data.
D. Turn off the BlackBerry.

Answer: C

Question No : 11 - (Topic 1)

You are reviewing a Service Level Agreement between your company and a Web development vendor.

Which of the following are security requirements you should look for in this SLA?

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

A. Time to respond to bug reports
B. Encryption standards
C. Security Monitoring
D. Guarantees on known security flaws

Answer: A,B,C,D

Question No : 12 - (Topic 1)

Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?

A. Confidentiality
B. Authentication
C. Non-repudiation
D. Integrity

Answer: C

Question No : 13 - (Topic 1)

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

Answer: A,B,D

Question No : 14 - (Topic 1)

John works for an Internet Service Provider (ISP) in the United States. He discovered child

pornography material on a Web site hosted by the ISP. John immediately informed law enforcement authorities about this issue. Under which of the following Acts is John bound to take such an action?

A. Civil Rights Act of 1991
B. PROTECT Act
C. Civil Rights Act of 1964
D. Sexual Predators Act

Answer: D

Question No : 15 - (Topic 1)

Adam works as a professional Computer Hacking Forensic Investigator with the local police of his area. A project has been assigned to him to investigate a PDA seized from a local drug dealer. It is expected that many valuable and important information are stored in this PDA. Adam follows investigative methods, which are required to perform in a pre-defined sequential manner for the successful forensic investigation of the PDA. Which of the following is the correct order to perform forensic investigation of PDA?

A. Identification, Collection, Examination, Documentation
B. Examination, Collection, Identification, Documentation
C. Documentation, Examination, Identification, Collection
D. Examination, Identification, Collection, Documentation

Answer: D

Question No : 16 - (Topic 1)

Normally, RAM is used for temporary storage of data. But sometimes RAM data is stored in the hard disk, what is this method called?

A. Cache memory
B. Static memory
C. Virtual memory
D. Volatile memory

Answer: C

Question No : 17 - (Topic 1)

Which of the following file systems contains hardware settings of a Linux computer?

A. /var
B. /etc
C. /proc

D. /home

Answer: C

Question No : 18 - (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 : 19 - (Topic 1)

Adam works as an Incident Handler for Umbrella Inc. He is informed by the senior authorities that the server of the marketing department has been affected by a malicious hacking attack. Supervisors are also claiming that some sensitive data are also stolen. Adam immediately arrived to the server room of the marketing department and identified the event as an incident. He isolated the infected network from the remaining part of the network and started preparing to image the entire system. He captures volatile data, such as running process, ram, and network connections.

Which of the following steps of the incident handling process is being performed by Adam?

A. Recovery
B. Eradication
C. Identification
D. Containment

Answer: D

Question No : 20 - (Topic 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.

Answer: A,B,C

Question No : 21 - (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 : 22 - (Topic 1)

You work as a Web developer for ABC Inc. You want to investigate the Cross-Site Scripting attack on your company's Web site. Which of the following methods of investigation can you use to accomplish the task?

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

A. Review the source of any HTML-formatted e-mail messages for embedded scripts or links in the URL to the company's site.
B. Look at the Web server's logs and normal traffic logging.
C. Use Wireshark to capture traffic going to the server and then searching for the requests going to the input page, which may give log of the malicious traffic and the IP address of the source.
D. Use a Web proxy to view the Web server transactions in real time and investigate any communication with outside servers.

Answer: A,B,D

Question No : 23 - (Topic 1)

Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

A. Snooping
B. Copyright
C. Utility model
D. Patent

Answer: D

Question No : 24 - (Topic 1)

You work as the Network Administrator for McNeil Inc. The company has a Unix-based network. You want to allow direct access to the filesystems data structure. Which of the following Unix commands can you use to accomplish the task?

A. du
B. debugfs
C. df
D. dosfsck

Answer: B

Question No : 25 - (Topic 1)

You are the Network Administrator and your company has recently implemented encryption for all emails. You want to check to make sure that the email packages are being encrypted. What tool would you use to accomplish this?

A. Password cracker
B. Packet sniffer
C. Performance Monitor
D. Vulnerability analyzer

Answer: B

Question No : 26 - (Topic 1)

Sandra, a novice computer user, works on Windows environment. She experiences some problem regarding bad sectors formed in a hard disk of her computer. She wants to run CHKDSK command to check the hard disk for bad sectors and to fix the errors, if any, occurred. Which of the following switches will she use with CHKDSK command to accomplish the task?

A. CHKDSK /I
B. CHKDSK /C /L
C. CHKDSK /V /X
D. CHKDSK /R /F

Answer: D

Question No : 27 - (Topic 1)

You are handling technical support calls for an insurance company. A user calls you complaining that he cannot open a file, and that the file name appears in green while opening in Windows Explorer.

What does this mean?

A. The file is encrypted.
B. The file belongs to another user.
C. The file is infected with virus.
D. The file is compressed.

Answer: A

Question No : 28 - (Topic 1)

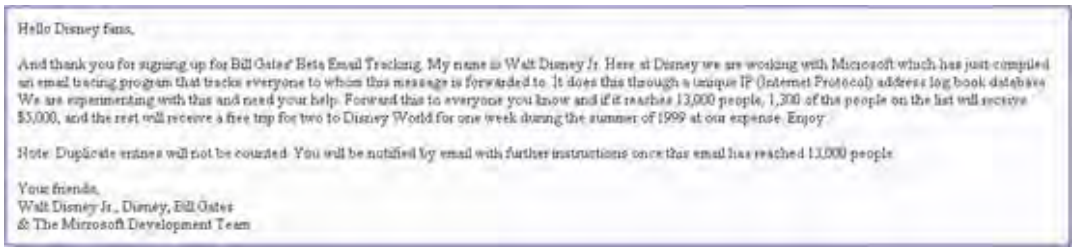
An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

A. Network security policy
B. User password policy
C. Privacy policy
D. Backup policy

Answer: C

Question No : 29 - (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 the 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 : 30 - (Topic 1)

Which of the following types of evidence proves or disproves a specific act through oral testimony based on information gathered through the witness's five senses?

A. Conclusive evidence
B. Best evidence
C. Hearsay evidence
D. Direct evidence

Answer: D

Question No : 31 - (Topic 1)

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate the main server of SecureEnet Inc. The server runs on Debian Linux operating system. Adam wants to investigate and review the GRUB configuration file of the server system.

Which of the following files will Adam investigate to accomplish the task?

A. /boot/grub/menu.lst
B. /boot/grub/grub.conf
C. /boot/boot.conf
D. /grub/grub.com

Answer: A

Question No : 32 - (Topic 1)

Adam works as a professional Computer Hacking Forensic Investigator. He has been assigned with the project of investigating an iPod, which is suspected to contain some explicit material. Adam wants to connect the compromised iPod to his system, which is running on Windows XP (SP2) operating system. He doubts that connecting the iPod with his computer may change some evidences and settings in the iPod. He wants to set the iPod to read-only mode. This can be done by changing the registry key within the Windows XP (SP2) operating system. Which of the following registry keys will Adam change to accomplish the task?

A. HKEY_LOCAL_MACHINE\System\CurrentControlset\Control\StorageDevicePolicies
B. HKEY_LOCAL_MACHINE\CurrentControlset\Control\StorageDevicePolicies
C. HKEY_LOCAL_MACHINE\System\CurrentControlset\StorageDevicePolicies
D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion

Answer: A

Question No : 33 - (Topic 1)

Which of the following file systems supports the hot fixing feature?

A. FAT16

B. exFAT
C. FAT32
D. NTFS

Answer: D

Question No : 34 - (Topic 1)

Which of the following two cryptography methods are used by NTFS Encrypting File System (EFS) to encrypt the data stored on a disk on a file-by-file basis?

A. Digital certificates
B. Public key
C. RSA
D. Twofish

Answer: A,B

Question No : 35 - (Topic 1)

Which of the following switches of the XCOPY command copies attributes while copying files?

A. /o
B. /p
C. /k
D. /s

Answer: D

Question No : 36 - (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