

Module Name-1 : (60 Minutes)

- Q1. If you come across a sheepdip machine at your client site , what would you infer ?  
a) A sheepdip coordinates several honeypots  
b) A sheepdip computer is another name for a honeypot  
c) A sheepdip computer is used only for virus-checking.  
d) A sheepdip computer defers a denial of service attack
- Q2. In a computer forensics investigation , what describes the route that evidence takes from the time you find it until the case is closed or goes to court?  
a) Rules of evidence  
b) Law of probability  
c) Chain of custody  
d) Policy of separation
- Q3. How many characters long is the fixed length MD5 algorithm checksum of a critical system file?  
a) 128  
b) 64  
c) 32  
d) 16
- Q4. Before you are called to testify as an expert , what must an attorney do first?  
a) Engage in damage control  
b) Prove that the tools you used to conduct your examination are perfect  
c) Read your curriculum vitae to the jury  
d) Qualify you as an expert witness
- Q5. You are contracted to work as a computer forensics investigator for a regional bank that four 30TB storage area networks that store customer data. What method would be most efficient for you to acquire digital evidence from this network?  
a) Create a compressed copy of the file with DoubleSpace  
b) Create a sparse data copy of a folder or file  
c) Make a bit-stream disk-to-image file  
d) Make a bit-stream disk-to-disk file
- Q6. What file structure database would you expect to find on floppy disks?  
a) NTFS  
b) FAT32  
c) FAT16  
d) FAT12
- Q7. What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?  
a) Digital Attack  
b) Denial of Service  
c) Physical Attack  
d) ARP redirect
- Q8. When examining a file with a Hex Editor , what space does the file header occupy?  
a) The last several bytes of the file  
b) The first several bytes of the file  
c) None, file headers are contained in the FAT
- Q9. In the context of file deletion process , which of the following statement holds true?  
a) When files are deleted, the data is overwritten and the cluster marked as available  
b) The longer a disk is in use, the less likely it is that deleted files will be overwritten  
c) While booting, the machine may create temporary files that can delete evidence  
d) Secure delete programs work by completely overwriting the file in one go
- Q10. A suspect is accused of violating the acceptable use of computing resources , as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However , the suspect has cleared the search history and emptied the cookie cache . Moreover , he has removed any images he might have downloaded. What can the investigator do to prove the violation? Choose the most feasible option.  
a) Image the disk and try to recover deleted files  
b) Seek the help of co-workers who are eye-witnesses  
c) Check the Windows registry for connection data (You may or may not recover)  
d) Approach the websites for evidence
- Q11. A(n) \_\_\_\_\_ is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.  
a) Blackout Attack.  
b) Automated Attack  
c) Distributed Attack  
d) Central Processing Attack
- Q12. The offset in hexadecimal code is :  
a) The last byte after the colon  
b) The ox at the beginning of the code  
c) The ox at the end of the code  
d) The first byte after the colon
- Q13. It takes \_\_\_\_\_ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?  
a) by law, three  
b) quite a few  
c) only one  
d) atleast two
- Q14. With the standard Linux second extended file system (EXT2fs) , a file is deleted when the inode internal link count reaches \_\_\_\_\_  
a) 0  
b) 10  
c) 100  
d) 1
- Q15. An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are

\_\_\_\_\_ media used to store large amounts of data and are not affected by the magnet.

- a) logical
- b) anti-magnetic
- c) magnetic
- d) optical

Q16. What does the acronym POST mean as it relates to a PC?

- a) Primary Operations Short Test
- b) Power On Self Test
- c) Pre Operational Situation Test
- d) Primary Operating System Test

Q17. Which legal document allows a law enforcement to search an office , place of business , or other locale for evidence relating to an alleged crime?

- a) Bench warrant
- b) Wire Tap
- c) Subpoena
- d) Search warrant

Q18. You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager instructs you to complete one multi evidence form for the entire case and a single evidence form for each hard drive. How will these forms be stored to help preserve the chain of the custody case?

- a) All forms should be placed in an approved secure container because they are now primary evidence in the case
- b) The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.
- c) The multi-evidence form should be placed in an approved secure container with the hard drives and the single evidence
- d) All forms should be placed in the report file because they are now primary evidence in the case.

Q19. The MD5 program is used to :

- a) wipe magnetic media before recycling it
- b) make directories on a evidence disk
- c) view graphics files on an evidence drive
- d) verify that a disk is not altered when you examine it

Q20. Which is the standard procedure to perform during all computer forensics investigations?

- a) with the hard drive removed from the suspect PC, check the date and time in the system's CMOS
- b) with the hard drive in the suspect PC, check the date and time in the File Allocation Table
- c) with the hard drive removed from the suspect PC, check the date and time in the system's RAM

d) with the hard drive in the suspect PC, check the date and time in the system's CMOS

Q21. In a forensic examination of hard drives for digital evidence , what type of user is most likely to have the most file slack to analyze?

- a) one who has NTFS 4 or 5 partitions
- b) one who uses dynamic swap file capability
- c) one who uses hard disk writes on IRQ 13 and 21
- d) one who has lots of allocation units per block or cluster

Q22. You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case , you have followed every applicable procedure , however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?

- a) make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab
- b) make an MD5 hash of the evidence and compare it to the standard database developed by NIST
- c) there is no reason to worry about this possible claim because state labs are certified
- d) sign a statement attesting that the evidence is the same as it was when it entered the lab

Q23. When monitoring for both intrusion and security events between multiple computers , it is essential that the computer's clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple computers. Without synchronized time , it is very difficult to determine exactly when specific events took place and how events interlace. What is the name of the service used to synchronize time among multiple computers?

- a) Universal Time Set
- b) Network Time Protocol
- c) SyncTime Service
- d) Time-Sync Protocol

Q24. When investigating a potential e-mail crime , what is your first step in investigation?

- a) Trace the IP address to its origin
- b) Write a report
- c) Determine whether a crime was actually committed
- d) Recover the evidence

Q25. If a suspect computer is located in an area that may have toxic chemicals , you must:

- a) coordinate with the HAZMAT team
- b) determine a way to obtain the suspect computer
- c) assume the suspect machine is contaminated

- d) do not enter alone
- Q26. What happens when a file is deleted by a Microsoft operating system using the FAT file system?
- a) only the reference to the file is removed from the FAT
  - b) the file is erased and cannot be recovered
  - c) a copy of the file is stored and the original file is erased
  - d) the file is erased but can be recovered
- Q27. What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?
- a) rootkit
  - b) key escrow
  - c) steganography
  - d) offset
- Q28. During the course of an investigation , you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore you report this evidence. This type of evidence is known as :
- a) Inculpatory evidence
  - b) Mandatory evidence
  - c) Exculpatory evidence
  - d) Terrible evidence
- Q29. What binary coding is used most often for e-mail purpose?
- a) MIME
  - b) Uuencode
  - c) IMAP
  - d) SMTP
- Q30. What does the Superblock in Linux define?
- a) File synames
  - b) Disk geometr
  - c) Location of the first inode
  - d) Available space
- Q31. \_\_\_\_\_ identifies the trustees that are allowed or denied access to a securable object?
- a) SACL
  - b) DACL
  - c) TACL
  - d) UACL
- Q32. \_\_\_\_\_ enables administrators to log attempts to access a secured object.
- a) SACL
  - b) DACL
  - c) TACL
  - d) UACL
- Q33. The \_\_\_\_\_ setting is used to audit each event that is related to a user logging on to , logging off from , or making a network connection to the computer.
- a) Audit account logon events
  - b) Audit account management
  - c) Audit directory service access
  - d) Audit logon events
- Q34. On a linux machine , the \_\_\_\_\_ is responsible for writing audit records to the disk.
- a) log deamon
  - b) syslogd daemon
  - c) auditeddaemon
  - d) track daemon
- Q35. The \_\_\_\_\_ command is used to assist controlling the kernel's audit system.
- a) auditctl
  - b) ausearch
  - c) aureport
  - d) syslogd
- Q36. The \_\_\_\_\_ command is used to set a audit watch on a file.
- a) auditctl
  - b) ausearch
  - c) aureport
  - d) syslogd
- Q37. \_\_\_\_\_ is a linux command that can query the audit daemon logs based for events based on different search criteria.
- a) logsearch
  - b) ausearch
  - c) search
  - d) syslogd
- Q38. \_\_\_\_\_ is a linux tool that produces summary reports of the audit system logs.
- a) auditctl
  - b) ausearch
  - c) aureport
  - d) syslogd
- Q39. ETW stands for :
- a) Event Tracking for Windows
  - b) Event Tracing for Windows
  - c) Entry Tracking for Windows
  - d) Engress Tracking for Windows
- Q40. In Kerberos , TGT is the short for for :
- a) Token Granting Terminal
  - b) Token Granting Ticket
  - c) Ticket Granting Ticket
  - d) Ticket Granting Terminal

Module Name -2 (60 Minute)

- Q41. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q42. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q43. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q44. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q45. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q46. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q47. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q48. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q49. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q50. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q51. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q52. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q53. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q54. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q55. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q56. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q57. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q58. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q59. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q60. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q61. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)

- Q62. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q63. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q64. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q65. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q66. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q67. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q68. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q69. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q70. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q71. Nay new class you define when working

- with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q72. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q73. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q74. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q75. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q76. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q77. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q78. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q79. Nay new class you define when working with the Foundation framework should also
- a)
  - b)
  - c)
  - d)
- Q80. Nay new class you define when working with the Foundation framework should also

- a)
- b)
- c)
- d)