Online Examinations (Even Sem/Part-I/Part-II Examinations 2020 - 2021

Course Name - Digital Security and Forensic Fundamental
Course Code - MNCS403

* You can submit the form ONLY ONCE.
* Fill the following information for further process.

* Required

1. Email *

2. Name of the Student *

3. Enter Full Student Code *

4. Enter Roll No *

5. Enter Registration No *

6. Enter Course Code *

7.   Enter Course Name *

_____

8. *

Mark only one oval.

○ Diploma in Pharmacy

○ Bachelor of Pharmacy

○ B.TECH.(CSE)

○ B.TECH.(ECE)

○ BCA

○ B.SC.(CS)

○ B.SC.(BT)

○ B.SC.(ANCS)

○ B.SC.(HN)

○ B.Sc.(MM)

○ B.A.(MW)

○ BBA

○ B.COM

○ B.A.(JMC)

○ BBA(HM)

○ BBA(LLB)

○ B.OPTOMETRY

○ B.SC.(MB)

○ B.SC.(MLT)

○ B.SC.(MRIT)

○ B.SC.(PA)

○ LLB

○ B.SC(IT)-AI

○ B.SC.(MSJ)

○ Bachelor of Physiotherapy

○ B.SC.(AM)

○ Dip.CSE

○ Dip.ECE

○ DIP.EE

○ DIP.CE

◯ DIP.ME

◯ PGDHM

◯ MBA

◯ M.SC.(BT)

◯ M.TECH(CSE)

◯ LLM

◯ M.A.(JMC)

◯ M.A.(ENG)

◯ M.SC.(MATH)

◯ M.SC.(MB)

◯ MCA

◯ M.SC.(MSJ)

◯ M.SC.(AM)

◯ M.SC.CS)

◯ M.SC.(ANCS)

◯ M.SC.(MM)

◯ B.A.(Eng)

Answer all the questions. Each question carry one mark.

9. 1. You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?

Mark only one oval.

◯ Net sessions

◯ Net config

◯ Net share

◯ Net use

10.   2. Which of the following standard represents a legal precedent sent in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

Mark only one oval.

⬭ IOCE

⬭ SWGDE & SWGIT

⬭ Frye

⬭ Daubert

11.   3. Which network attack is described by the following statement?"At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."

Mark only one oval.

⬭ DDoS

⬭ Sniffer Attack

⬭ Buffer Overflow

⬭ Man-in-the-Middle Attack

12.   4. Which password cracking technique uses details such as length of password, character sets used to construct the password, etc.?

Mark only one oval.

⬭ Dictionary attack

⬭ Brute force attack

⬭ Rule-based attack

⬭ Man in the middle attack

13.   5. Which of the following techniques delete the files permanently?

Mark only one oval.

○ Trail obfuscation

○ Data Hiding

○ Steganography

○ Artifact Wiping

14.   6. What type of attack sends spoofed UDP packets (instead of ping packets) with a
       fake source address to the IP broadcast address of a large network?

Mark only one oval.

○ Fraggle

○ Smurf scan

○ SYN flood

○ Teardrop

15.   7. While presenting his case to the court, Simon calls many witnesses to the stand
       to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary
       is a lay witness, what field would she be considered an expert in?

Mark only one oval.

○ Technical material related to forensics

○ No particular field

○ Judging the character of defendants/victims

○ Legal issues

16.   8. Harold is finishing up a report on a case of network intrusion, corporate spying, and embezzlement that he has been working on for over six months. He is trying to find the right term to use in his report to describe network enabled spying. What term should Harold use?

Mark only one oval.

- Spycrack
- Spynet
- Netspionage
- Hackspionage

17.   9. Before performing a logical or physical search of a drive in Encase, what must be added to the program?

Mark only one oval.

- File signatures
- Keywords
- Hash sets
- Bookmarks

18.   10. Using Linux to carry out a forensics investigation, what would the following command accomplish? dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror

Mark only one oval.

- Search for disk errors within an image file
- Backup a disk to an image file
- Copy a partition to an image file
- Restore a disk from an image file

19. 11. Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company PBX system be called?

Mark only one oval.

◯ Phreaking

◯ Squatting

◯ Crunching

◯ Pretexting

20. 12. What is the first step taken in an investigation for laboratory forensic staff members?

Mark only one oval.

◯ Packaging the electronic evidence

◯ Securing and evaluating the electronic crime scene

◯ Conducting preliminary interviews

◯ Transporting the electronic evidence

21.　13. You have been called in to help with an investigation of an alleged network intrusion. After questioning the members of the company IT department, you search through the server log files to find any trace of the intrusion. After that you decide to telnet into one of the company routers to see if there is any evidence to be found. While connected to the router, you see some unusual activity and believe that the attackers are currently connected to that router. You start up an ethereal session to begin capturing traffic on the router that could be used in the investigation. At what layer of the OSI model are you monitoring while watching traffic to and from the router?

Mark only one oval.

◯ Network

◯ Transport

◯ Option 3

◯ Session

22.　14. A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

Mark only one oval.

◯ Blu-Ray single-layer

◯ HD-DVD

◯ Blu-Ray dual-layer

◯ DVD-18

23.   15. Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?

Mark only one oval.

○ IT personnel

○ Employees themselves

○ Supervisors

○ Administrative assistant in charge of writing policies

24.   16. John is working on his company policies and guidelines. The section he is currently working on covers company documents; how they should be handled, stored, and eventually destroyed. John is concerned about the process whereby outdated documents are destroyed. What type of shredder should John write in the guidelines to be used when destroying documents?

Mark only one oval.

○ Strip-cut shredder

○ Cross-cut shredder

○ Cross-hatch shredder

○ Cris-cross shredder

25.   17. John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf purportedly used as a botnet server. John thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. John decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce?

Mark only one oval.

○ It contains the times and dates of when the system was last patched

○ It is not necessary to scan the virtual memory of a computer

○ It contains the times and dates of all the system files

○ Hidden running processes

26.   18.Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the PCs found in the hackers hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?

Mark only one oval.

○ Place PDA, including all devices, in an antistatic bag

○ Unplug all connected devices

○ Power off all devices if currently on

○ Photograph and document the peripheral devices

27. 19. What type of attack sends SYN requests to a target system with spoofed IP addresses?

Mark only one oval.

○ SYN flood

○ Ping of death

○ Cross site scripting

○ Land

28. 20. What advantage does the tool Evidor have over the built-in Windows search?

Mark only one oval.

○ It can find deleted files even after they have been physically removed

○ It can find bad sectors on the hard drive

○ It can search slack space

○ It can find files hidden within ADS

29. 21. Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish?dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync

Mark only one oval.

○ Fill the disk with zeros

○ Low-level format

○ Fill the disk with 4096 zeros

○ Copy files from the master disk to the slave disk on the secondary IDE controller

30. 22. A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\\RECYCLED using a command line tool but does not find anything. What is the reason for this?

Mark only one oval.

○ He should search in C:\\Windows\\System32\\RECYCLED folder

○ The Recycle Bin does not exist on the hard drive

○ The files are hidden and he must use switch to view them

○ Only FAT system contains RECYCLED folder and not NTFS

31. 23. Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?

Mark only one oval.

○ Typography

○ Steganalysis

○ Picture encoding

○ Steganography

32. 24. Heather, a computer forensics investigator, is assisting a group of investigators working on a large computer fraud case involving over 20 people. These 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather responsibility is to find out how the accused people communicated between each other. She has searched their email and their computers and has not found any useful evidence. Heather then finds some possibly useful evidence under the desk of one of the accused. In an envelope she finds a piece of plastic with numerous holes cut out of it. Heather then finds the same exact piece of plastic with holes at many of the other accused peoples desks. Heather believes that the 20 people involved in the case were using a cipher to send secret messages in between each other. What type of cipher was used by the accused in this case?

Mark only one oval.

◯ Grill cipher

◯ Null cipher

◯ Text semagram

◯ Visual semagram

33. 25. Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryltakes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully. Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices. How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?

Mark only one oval.

◯ Two

◯ One

◯ Three

◯ Four

34.   26. An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

Mark only one oval.

⬭ Smurf

⬭ Ping of death

⬭ Fraggle

⬭ Nmap scan

35.   27. Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

Mark only one oval.

⬭ Computers on his wired network

⬭ Satellite television

⬭ 2.4Ghz Cordless phones

⬭ CB radio

36. 28. After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

Mark only one oval.

◯ RestrictAnonymous must be set to "10" for complete security

◯ RestrictAnonymous must be set to "3" for complete security

◯ RestrictAnonymous must be set to "2" for complete security

◯ There is no way to always prevent an anonymous null session from establishing

37. 29. After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts respond to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

Mark only one oval.

◯ Only IBM AS/400 will reply to this scan

◯ Only Windows systems will reply to this scan

◯ A switched network will not respond to packets sent to the broadcast address

◯ Only Unix and Unix-like systems will reply to this scan

38.   30. Julia is a senior security analyst for Berber Consulting group. She is currently
working on a contract for a small accounting firm in Florid a. They have given her
permission to perform social engineering attacks on the company to see if their in-
house training did any good. Julia calls the main number for the accounting firm
and talks to the receptionist. Julia says that she is an IT technician from the
company's main office in Iowa. She states that she needs the receptionist's
network username and password to troubleshoot a problem they are having. Julia
says that Bill Hammond, the CEO of the company, requested this information. After
hearing the name of the CEO, the receptionist gave Julia all the information she
asked for. What principal of social engineering did Julia use?

Mark only one oval.

◯ Social Validation

◯ Scarcity

◯ Friendship/Liking

◯ Reciprocation

39.   31. You are the security analyst working for a private company out of France. Your
current assignment is to obtain credit card information from a Swiss bank owned
by that company. After initial reconnaissance, you discover that the bank security
defenses are very strong and would take too long to penetrate. You decide to get
the information by monitoring the traffic between the bank and one of its
subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP
packets traveling back and forth. You want to sniff the traffic and extract
usernames and passwords. What tool could you use to get this information?

Mark only one oval.

◯ Airsnort

◯ Snort

◯ Ettercap

◯ RaidSniff

40.   32. You are running known exploits against your network to test for possible
       vulnerabilities. To test the strength of your virus software, you load a test network
       to mimic your production network. Your software successfully blocks some simple
       macro and encrypted viruses. You decide to really test the software by using virus
       code where the code rewrites itself entirely and the signatures change from child
       to child, but the functionality stays the same. What type of virus is this that you are
       testing?

       Mark only one oval.

       ( ) Polymorphic

       ( ) Metamorphic

       ( ) Oligomorhic

       ( ) Transmorphic

41.   33. Harold is a web designer who has completed a website for ghttech.net. As part
       of the maintenance agreement he signed with the client, Harold is performing
       research online and seeing how much exposure the site has received so far. Harold
       navigates to google.com and types in the following search. link:www.ghttech.net
       What will this search produce?

       Mark only one oval.

       ( ) All sites that ghttech.net links to

       ( ) All sites that link to ghttech.net

       ( ) All search engines that link to .net domains

       ( ) Sites that contain the code: link:www.ghttech.net

42. 34. You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

Mark only one oval.

◯ Poison the DNS records with false records

◯ Enumerate MX and A records from DNS

◯ Establish a remote connection to the Domain Controller

◯ Enumerate domain user accounts and built-in groups

43. 35. Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

Mark only one oval.

◯ Tailgating

◯ Backtrapping

◯ Man trap attack

◯ Fuzzing

44. 36. Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test. The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

Mark only one oval.

◯ False negatives

◯ False positives

◯ True negatives

◯ True positives

45. 37. Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

Mark only one oval.

◯ APIPA

◯ IANA

◯ CVE

◯ RIPE

46.　38. After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

Mark only one oval.

◯ Enable direct broadcasts

◯ Disable direct broadcasts

◯ Disable BGP

◯ Enable BGP

47.　39. George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time–based induction machine" be used. What IDS feature must George implement to meet this requirement?

Mark only one oval.

◯ Signature-based anomaly detection

◯ Pattern matching

◯ Real-time anomaly detection

◯ Statistical-based anomaly detection

48.   40. Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers.Bill protects the PDF documents with a password and sends them to their intended recipients.Why PDF passwords do not offer maximum protection?

Mark only one oval.

○ PDF passwords can easily be cracked by software brute force tools

○ PDF passwords are converted to clear text when sent through E-mail

○ PDF passwords are not considered safe by Sarbanes-Oxley

○ When sent through E-mail, PDF passwords are stripped from the document completely

49.   41. You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so Quickly?

Mark only one oval.

○ Passwords of 14 characters or less are broken up into two 7-character hashes

○ A password Group Policy change takes at least 3 weeks to completely replicate throughout a network

○ Networks using Active Directory never use SAM databases so the SAM database pulled was empty

○ The passwords that were cracked are local accounts on the Domain Controller

50.   42. You work as an IT security auditor hired by a law firm in Boston to test whether
       you can gain access to sensitive information about the company clients. You have
       rummaged through their trash and found very little information. You do not want to
       set off any alarms on their network, so you plan on performing passive foot
       printing against their Web servers. What tool should you use?

Mark only one oval.

   ⬭ Ping sweep

   ⬭ Nmap
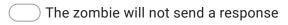
   ⬭ Netcraft

   ⬭ Dig

51.   43. You are assisting a Department of Defense contract company to become
       compliant with the stringent security policies set by the DoD. One such strict rule
       is that firewalls must only allow incoming connections that were first initiated by
       internal computers. What type of firewall must you implement to abide by this
       policy?

Mark only one oval.

   ⬭ Packet filtering firewall

   ⬭ Circuit-level proxy firewall

   ⬭ Application-level proxy firewall

   ⬭ Stateful firewall

52.   44. If an attacker's computer sends an IPID of 31400 to a zombie computer on an
       open port in IDLE scanning, what will be the response?

Mark only one oval.

   ⬭ The zombie will not send a response

   ⬭ 31402

   ⬭ 31399

   ⬭ 31401

53.   45. What will the following command produce on a website login page? SELECT
      email, passwd, login_id, full_name FROM members WHERE email =
      'someone@somehwere.com'; DROP TABLE members; –'

Mark only one oval.

⬭ Deletes the entire members table

⬭ Inserts the Error! Reference source not found.email address into the members table

⬭ Retrieves the password for the first user in the members table

⬭ This command will not produce anything since the syntax is incorrect

54.   46. When you are running a vulnerability scan on a network and the IDS cuts off
      your connection, what type of IDS is being used?

Mark only one oval.

⬭ Passive IDS

⬭ Active IDS

⬭ Progressive IDS

⬭ NIPS

55.   47. You are assisting in the investigation of a possible Web Server Hack. The
        company who called you stated that customers reported to them that whenever
        they entered the web address of the company in their browser, what they received
        was a porno graphic web site. The company checked the web server and nothing
        appears wrong. When you type in the IP address of the web site in your browser
        everything appears normal. What is the name of the attack that affects the DNS
        cache of the name resolution servers, resulting in those servers directing users to
        the wrong web site?

        Mark only one oval.

        ◯ ARP Poisoning

        ◯ DNS Poisoning

        ◯ HTTP redirect attack

        ◯ IP Spoofing

56.   48. As a CHFI professional, which of the following is the most important to your
        professional reputation?

        Mark only one oval.

        ◯ Your Certifications

        ◯ The correct, successful management of each and every case

        ◯ The free that you charge

        ◯ The friendship of local law enforcement officers

57.   49. When cataloging digital evidence, the primary goal is to?

        Mark only one oval.

        ◯ Make bit-stream images of all hard drive

        ◯ Preserve evidence integrity

        ◯ Not remove the evidence from the scene

        ◯ Not allow the computer to be turned off

58. 50. You are working as a Computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject's computer. You inform the officer that you will not be able to comply with that request because doing so would:

Mark only one oval.

○ Violate your contract

○ Cause network congestion

○ Make you an agent of law enforcement

○ Write information to the subject's hard drive

59. 51. What is the target host IP in the following command? c:\>firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP

Mark only one oval.

○ 172.16.28.95

○ 10.10.150.1

○ Firewalk does not scan target hosts

○ This command is using FIN packets, which cannot scan target hosts

60.   52. Law enforcement officers are conducting a legal search for which a valid
      warrant was obtained.While conducting the search, officers observe an item of
      evidence for an unrelated crime that was not included in the warrant. The item was
      clearly visible to the officers and immediately identified as evidence.What is the
      term used to describe how this evidence is admissible?

      Mark only one oval.

      ⬭ Plain view doctrine

      ⬭ Corpus delicti

      ⬭ Locard Exchange Principle

      ⬭ Ex Parte Order

61.   53. Chris has been called upon to investigate a hacking incident reported by one of
      his clients. The company suspects the involvement of an insider accomplice in the
      attack. Upon reaching the incident scene, Chris secures the physical area, records
      the scene using visual media. He shuts the system down by pulling the power plug
      so that he does not disturb the system in any way. He labels all cables and
      connectors prior to disconnecting any. What do you think would be the next
      sequence of events?

      Mark only one oval.

      ⬭ Connect the target media; prepare the system for acquisition; Secure the evidence;
      Copy the media

      ⬭ Prepare the system for acquisition; Connect the target media; copy the media; Secure
      the evidence

      ⬭ Connect the target media; Prepare the system for acquisition; Secure the evidence;
      Copy the media

      ⬭ Secure the evidence; prepare the system for acquisition; Connect the target media;
      copy the media

62.   54. When investigating a Windows System, it is important to view the contents of
       the page or swap file because of which of the following reason?

       Mark only one oval.

          ⬭ Windows stores all of the systems configuration information in this file

          ⬭ This is file that windows use to communicate directly with Registry

          ⬭ A Large volume of data can exist within the swap file of which the computer user has
          no knowledge

          ⬭ This is the file that windows use to store the history of the last 100 commands that
          were run from the command line

63.   55. When you carve an image, recovering the image depends on which of the
       following skills?

       Mark only one oval.

          ⬭ Recognizing the pattern of the header content

          ⬭ Recovering the image from a tape backup

          ⬭ Recognizing the pattern of a corrupt file

          ⬭ Recovering the image from the tape backup

64.   56. To make sure the evidence you recover and analyze with computer forensics
       software can be admitted in court, you must test and validate the software. What
       group is actively providing tools and creating procedures for testing and validating
       computer forensics software?

       Mark only one oval.

          ⬭ Computer Forensics Tools and Validation Committee

          ⬭ Association of Computer Forensics Software Manufactures

          ⬭ National Institute of Standards and Technology

          ⬭ Society for Valid Forensics Tools and Testing

65. 57. Bob has been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the System for a period of three weeks. However, law enforcement agencies were recoding his every activity and this was later presented as evidence. The organization had used a Virtual Environment to trap Bob. What is a Virtual Environment?

Mark only one oval.

   ◯ A Honeypot that traps hackers

   ◯ A system Using Trojaned commands

   ◯ An environment set up after the user logs in

   ◯ An environment set up before a user logs out

66. 58. When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?

Mark only one oval.

   ◯ a write-blocker

   ◯ a protocol analyzer

   ◯ a firewall

   ◯ a disk editor

67. 59. If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?

Mark only one oval.

   ◯ The system files have been copied by a remote attacker

   ◯ The system administrator has created an incremental backup

   ◯ The system has been compromised using a t0rnrootkit

   ◯ Nothing in particular as these can be operational files

68.   60. 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?

Mark only one oval.

- ◯ rootkit
- ◯ key escrow
- ◯ steganography
- ◯ Offset

This content is neither created nor endorsed by Google.

Google Forms