BRAINWARE UNIVERSITY

Term End Examination 2021 - 22

Programme – Master of Science in Advanced Networking & Cyber Security

Course Name – Digital Security and Forensic Fundamental

Course Code - MNCS403

(Semester IV)

Time allotted : 1 Hrs.15 Min. **Full Marks : 60**

[The figure in the margin indicates full marks.]

Group-A

(Multiple Choice Type Question) 1 x 60=60

Choose the correct alternative from the following :

(1) Wireless access control attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allow the attacker to set up a rogue access point outside the corporate perimeter and then lure the employees of the organization to connect to it?

a) Ad hoc associations b) Client mis-association

c) MAC spoofing d) Rogue access points

(2) Which of the following tool captures and allows you to interactively browse the traffic on a network?

a) Security Task Manager b) Wireshark

c) ThumbsDisplay d) RegScanner

(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.”

a) DDoS b) Sniffer Attack

c) Buffer Overflow d) Man-in-the-Middle Attack

(4) Which US law does the interstate or international transportation and receiving of child pornography fall under?

a) §18. U.S.C. 1466A b) §18. U.S.C 252

c) §18. U.S.C 146A d) §18. U.S.C 2252

(5) Which of the following file contains the traces of the applications installed, run, or uninstalled from a system?

a) Shortcut Files
b) Virtual files
c) Prefetch Files
d) Image Files

(6) Which of the following tasks DOES NOT come under the investigation phase of a cybercrime forensics investigation case?

a) Data collection
b) Secure the evidence
c) First response
d) Data analysis

(7) What stage of the incident handling process involves reporting events?

a) Containment
b) Follow-up
c) Identification
d) Recovery

(8) While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte 5h. What does this indicate on the computer?

a) The files have been marked as hidden
b) The files have been marked for deletion
c) The files are corrupt and cannot be recovered
d) The files have been marked as read-only

(9) Why would you need to find out the gateway of a device when investigating a wireless attack?

a) The gateway will be the IP of the proxy server used by the attacker to launch the attack
b) The gateway will be the IP of the attacker computer
c) The gateway will be the IP used to manage the RADIUS server
d) The gateway will be the IP used to manage the access point

(10) What will the following Linux command accomplish? dd if=/dev/mem of=/home /sam/mem.bin bs=1024

a) Copy the master boot record to a file
b) Copy the contents of the system folder to a file
c) Copy the running memory to a file
d) Copy the memory dump file to an image file

(11) When investigating a wireless attack, what information can be obtained from the DHCP logs?

a) The operating system of the attacker and victim computers
b) IP traffic between the attacker and the victim
c) MAC address of the attacker
d) If any computers on the network are running in promiscuous mode

(12) What type of analysis helps to identify the time and sequence of events in an investigation?

a) Time-based
b) Functional
c) Relational
d) Temporal

(13) Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

a) Point-to-point
b) End-to-end
c) Thorough
d) Complete event analysis

(14) Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

a) Three

b) One

c) Two

d) Four

(15) Julie is a college student majoring in Information Systems and Computer Science. She is currently writing an essay for her computer crimes class. Julie paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subject. Julie would like to focus the subject of the essay on the most common type of crime found in corporate America. What crime should Julie focus on?

a) Physical theft

b) Copyright infringement

c) Industrial espionage

d) Denial of Service attacks

(16) When should an MD5 hash check be performed when processing evidence?

a) After the evidence examination has been completed

b) On an hourly basis during the evidence examination

c) Before and after evidence examination

d) Before the evidence examination has been completed

(17) Jacob is a computer forensics investigator with over 10 years experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob testimony in this case?

a) Justification

b) Authentication

c) Reiteration

d) Certification

(18) What technique is used by JPEGs for compression?

a) ZIP

b) TCD

c) DCT

d) TIFF-8

(19) Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company where stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way, the buyers knew when and where to meet with the alleged suspects to buy the stolen material. What type of steganography did these two suspects use?

a) Text semagram

b) Visual semagram

c) Grill cipher

d) Visual cipher

(20) An on-site incident response team is called to investigate an alleged case of computer tampering within their company. Before proceeding with the investigation, the CEO informs them that the incident will be classified as low level. How long will the team have to respond to the incident?

a) One working day

b) Two working days

c) Immediately

d) Four hours

(21) A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file. What kind of picture is this file?

a) Raster image
b) Vector image
c) Metafile image
d) Catalog image

(22) Why should you never power on a computer that you need to acquire digital evidence from?

a) When the computer boots up, files are written to the computer rendering the data nclean
b) When the computer boots up, the system cache is cleared which could destroy evidence
c) When the computer boots up, data in the memory buffer is cleared which could destroy evidence
d) Powering on a computer has no affect when needing to acquire digital evidence from it

(23) Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for. Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report?

a) TIFF-8
b) DOC
c) WPD
d) PDF

(24) When needing to search for a website that is no longer present on the Internet today but was online few years back, what site can be used to view the website collection of pages?

a) Proxify.net
b) Dnsstuff.com
c) Samspade.org
d) Archive.org

(25) What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

a) Cracks every password in 10 minutes
b) Distribute processing over 16 or fewer computers
c) Support for Encrypted File System
d) Support for MD5 hash verification

(26) A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

a) Searching for evidence themselves would not have any ill effects
b) Searching could possibly crash the machine or device
c) Searching creates cache files, which would hinder the investigation
d) Searching can change date/time stamps

(27) If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

a) Keep the device powered on
b) Turn off the device immediately
c) Remove the battery immediately
d) Remove any memory cards immediately

(28) In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on “bringing down the Internet”. Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

a) The change in the routing fabric to bypass the affected router

b) More RESET packets to the affected router to get it to power back up

c) RESTART packets to the affected router to get it to power back up

d) STOP packets to all other routers warning of where the attack originated

(29) 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?

a) RestrictAnonymous must be set to "10" for complete security

b) RestrictAnonymous must be set to "3" for complete security

c) RestrictAnonymous must be set to "2" for complete security

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

(30) Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

a) Block all internal MAC address from using SNMP

b) Block access to UDP port 171

c) Block access to TCP port 171

d) Change the default community string names

(31) Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? Needs?

a) Circuit-level proxy firewall

b) Packet filtering firewall

c) Application-level proxy firewall

d) Data link layer firewall

(32) As a security analyst, you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

a) The IP address of the employees' computers

b) Bank account numbers and the corresponding routing numbers

c) The employees network usernames and passwords

d) The MAC address of the employees' computers

(33) What is a good security method to prevent unauthorized users from "tailgating"?

a) Man trap

b) Electronic combination locks

c) Pick-resistant locks

d) Electronic key systems

(34) James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

a) Smurf

b) Trinoo

c) Fraggle

d) SYN flood

(35) Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

a) Trick the switch into thinking it already has a session with Terri's computer

b) Poison the switch's MAC address table by flooding it with ACK bits

c) Crash the switch with a DoS attack since switches cannot send ACK bits

d) Enable tunneling feature on the switch

(36) Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

a) Entrapment

b) Enticement

c) Intruding into a honeypot is not illegal

d) Intruding into a DMZ is not illegal

(37) 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?

a) Tailgating

b) Backtrapping

c) Man trap attack

d) Fuzzing

(38) You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

a) Show outdated equipment so it can be replaced

b) List weak points on their network

c) Use attack as a launching point to penetrate deeper into the network

d) Demonstrate that no system can be protected against DoS attacks

(39) George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

a) src port 23 and dst port 23

b) udp port 22 and host 172.16.28.1/24

c) net port 22

d) src port 22 and dst port 22

(40) George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

a) Nessus is too loud

b) Nessus cannot perform wireless testing

c) Nessus is not a network scanner

d) There are no ways of performing a "stealthy" wireless scan

(41) John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

a) Firewalk cannot pass through Cisco firewalls

b) Firewalk sets all packets with a TTL of zero

c) Firewalk cannot be detected by network sniffers

d) Firewalk sets all packets with a TTL of one

(42) Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?

a) EFS Encryption

b) DFS Encryption

c) IPS Encryption

d) SDW Encryption

(43) 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?

a) PDF passwords can easily be cracked by software brute force tools

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

c) PDF passwords are not considered safe by Sarbanes-Oxley

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

(44) John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

a) Hillary network username and password hash

b) The SID of Hillary network account

c) The SAM file from Hillary computer

d) The network shares that Hillary has permissions

(45) Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?

a) Router Penetration Testing

b) DoS Penetration Testing

c) Firewall Penetration Testing

d) Internal Penetration Testing

(46) Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

a) Tracert

b) Smurf scan

c) Ping trace

d) ICMP ping sweep

(47) Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

a) Closed b) Open
c) Stealth d) Filtered

(48) You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site that recommends inputting the following code into a search field on web pages to check for vulnerabilities: When you type this and click on search, you receive a pop-up window that says: “This is a test.” What is the result of this test?

a) Your website is vulnerable to CSS
b) Your website is not vulnerable
c) Your website is vulnerable to SQL injection
d) Your website is vulnerable to web bugs

(49) Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company’s network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

a) Send DOS commands to crash the DNS servers
b) Perform DNS poisoning
c) Perform a zone transfer
d) Enumerate all the users in the domain

(50) 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?

a) Plain view doctrine
b) Corpus delicti
c) Locard Exchange Principle
d) Ex Parte Order

(51) In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

a) The ISP can investigate anyone using their service and can provide you with assistance
b) The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant
c) The ISP can’t conduct any type of investigations on anyone and therefore can’t assist you
d) ISP’s never maintain log files so they would be of no use to your investigation

(52) You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?

a) Stringsearch
b) grep
c) dir
d) vim

(53) The police believe that Melvin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers and Educational Institutions. They also suspect that he has been stealing, copying and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspects door and searching his home and seizing all of his computer equipment if they have not yet

obtained a warrant?

a) The Fourth Amendment
b) The USA patriot Act
c) The Good Samaritan Laws
d) The Federal Rules of Evidence

(54) George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network.What filter should George use in Ethereal?

a) src port 23 and dst port 23
b) udp port 22 and host 172.16.28.1/24
c) net port 22
d) src port 22 and dst port 22

(55) You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers: http://172.168.4.131/level/99/exec/show/config. After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

a) HTTP Configuration Arbitrary Administrative Access Vulnerability
b) HTML Configuration Arbitrary Administrative Access Vulnerability
c) Cisco IOS Arbitrary Administrative Access Online Vulnerability
d) URL Obfuscation Arbitrary Administrative Access Vulnerability

(56) Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their various activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?

a) The manufacturer of the system compromised
b) The logic, formatting and elegance of the code used in the attack
c) The nature of the attack
d) The vulnerability exploited in the incident

(57) A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation. During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?

a) They examined the actual evidence on an unrelated system
b) They attempted to implicate personnel without proof
c) They tampered with evidence by using it
d) They called in the FBI without correlating with the fingerprint data

(58) While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?

a) Keep the information of file for later review
b) Destroy the evidence
c) Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge
d) Present the evidence to the defense attorney

(59) You have used a newly released forensic investigation tool, which doesn’t meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?

a) The tool hasn’t been tested by the International Standards Organization

b) Only the local law enforcement should use the tool

c) The total has not been reviewed and accepted by your peers

d) You are not certified for using the tool

(60) 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?

a) Computer Forensics Tools and Validation Committee

b) Association of Computer Forensics Software Manufactures

c) National Institute of Standards and Technology

d) Society for Valid Forensics Tools and Testing