BRAINWARE UNIVERSITY

Term End Examination 2021 - 22
Programme – Master of Science in Advanced Networking & Cyber Security
Course Name – Cyber Security-II
Course Code - MNCS401
(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) Which of the following best describes footprinting?
- a) Enumeration of services
- b) Discovery of services
- c) Discussion with people
- d) Investigation of a target

(2) Why use Google hacking?
- a) To fine-tune search results
- b) To speed up searches
- c) To target a domain
- d) To look for information about Google

(3) What is EDGAR used to do?
- a) Validate personnel
- b) Check financial filings
- c) Verify a website
- d) Gain technical details

(4) Which of the following can be used to tweak or fine-tune search results?
- a) Archiving
- b) Operators
- c) Hacking
- d) Refining

(5) Which of the following can an attacker use to determine the technology and structure within an organization?
- a) Job boards
- b) Archives
- c) Google hacking
- d) Social engineering

(6) Which of the following can help you determine business processes of your target through human interaction?
- a) Social engineering
- b) Email
- c) Website
- d) Job boards

(7) What can be configured in most search engines to monitor and alert you of changes to content?

a) Notifications
b) Schedules
c) Alerts
d) HTTP

(8) If you can not gain enough information directly from a target, what is another option?

a) EDGAR
b) Social engineering
c) Scanning
d) Competitive analysis

(9) Which of the following would be a very effective source of information as it relates to social engineering?

a) Social networking
b) Port scanning
c) Websites
d) Job boards

(10) Footprinting can determine all of the following except which one?

a) Hardware types
b) Software types
c) Business processes
d) Distribution and number of personnel

(11) Which tool can trace the path of a packet?

a) Ping
b) Tracert
c) Whois
d) DNS

(12) Enumeration does not uncover which of the following pieces of information?

a) Services
b) User accounts
c) Ports
d) Shares

(13) Which command can be used to view NetBIOS information?

a) netstat
b) nmap
c) nbtstat
d) telnet

(14) Which ports does SNMP use to function?

a) 160 and 161
b) 160 and 162
c) 389 and 160
d) 161 and 162

(15) SNMP is used to perform which function in relation to hardware?

a) Trap messages
b) Monitor and manage traffic
c) Manage users and groups
d) Monitor security and violations

(16) Which of the following is used for identifying a web server OS?

a) Telnet
b) Netcraft
c) Fragroute
d) Wireshark

(17) Which of the following involves grabbing a copy of a zone file?

a) Zone transfer
b) nslookup transfers
c) DNS transfer
d) Zone update

(18) Which of the method is for expanding an email list?

a) VRFY
b) EXPN
c) RCPT TO
d) SMTP

(19) LDAP is used to perform which function?

a) Query a network
b) Query a database
c) Query a directory
d) Query a file system

(20) A DNS zone transfer is used to do which of the following?

a) Copy files
b) Perform searches
c) Synchronize server information
d) Decommission servers

(21) How would you use Netcat to set up a server on a system?

a) nc –l –p 192.168.1.1
b) nc –l –p 1000
c) nc –p –u 1000
d) nc –l –p –t 192.168.1.1

(22) How is a brute-force attack performed?

a) By trying all possible combinations of characters
b) By trying dictionary words
c) By capturing hashes
d) By comparing hashes

(23) An attacker can use which of following method to return to a system?

a) Backdoor
b) Cracker
c) Account
d) Service

(24) Which system should be used instead of LM or NTLM?

a) NTLMv2
b) SSL
c) Kerberos
d) LM

(25) Which of the following is a utility used to reset passwords?

a) TRK
b) ERC
c) WinRT
d) IRD

(26) Alternate Data Streams are supported in which file systems?

a) FAT16
b) FAT32
c) NTFS
d) CDFS

(27) A virus does not do which of the following?

a) Replicate with user interaction
b) Change configuration settings
c) Exploit vulnerabilities
d) Display pop-ups

(28) What are worms typically known for?

a) Rapid replication
b) Configuration changes
c) Identity theft
d) DDoS

(29) Which utility will tell you in real time which ports are listening or in another state?

a) Netstat
b) TCPView
c) Nmap
d) Loki

(30) Which of the following is capable of port redirection?

a) Netstat
b) TCPView
c) Netcat
d) Loki

(31) What is a covert channel?

a) An obvious method of using a system
b) A defined process in a system
c) A backdoor
d) A Trojan on a system

(32) A covert channel or backdoor may be detected using all of the following except which of the following?

a) Nmap
b) Sniffers
c) An SDK
d) Netcat

(33) A remote access Trojan would be used to do all of the following except which of the following?

a) Steal information
b) Remotely control a system
c) Sniff traffic
d) Attack another system

(34) A logic bomb is activated by which of the following?

a) Time and date
b) Vulnerability
c) Actions
d) Events

(35) Which of the following feature is of a sparse infector virus

a) Creates backdoors
b) Infects data and executables
c) Infects files selectively
d) Rewrites itself

(36) Which of the following prevents ARP poisoning?

a) ARP Ghost
b) IP DHCP Snooping
c) IP Snoop
d) DNSverf

(37) MAC spoofing applies a legitimate MAC address to an unauthenticated host, which allows the attacker to pose as a valid user. Based on your understanding of ARP, what would indicate a bogus client?

a) The MAC address doesn't map to a manufacturer
b) The MAC address is two digits too long
c) A reverse ARP request maps to two hosts
d) The host is receiving its own traffic

(38) What technique funnels all traffic back to a single client, allowing sniffing from all connected hosts?

a) ARP redirection
b) ARP poisoning
c) ARP flooding
d) ARP partitioning

(39) Jennifer is using tcpdump to capture traffic on her network. She would like to save the capture for later review. What command can Jennifer use?

a) tcpdump –r capture.log
b) tcpdump –l capture.log
c) tcpdump –t capture.log
d) tcpdump –w capture.log

(40) Tiffany is analyzing a capture from a client's network. She is particularly interested in NetBIOS traffic. What port does Tiffany filter for?

a) 123
b) 139
c) 161
d) 110

(41) Wireshark requires a network card to be able to enter which mode to sniff all network traffic?

a) Capture mode
b) Promiscuous mode
c) Pcap mode
d) Gather mode

(42) Janet receives an email enticing her to click a link. But when she clicks this link she is taken to a website for her bank, asking her to reset her account info. However, Janet noticed that the bank is not hers and the website is not for her bank. What type of attack is this?

a) Whaling
b) Vishing
c) Phishing
d) Piggybacking

(43) Jason receives notices that he has unauthorized charges on his credit card account. What type of attack is Jason a victim of?

a) Social engineering
b) Phishing
c) Identity theft
d) Bad luck

(44) What is a vulnerability scan designed to provide to those executing it?

a) A way to find open ports
b) A way to diagram a network
c) A proxy attack
d) A way to reveal vulnerabilities

(45) An attacker can use which technique to influence a victim?

a) Tailgating
b) Piggybacking
c) Name-dropping
d) Acting like tech support

(46) Social engineering can be used to carry out email campaigns by which of the following?

a) Spamming
b) Phishing
c) Vishing
d) Splashing

(47) Zombies Inc. is looking for ways to better protect their web servers from potential DoS attacks. Their web admin proposes the use of a network appliance that receives all incoming web requests and forwards them to the web server. He says it will prevent direct customer contact with the server and reduce the risk of DoS attacks. What appliance is he proposing?

a) Web proxy
b) IDS
c) Reverse proxy
d) Firewall

(48) What command-line utility can you use to craft custom packets with specific flags set?

a) Nmap
b) Zenmap
c) Ping
d) hping3

(49) Which statement defines session hijacking most accurately?

a) Session hijacking involves stealing a user's login information and using that information to pose as the user later
b) Session hijacking involves assuming the role of a user through the compromise of physical tokens such as common access cards
c) Session hijacking is an attack that aims at stealing a legitimate session and posing as that user while communicating with the web resource or host machine
d) Session hijacking involves only web applications and is specific to stealing session IDs from compromised cookies

(50) Jennifer is a junior system administrator for a small firm of 50 employees. For the last week a few users have been complaining of losing connectivity intermittently with no suspect behavior on their part such as large downloads or intensive processes. Jennifer runs Wireshark on Monday morning to investigate. She sees a large amount of ARP broadcasts being sent at a fairly constant rate. What is Jennifer most likely seeing?

a) ARP poisoning
b) ARP caching
c) ARP spoofing
d) DNS spoofing

(51) An ethical hacker sends a packet with a deliberate and specific path to its destination. What technique is the hacker using?

a) IP spoofing
b) Source routing
c) ARP poisoning
d) Host routing

(52) A public use workstation contains the browsing history of multiple users who logged in during the last seven days. While digging through the history, a user runs across the following web address: www.snaze.com/&w25/session=22525. What kind of embedding are you seeing?

a) URL embedding
b) Session embedding
c) Hidden form embedding
d) Tracking cookie

(53) Which technology can provide protection against session hijacking?

a) IPSec
b) UDP
c) TCP
d) IDS

(54) A man-in-the-middle attack is an attack where the attacking party does which of the following?

a) Infect the client system
b) Infect the server system
c) Insert themselves into an active session
d) Insert themselves into a web application

(55) Session hijacking can do all of the following except which one?

a) Take over an authenticated session
b) Be used to steal cookies
c) Take over a session
d) Place a cookie on a server

(56) Which of the following is used to access content outside the root of a website?

a) Brute force
b) Port scanning
c) SQL injection
d) Directory traversal

(57) In the field of IT security, the concept of defense in depth is layering more than one control on another. Why would this be helpful in the defense of a system of session hijacking?

a) To provide better protection
b) To build dependency among layers
c) To increase logging ability
d) To satisfy auditors

(58) Which attack can be used to take over a previous session?

a) Cookie snooping
b) Session hijacking
c) Cookie hijacking
d) Session sniffing

(59) Input validation is used to prevent which of the following?

a) Bad input
b) Formatting issues
c) Language issues
d) SQL injection

(60) Proper input validation can prevent what from occurring?

a) Client-side issues
b) Operating system exploits
c) SQL injection attacks
d) Software failure