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

Course Name - –Cyber Security-II
Course Code - MNCS401

* 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. Which of the following best describes footprinting?

*Mark only one oval.*

- [ ] Enumeration of services
- [ ] Discovery of services
- [ ] Discussion with people
- [ ] Investigation of a target

10. 2. Why use Google hacking?

*Mark only one oval.*

- ◯ To fine-tune search results
- ◯ To speed up searches
- ◯ To target a domain
- ◯ To look for information about Google

11. 3. What is EDGAR used to do?

*Mark only one oval.*

- ◯ Validate personnel
- ◯ Check financial filings
- ◯ Verify a website
- ◯ Gain technical details

12. 4. Which of the following can an attacker use to determine the technology and structure within an organization?

*Mark only one oval.*

- ◯ Job boards
- ◯ Archives
- ◯ Google hacking
- ◯ Social engineering

13. 5. Which of the following can help you determine business processes of your target through human interaction?

*Mark only one oval.*

- Social engineering
- Email
- Website
- Job boards

14. 6. What can be configured in most search engines to monitor and alert you of changes to content?

*Mark only one oval.*

- Notifications
- Schedules
- Alerts
- HTTP

15. 7. If you can not gain enough information directly from a target, what is another option?

*Mark only one oval.*

- EDGAR
- Social engineering
- Scanning
- Competitive analysis

16. 8. Which of the following would be a very effective source of information as it relates to social engineering?

*Mark only one oval.*

- Social networking
- Port scanning
- Websites
- Job boards

17. 9. Footprinting has two phases. What are they?

*Mark only one oval.*

- Active and pseudonymous
- Active and passive
- Social and anonymous
- Scanning and enumerating

18. 10. Enumeration is useful to system hacking because it provides which of the following?

*Mark only one oval.*

- Passwords
- IP ranges
- Configurations
- Usernames

19. 11. Which of the following is used to connect to a remote system using NetBIOS?

*Mark only one oval.*

- NULL session
- Hash
- Rainbow table
- Rootkit

20. 12. SNS can is used to access information for which protocol?

*Mark only one oval.*

- SMTP
- FTP
- SNMP
- HTTP

21. 13. SNMP is used to do which of the following?

*Mark only one oval.*

- Transfer files
- Synchronize clocks
- Monitor network devices
- Retrieve mail from a server

22. 14. Which of the following is used for banner grabbing?

*Mark only one oval.*

- Telnet
- FTP
- SSH
- Wireshark

23. 15. Which of the following is used to perform customized network scans?

*Mark only one oval.*

- Nessus
- Wireshark
- AirPcap
- nmap

24. 16. An attacker can use which of the following method to enumerate users on a system?

*Mark only one oval.*

- NetBIOS
- TCP/IP
- NetBEUI
- NNTP

25. 17. VRFY is used to do which of the following?

*Mark only one oval.*

- Validate an email address
- Expand a mailing list
- Validate an email server
- Test a connection

26. 18. What is an SID used to do?

*Mark only one oval.*

- Identify permissions
- Identify a domain controller
- Identify a user
- Identify a mail account

27. 19. What does the enumeration phase not discover?

*Mark only one oval.*

- Services
- User accounts
- Ports
- Shares

28. 20. Which of the following is the process of exploiting services on a system?

*Mark only one oval.*

- System hacking
- Privilege escalation
- Enumeration
- Backdoor

29. 21. An attacker can use which of following method to return to a system?

*Mark only one oval.*

- Backdoor
- Cracker
- Account
- Service

30. 22. Which system should be used instead of LM or NTLM?

*Mark only one oval.*

- NTLMv2
- SSL
- Kerberos
- LM

31. 23. Which of the following is a utility used to reset passwords?

*Mark only one oval.*

- TRK
- ERC
- WinRT
- IRD

32. 24. Alternate Data Streams are supported in which file systems?

*Mark only one oval.*

- FAT16
- FAT32
- NTFS
- CDFS

33. 25. A virus does not do which of the following?

*Mark only one oval.*

- Replicate with user interaction
- Change configuration settings
- Exploit vulnerabilities
- Display pop-ups

34. 26. What are worms typically known for?

*Mark only one oval.*

- Rapid replication
- Configuration changes
- Identity theft
- DDoS

35. 27. Which utility will tell you in real time which ports are listening or in another state?

*Mark only one oval.*

- Netstat
- TCPView
- Nmap
- Loki

36. 28.Which of the following is capable of port redirection?

*Mark only one oval.*

- Netstat
- TCPView
- Netcat
- Loki

37. 29. What is a covert channel?

*Mark only one oval.*

- An obvious method of using a system
- A defined process in a system
- A backdoor
- A Trojan on a system

38. 30. What is an Overt Channel?

*Mark only one oval.*

- An obvious method of using a system
- A defined backdoor process in a system
- A backdoor
- A Trojan on a system

39. 31. A covert channel or backdoor may be detected using all of the following except which of the following?

*Mark only one oval.*

- Nmap
- Sniffers
- An SDK
- Netcat

40. 32. A logic bomb has how many parts, typically?

*Mark only one oval.*

- One
- Two
- Three
- Four

41. 33. Which of the following feature is of a polymorphic virus

*Mark only one oval.*

- Evades detection through backdoors
- Evades detection through heuristics
- Evades detection through rewriting itself
- Evades detection through luck

42. 34. What mode must be configured to allow an NIC to capture all traffic on the wire?

*Mark only one oval.*

- Extended mode
- 10/100
- Monitor mode
- Promiscuous mode

43. 35. Jennifer is a system administrator who is researching a technology that will secure network traffic from potential sniffing by unauthorized machines. Jennifer is not concerned with the future impact on legitimate troubleshooting. What technology can Jennifer implement?

*Mark only one oval.*

- SNMP
- LDAP
- SSH
- FTP

44. 36. Bob is attempting to sniff a wired network in his first pen test contract. He sees only traffic from the segment he is connected to. What can Bob do to gather all switch traffic?

*Mark only one oval.*

- MAC flooding
- MAC spoofing
- IP spoofing
- DOS attack

45. 37. What common tool can be used for launching an ARP poisoning attack?

*Mark only one oval.*

- Cain & Abel
- Nmap
- Scooter
- Tcpdump

46. 38. What is the generic syntax of a Wireshark filter?

*Mark only one oval.*

- protocol.field operator value
- field.protocol operator value
- operator.protocol value field
- protocol.operator value field

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

*Mark only one oval.*

- 123
- 139
- 161
- 110

48. 40. Jennifer is using tcpdump to capture traffic on her network. She would like to review a capture log gathered previously. What command can Jennifer use?

*Mark only one oval.*

- tcpdump –r capture.log
- tcpdump – l capture.log
- tcpdump –t capture.log
- tcpdump –w capture.log

49. 41. Jennifer receives an email claiming that her bank account information has been lost and that she needs to click a link to update the bank's database. However, she doesn't recognize the bank, because it is not one she does business with. What type of attack is she being presented with?

*Mark only one oval.*

- Phishing
- Spam
- Whaling
- Vishing

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

*Mark only one oval.*

- Social engineering
- Phishing
- Identity theft
- Bad luck

51. 43. What is a vulnerability scan designed to provide to those executing it?

*Mark only one oval.*

- A way to find open ports
- A way to diagram a network
- A proxy attack
- A way to reveal vulnerabilities

52. 44. Jason notices that he is receiving mail, phone calls, and other requests for information. He has also noticed some problems with his credit checks such as bad debts and loans he did not participate in. What type of attack did Jason become a victim of?

*Mark only one oval.*

- Social engineering
- Phishing
- Identity theft
- Bad luck

53. 45. Jason is the local network administrator who has been tasked with securing the network from possible DoS attacks. Within the last few weeks, some traffic logs appear to have internal clients making requests from outside the internal LAN. Based on the traffic Jason has been seeing, what action should he take?

*Mark only one oval.*

- Throttle network traffic
- Update antivirus definitions
- Implement egress filtering
- Implement ingress filtering

54. 46. What is a single-button DDoS tool suspected to be used by groups such as Anonymous?

*Mark only one oval.*

- Trinoo
- Crazy Pinger
- LOIC
- DoSHTTP

55. 47. What response is missing in a SYN flood attack?

*Mark only one oval.*

- ACK
- SYN
- SYN-ACK
- URG

56. 48. Jennifer has been working with sniffing and session-hijacking tools on her company network. Since she wants to stay white hat, that is, ethical, she has gotten permission to undertake these activities. What would Jennifer's activities be categorized as?

*Mark only one oval.*

- Passive
- Monitoring
- Active
- Sniffing

57. 49. 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?

*Mark only one oval.*

- ARP poisoning
- ARP caching
- ARP spoofing
- DNS spoofing

58. 50. Which kind of values is injected into a connection to the host machine in an effort to increment the sequence number in a predictable fashion?

*Mark only one oval.*

- Counted
- Bit
- Null
- IP

59. 51. Network-level hijacking focuses on the mechanics of a connection such as the manipulation of packet sequencing. What is the main focus of web app session hijacking?

*Mark only one oval.*

- Breaking user logins
- Stealing session IDs
- Traffic redirection
- Resource DoS

60. 52. Julie has sniffed an ample amount of traffic between the targeted victim and an authenticated resource. She has been able to correctly guess the packet sequence numbers and inject packets, but she is unable to receive any of the responses. What does this scenario define?

*Mark only one oval.*

- Switched network
- SSL encryption
- TCP hijacking
- Blind hijacking

61. 53. XSS is typically targeted toward which of the following?

*Mark only one oval.*

- Web applications
- Email clients
- Web browsers
- Users

62. 54. A session hijack can happen with which of the following?

*Mark only one oval.*

- Networks and applications
- Networks and physical devices
- Browsers and applications
- Cookies and devices

63. 55. Which of the following best describes a web application?

*Mark only one oval.*

- Code designed to be run on the client
- Code designed to be run on the server
- SQL code for databases
- Targeting of web services

64. 56. Which of the following can prevent bad input from being presented to an application through a form?

*Mark only one oval.*

- Request filtering
- Input validation
- Input scanning
- Directory traversing

65. 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?

*Mark only one oval.*

- To provide better protection
- To build dependency among layers
- To increase logging ability
- To satisfy auditors

66. 58. A POODLE attack targets what exactly?

*Mark only one oval.*

- SSL
- TLS
- VPN
- AES

67. 59. Which of the following is the common attack against web servers and web applications?

*Mark only one oval.*

- Banner grab
- Input validation
- Buffer validations
- Buffer overflow

68. 60. Databases can be a victim of code exploits depending on which of the following?

*Mark only one oval.*

- Configuration
- Vendor
- Patches
- Client version