SECTION A. – OBJECTIVES

Answer all questions

30 Marks

1. Firewalls are to protect against
   a. Virus Attacks
   b. Fire Attacks
   c. Data Driven Attacks
   d. Unauthorized Attacks

2. Which of the following is considered as the unsolicited commercial email?
   a. Virus
   b. Malware
   c. Spam
   d. All of the above

3. Which one of the following can be considered as the class of computer threats?
   a. Dos Attack
   b. Phishing
   c. Soliciting
   d. Both A and C

4. Which of the following usually observe each activity on the internet of the victim, gather all information in the background, and send it to someone else?
   a. Malware
   b. Spyware
   c. Adware
   d. All of the above

5. Which of the following refers to stealing one's idea or invention of others and use it for their own benefits?
   a. Piracy
   b. Plagiarism
   c. Intellectual property rights
   d. All of the above

6. Read the following statement carefully and find out whether it is correct about the hacking or not?

   "It can be possible that in some cases, hacking a computer or network can be legal."

   a. No, in any situation, hacking cannot be legal
   b. It may be possible that in some cases, it can be referred to as a legal task
   c. Hacking can only be legal when warrant is taken from a law enforcement agency.
   d. Hacking is not a good practice.

7. Which one of the following refers to the technique used for verifying the integrity of the message?
    a. Digital signature
    b. Decryption algorithm
    c. Protocol
    d. Message Digest

8. In system hacking, which of the following is the most crucial activity?
    a. Information gathering
    b. Covering tracks
    c. Cracking passwords
    d. None of the above

9. Which of the following are the types of scanning?
    a. Network, vulnerability, and port scanning
    b. Port, network, and services
    c. Client, Server, and network
    d. None of the above

10. In the computer networks, the encryption techniques are primarily used for improving the ________
    a. Security
    b. Performance
    c. Reliability
    d. Longevity

11. Suppose an employee demands the root access to a UNIX system, where you are the administrator; that right or access should not be given to the employee unless that employee has work that requires certain rights, privileges. It can be considered as a perfect example of which principle of cyber security?
    a. Least privileges
    b. Open Design
    c. Separation of Privileges
    d. Both A & C

12. The web application like banking websites should ask its users to log-in again after some specific period of time, let say 30 min. It can be considered as an example of which cyber security principle?
    a. Compromise recording
    b. Psychological acceptability
    c. Complete mediation
    d. None of the above

13. Which of the following statements is true about the Trojans?
    a. Trojans perform tasks for which they are designed or programmed
    b. Trojans replicates them self's or clone them self's through an infections
    c. Trojans do nothing harmful to the user's computer systems
    d. None of the above

14. DNS translates a Domain name into
    a. Hex
    b. Binary
    c. IP
    d. URL

15. In order to ensure the security of the data/ information, we need to ____________ the data:
    a. Encrypt
    b. Decrypt
    c. Delete
    d. None of the above

16. Which of the following known as the oldest phone hacking techniques used by hackers to make free calls?
    a. Phreaking
    b. Phishing
    c. Cracking
    d. Spraining

17. Which of the following are famous and common cyber-attacks used by hackers to infiltrate the user's system?
    a. DDos and Derive-by Downloads
    b. Malware & Malvertising
    c. Phishing and Password attacks
    d. All of the above

18. Which one of the following is also referred to as malicious software?
    a. Maliciousware
    b. Badware
    c. Ilegalware
    d. Malware

19. The mouse on your computer screen starts to move around on its own and click on things on your desktop. What do you do?
    i. *Call your co-workers over so they can see*
    ii. *Disconnect your computer from the network*
    iii. *Unplug your mouse*
    iv. *Tell your supervisor*
    v. *Turn your computer off*
    vi. *Run anti-virus*

    a. I & III only
    b. II & III only
    c. II & IV only
    d. Do all listed above

20. Which of the following can be considered as the elements of cyber security or computer security?
    a. Application Security
    b. Operational Security
    c. Network Security
    d. All of the above

21. In which of the following, a person is constantly followed/chased by another person or group of several peoples?
    a. Phishing
    b. Bulling
    c. Stalking
    d. Identity theft

22. _______ is a type of software designed to help the user's computer detect viruses and avoid them.
    a. Malware
    b. Adware
    c. Antivirus
    d. Both B and C

23. Which one of the following is a type of antivirus program?
    a. Quick heal
    b. McAfee
    c. Kaspersky
    d. All of the above

24. It can be a software program or a hardware device that filters all data packets coming through the internet, a network, etc. it is known as the_______:
    a. Antivirus
    b. Firewall
    c. Cookies
    d. Malware

25. Which of the following refers to stealing one's idea or invention of others and use it for their own benefits?
    a. Piracy
    b. Plagiarism
    c. Intellectual property rights
    d. All of the above

26. Which one of the following statements is correct about Email security in the network security methods?
    a. One has to deploy hardware, software, and security procedures to lock those apps down.
    b. One should know about what the normal behaviour of a network look likes so that he/she can spot any changes, breaches in the behaviour of the network.
    c. Phishing is one of the most commonly used methods that are used by hackers to gain access to the network
    d. All of the above

27. Which of the following statements is true about the VPN in Network security?
    a. It is a type of device that helps to ensure that communication between a device and a network is secure.
    b. It is usually based on the IPsec(IP Security) or SSL (Secure Sockets Layer)

c. It typically creates a secure, encrypted virtual "tunnel" over the open internet

d. All of the above

28. Which of the following type of text is transformed with the help of a cipher algorithm?

a. Transformed text

b. Complex text

c. Scalar text

d. Plain text

29. The term "CHAP" stands for

a. Circuit Hardware Authentication Protocols

b. Challenge Hardware Authentication Protocols

c. Challenge Handshake Authentication Protocol

d. Circuit Handshake Authentication Protocols

30. Which type of the following malware does not replicate or clone them self's through infection?

a. Rootkits

b. Trojans

c. Worms

d. Viruses

31. Which of the following is a type of independent malicious program that never required any host program?

a. Trojan Horse

b. Worm

c. Trap Door

d. Virus

32. Which one of the following systems cannot be considered as an example of the operating systems?

a. Windows 8

b. Red Hat Linux

c. BSD Linux

d. Microsoft Office

33. In the CIA Triad, which one of the following is not involved?

a. Availability

b. Confidentiality

c. Authenticity

d. Integrity

34. Which of the following known as the oldest phone hacking techniques used by hackers to make free calls?

a. Phreaking

b. Phishing

c. Cracking

d. Spraining

35. _______ is the practice and precautions taken to protect valuable information from unauthorised access, recording, disclosure or destruction.

a. Network Security
b. Database Security
c. Information Security
d. Physical Security

36. From the options below, which of them is not a threat to information security?

a. Disaster
b. Eavesdropping
c. Information leakage
d. Unchanged default password

37. From the options below, which of them is not a vulnerability to information security?

a. Flood
b. without deleting data, disposal of storage media
c. unchanged default password
d. latest patches and updates not done

38. Which of the following information security technology is used for avoiding browser-based hacking?

a. Anti-malware in browsers
b. Remote browser access
c. Adware remover in browsers
d. Incognito mode in a browser

39. The full form of EDR is _______

a. Endpoint Detection and recovery
b. Early detection and response
c. Endpoint Detection and response
d. Endless Detection and Recovery

40. Compromising confidential information comes under _________

a. Bug
b. Threat
c. Vulnerability
d. Attack

41. Lack of access control policy is a ___________

a. Bug
b. Threat
c. Vulnerability
d. Attack

42. Possible threat to any information cannot be _______________

a. Reduced
b. Transferred
c. Protected
d. ignored

43. Name of the Hacker who breaks the SIPRNET system?

a. John Draper
b. Kevin Mitnick
c. John von Neumann
d. Kevin Poulsen

44. In order to ensure the security of the data/ information, we need to the data:

a. Encrypt

b. Decrypt

c. Delete

d. None of the above

45. Which of the following statements is true about the VPN in Network security?

a. It is a type of device that helps to ensure that communication between a device and a network is secure.

b. It is usually based on the IPsec(IP Security) or SSL (Secure Sockets Layer)

c. It typically creates a secure, encrypted virtual "tunnel" over the open internet

d. All of the above

46. Which of the following is not an example of physical data leakage?

a. Phishing

b. Dumpster diving

c. Shoulder surfing

d. Printers and photocopiers

47. What is the unauthorized movement of data?

a. Data cracking

b. Data infiltration

c. Data exfiltration

d. Database hacking

48. Which of the following is the most important activity in system hacking?

a. Covering tracks

b. Escalating privileges

c. Cracking passwords

d. Information gathering

49. What does TCP/ IP stands for?

a. Transaction control protocol / Internal protocol

b. Transmission control protocol / Internet protocol

c. Transmission contribution protocol / Internal protocol

d. None of the above

50. In system hacking, which of the following is the most crucial activity?

a. Covering tracks

b. Cracking passwords

c. Information gathering

d. None of the above

51. Which of the following is most important in design of secure system?

a. Assessing vulnerability

b. Changing or Updating System according to vulnerability

c. Both A & B

d. None of the above

52. Which of the following is also known as malicious software?

a. Badware

b. Illegalware

c. Malware

d. Maliciousware

53. Which of the following is the first computer virus?

a. Creeper

b. Blaster

c. Sasser

d. None of the above

54. Which of the following is not a type of scanning?

a. Xmas Tree Scan

b. Cloud scan

c. Null Scan

d. SYN Stealth

55. Code Red is a type of ________

a. An Antivirus Program

b. A photo editing software

c. A computer virus

d. A video editing software

56. Hackers usually used the computer virus for ______ purpose.

a. To log, monitor each and every user's stroke

b. To gain access the sensitive information like user's Id and Passwords

c. To corrupt the user's data stored in the computer system

d. All of the above

57. In Wi-Fi Security, which of the following protocol is more used?

a. WPA

b. WPA2

c. WPS

d. Both A and C

58. The response time and transit time is used to measure the ____________ of a network.

a. Security

b. Longevity

c. Reliability

d. Performance

59. Which of the following factor of the network gets hugely impacted when the number of users exceeds the network's limit?

a. Reliability

b. Performance

c. Security

d. Longevity

60. Which one of the following principles of cyber security refers that the security mechanism must be as small and simple as possible?

a. Open-Design

b. Economy of the Mechanism

c. Least privilege

d. Fail-safe Defaults