1. What is Cyber Security?
   a) Cyber Security provides security against malware
   b) Cyber Security provides security against cyber-terrorists
   c) Cyber Security protects a system from cyber attacks
   d) All of the mentioned
2. What does cyber security protect?
   a) Cyber security protects criminals
   b) Cyber security protects internet-connected systems
   c) Cyber security protects hackers
   d) None of the mentioned
3. Who is the father of computer security?
   a) August Kerckhoffs
   b) Bob Thomas
   c) Robert
   d) Charles
4. Which of the following is defined as an attempt to steal, spy, damage or destroy computer systems, networks, or their associated information?
   a) Cyber attack
   b) Computer security
   c) Cryptography
   d) Digital hacking
5. 5. Which of the following is a type of cyber security?
   a) Cloud Security

b) Network Security
c) Application Security
d) All of the above

6. What are the features of cyber security?
a) Compliance
b) Defense against internal threats
c) Threat Prevention
d) All of the above

7. Which of the following is an objective of network security?
a) Confidentiality
b) Integrity
c) Availability
d) All of the above

8. Which of the following is not a cybercrime?
a) Denial of Service
b) Man in the Middle
c) Malware
d) AES

9. Which of the following is a component of cyber security?
a) Internet Of Things
b) AI
c) Database
d) Attacks

10. Which of the following is a type of cyber attack?

a) Phishing
b) SQL Injections
c) Password Attack
d) All of the above

11. Which of the following is not an advantage of cyber security?

a) Makes the system slower
b) Minimizes computer freezing and crashes
c) Gives privacy to users
d) Protects system against viruses

12. “Cyberspace” was coined by _________

a) Richard Stallman
b) William Gibson
c) Andrew Tannenbaum
d) Scott Fahlman

13. In which year has hacking become a practical crime and a matter of concern in the field of cyber technology?

a) 1991
b) 1983
c) 1970
d) 1964

14. Governments hired some highly skilled hackers for providing cyber security for the country or state. These types of hackers are termed as _______

a) Nation / State sponsored hackers
b) CIA triad
c) Special Hackers
d) Government Hackers

15. Which of the following act violates cyber security?
a) Exploit
b) Attack
c) Threat
d) Vulnerability

16. Which of the following actions compromise cyber security?
a) Vulnerability
b) Attack
c) Threat
d) Exploit

17. Which of the following is the hacking approach where cyber-criminals design fake websites or pages for tricking or gaining additional traffic?
a) Pharming
b) Website-Duplication
c) Mimicking
d) Spamming

18. Which of the following is not a type of peer-to-peer cyber-crime?
a) MiTM

b) Injecting Trojans to a target victim
c) Credit card details leak in the deep web
d) Phishing

19. A cyber-criminal or penetration tester uses the additional data that stores certain special instructions in the memory for activities to break the system in which of the following attack?
a) Clickjacking
b) Buffer-overflow
c) Phishing
d) MiTM

20. Which of the following do Cyber attackers commonly target for fetching IP address of a target or victim user?
a) ip tracker
b) emails
c) websites
d) web pages

21. Which of the following is defined as an attempt to harm, damage or cause threat to a system or network?
a) Digital crime
b) Threats
c) System hijacking
d) Cyber Attack

22. They are nefarious hackers, and their main motive is to gain financial profit by doing cyber crimes. Who are

“they” referred to here?
a) White Hat Hackers
b) Black Hat Hackers
c) Hactivists
d) Gray Hat Hackers

23. IT security in any firm or organization is maintained and handled by ____________________
a) Software Security Specialist
b) CEO of the organization
c) Security Auditor
d) IT Security Engineer

24. Where did the term “hacker” originate?
a) MIT
b) New York University
c) Harvard University
d) Bell’s Lab

25. What is the existence of weakness in a system or network is known as?
a) Attack
b) Exploit
c) Vulnerability
d) Threat

26. Which of the following is an internet scam done by cyber-criminals where the user is convinced digitally to provide confidential information.

a) MiTM attack
b) Phishing attack
c) Website attack
d) DoS attack

27. Which of the following is not a step followed by cyber-criminals in data breaching?
a) Exfiltration
b) Research and info-gathering
c) Attack the system
d) Fixing the bugs

28. Which of the following online service's privacy cannot be protected using Tor?
a) Browsing data
b) Instant messaging
c) Login using ID
d) Relay chats

29. Which of the following term refers to a group of hackers who are both white and black hat?
a) Yellow Hat hackers
b) Grey Hat hackers
c) Red Hat Hackers
d) White-Black Hat Hackers

30. Which of the following is not an email-related hacking tool?
a) Mail Password

b) Email Finder Pro
c) Mail PassView
d) Sendinc

31. Which of the following DDoS in mobile systems wait for the owner to trigger the cyber attack?
a) botnets
b) programs
c) virus
d) worms

32. Which of the following is the least strong security encryption standard?
a) WPA3
b) WPA2
c) WPA
d) WEP

33. Which of the following is a Stuxnet?
a) Trojan
b) Antivirus
c) Worm
d) Virus

34. Which of the following ethical hacking technique is used for determining which operating system (OS) is running on a remote computer?
a) Operating System fingerprinting
b) Operating System penetration testing

c) Digital-printing
d) Machine printing

35. Which of the following can diminish the chance of data leakage?

a) Steganography
b) Chorography
c) Cryptography
d) Authentication

Question: A Proxy server is used for which of the following?

(a) To provide security against unauthorized users

(b) To process client requests for web pages

(c) To process client requests for database access

(d) To provide TCP/IP

Question: Passwords enable users to

(a) get into the system quickly

(b) make efficient use of time

(c) retain confidentiality of files

(d) simplify file structures

Question: Which will not harm computer resources?

(a) firewall

(b) Virus

(c) Trojan horse

(d) None of the above

Question: A program designed to destroy data on your computer which can travel to "infect" other computers is called a _

(a) disease

(b) torpedo

(c) hurricane

(d) virus

Question: Trojan-Horse programs

(a) are legitimate programs that allow unauthorized access

(b) are hacker programs that do not show up on the system

(c) really do not usually work
(d) are usually immediately discovered

Question: Technology, no longer protected by copyright, and is available to everyone, is considered to be:
(a) proprietary
(b) open
(c) experimental
(d) in the public domain.

Question: What is a backup?
(a) Restoring the information backup
(b) An exact copy of a system's information
(c) The ability to get a system up and running in the event of a system crash or failure
(d) All of these

Question: A computer checks the _____ of user names and passwords for a match before granting access.
(a) Website
(b) Network
(c) Backup file
(d) Data base

Question: All of the following are examples of real security and privacy risks. EXCEPT:
(a) Hackers
(b) Spam

(c) Viruses

(d) Identity theft

Question: Security violation due to

(a) malicious

(b) accidental

(c) both (a) and (b)

(d) none of these

Question: __ is a computer crime in which a criminal breaks into a computer system for exploring details of information etc.

(a) Hacking

(b) Spoofing

(c) Eavesdropping

(d) Phishing

Question: What does SSL stand for?

(a) Saving Sharing and Limits

(b) Safe, Secured and Locked

(c) Secure Socket Limbs

(d) Secure Socket Layers

Question: The security of a system can be improved by

(a) threat monitoring

(b) audit log

(c) both (a) and (b)

(d) none of these

Question: Which of the following would most likely NOT be a symptom of a virus?

(a) Existing program files and icons disappear
(b) The CD-ROM stops functioning
(c) The Web browser opens to an unusual home page
(d) Odd messages or images are displayed on the screen

Question: _____ are viruses that are triggered by the passage of time or on a certain date.
(a) Boot-sector viruses
(b) Macro viruses
(c) Time bombs
(d) Worms

Question: Verification of a login name and password is known as:
(a) configuration
(b) accessibility
(c) authentication
(d) logging in

Question: __ is a security protocol based on digital certificates.
(a) Digital signature
(b) Secure sockets layer protocol
(c) Secure electronic transactions
(d) None of these

Question: Worm was made up of
(a) one program
(b) two programs

(c) three programs
(d) all of these

Question: The ability to recover and read deleted or damaged files from a criminal's computer is an example of a law enforcement specialty called:
(a) robotics
(b) simulation
(c) computer forensics
(d) animation

Question: Firewalls are used to protect against __
(a) unauthorized Attacks
(b) virus Attacks
(c) Data Driven Attacks
(d) Fire Attacks

Question: Junk e-mail is also called
(a) spam
(b) spoof
(c) sniffer script
(d) spool

Question: Nowadays, phishing has become a criminal practice of using social engineering. For which of the following ?
(a) Social networking sites
(b) Mobile Phones
(c) E-mail
(d) Cyber cafes

Question: Back up of the data files will help to prevent .

(a) loss of confidentiality

(b) duplication of data

(c) virus infection

(d) loss of data

Question: What is backup?

(a) Adding more components to your network

(b) Protecting data by copying it from the original source to a different destination

(c) Filtering old data from new data

(d) Accessing data on tape

Question: __ can be used to minimize the risk of security breaches or viruses.

(a) Firewall

(b) Backups

(c) Encryption

(d) Digital signature

Question: Software, such as viruses, worms and Trojan horses, that has a malicious intent is known as:

(a) spyware

(b) adware

(c) spam

(d) malware

Question: A __ sometimes called a boot sector virus, executes when a computer boots up because it resides in the boot sector

of a floppy disk or the master boot record of a hard disk.
(a) system virus
(b) Trojan horse virus
(c) file virus
(d) None of these

Question: The digital signature is:
(a) A form of security for electronic records
(b) Copy
(c) Task
(d) Area

Question: A result of a computer virus can not lead to __
(a) Disk Crash
(b) Mother Board Crash
(c) Corruption of programs
(d) Deletion of files

Question: _____ is science that attempts to produce machines that display the same type of intelligence that humans do.
(a) Nanoscience
(b) Nanotechnology
(c) Simulation
(d) Artificial intelligence

Question: If you receive an e-mail from someone you don’t know, what should you do ?
(a) Forward it to the police immediately
(b) Delete it without opening it

(c) Open it and respond to them saying you don’t know them

(d) Reply and ask them for their personal information

Question: Secret key is used in

(a) Public key cryptography

(b) Symmetric cryptography

(c) Asymmetric cryptography

(d) none

Question: __ Is a specialized form of online identity theft.

(a) Spoofing

(b) Unauthorized disclosure

(c) Eavesdropping

(d) Phishing

Question: __ involves some one masquerading as someone else.

(a) Spoofing

(b) Unauthorized action

(c) Eavesdropping

(d) Phishing

Question: When information about transactions is transmitted in transparent way hackers can catch the transmissions to obtain customers sensitive information. This is known as __

(a) Spoofing

(b) Unauthorized disclosure

(c) Eavesdropping

(d) Phishing

Question: A competitor or an unhappy customer can alter a website so that it refuses services to potential clients. This is known as __

(a) Unauthorized action
(b) Unauthorized disclosure
(c) Eavesdropping
(d) Phishing

Question: __ can catch the transmissions to obtain customers sensitive information

(a) Firewall
(b) Antivirus
(c) Hackers
(d) None

Question: __ is online identity theft.

(a) Eavesdropping
(b) Phishing
(c) Spoofing
(d) None of these

Question: Which of the following is not a risk in internet based transaction

(a) eavesdropping
(b) spoofing
(c) encryption
(d) unauthorized action

Question: A security tool to verify the authenticity of the message and claimed identity of the sender and to verify the message integrity is

(a) encryption

(b) firewalls

(c) digital certificates

(d) digital signature

Question: __ are electronic files that are used to uniquely identify people and resources over the internet

(a) Digital signature

(b) Digital certificate

(c) Encryption recourse

(d) None

Question: An electronic file that uniquely identifies individuals and websites on the internet and enables secure, confidential communications.

(a) Digital signature

(b) Digital certificates

(c) Encryption

(d) Firewalls

Question: __ is designed to protect a person’s personal information.

(a) Data integrity

(b) Cyber law

(c) Private legislation

(d) None

Question: This acts like a gatekeeper that examines each user's identification before allowing them to enter the organization's internal networks.

(a) Antivirus program

(b) Biometrics

(c) Fire wall

(d) none

Question: SSL is the most widely deployed

(a) Security protocol

(b) Data encryption

(c) Cryptography

(d) None

Question: __ Is the process of coding and scrambling of messages to prevent unauthorized access to understanding of data being transmitted

(a) Cryptography

(b) Encryption

(c) Security key

(d) none

Question: __ is used to keep transmission private through the use of data encryption techniQuestion:

(a) Data encryption

(b) Cryptography

(c) Security key

(d) None

Question: The attacker monitors the data between the shoppers' computer and the server

(a) Spoofing

(b) snoofing

(c) Sniffing

(d) none

Question: The private content of a transaction, if unprotected, can be intercepted when it goes through the route over the internet is

(a) spoofing

(b) Snooping

(c) sniffing

(d) eavesdropping

Question: Creating illegitimate sites that appear to be published by established organizations are by this name

(a) Spamming

(b) Snooping

(c) Phishing

(d) Stealing

Question: A digital signature performs a similar function to a

(a) Thump impression

(b) Written Signature

(c) Scanning

(d) None

Question: ___are often delivered to a PC through an email attachment and are often designed to do harm.

(a) Viruses

(b) Spam

(c) Portals

(d) Email messages

1) 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

2) 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

3) Which of the following is considered as the unsolicited commercial email?

a. Virus
b. Malware
c. Spam
d. All of the above

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) _______ 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

6) Which one of the following is a type of antivirus program?

a. Quick heal

b. Mcafee

c. Kaspersky

d. All of the above

7) 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

8) 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

9) 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

10) Which of the following refers to exploring the appropriate, ethical behaviors related to the online environment and digital media platform?

a. Cyber low

b. Cyberethics

c. Cybersecurity

d. Cybersafety

11) Which of the following refers to the violation of the principle if a computer is no more accessible?

a. Access control

b. Confidentiality

c. Availability

d. All of the above

12) 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

13) Which one of the following usually used in the process of Wi-Fi-hacking?

a. Aircrack-ng

b. Wireshark

c. Norton

d. All of the above

14) Which of the following port and IP address scanner famous among the users?

a. Cain and Abel

b. Angry IP Scanner

c. Snort

d. Ettercap

15) In ethical hacking and cyber security, there are _______ types of scanning:

a. 1

b. 2

c. 3

d. 4

16) Which of the following is not a type of scanning?

a. Xmas Tree Scan
b. Cloud scan
c. Null Scan
d. SYN Stealth

17) 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

18) 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

19) Which one of the following is actually considered as the first computer virus?

a. Sasser
b. Blaster
c. Creeper

d. Both A and C

20) To protect the computer system against the hacker and different kind of viruses, one must always keep _________ on in the computer system.

a. Antivirus
b. Firewall
c. Vlc player
d. Script

21) Code Red is a type of ________

a. An Antivirus Program
b. A photo editing software
c. A computer virus
d. A video editing software

22) Which of the following can be considered as the elements of cyber security?

a. Application Security
b. Operational Security
c. Network Security
d. All of the above

23) 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

24) Which one of the following is also referred to as malicious software?

a. Maliciousware
b. Badware
c. Ilegalware
d. Malware

25) 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

26) In Wi-Fi Security, which of the following protocol is more used?

a. WPA
b. WPA2
c. WPS
d. Both A and C

27) The term "TCP/IP" stands for_____

a. Transmission Contribution protocol/ internet protocol
b. Transmission Control Protocol/ internet protocol
c. Transaction Control protocol/ internet protocol
d. Transmission Control Protocol/ internet protocol

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

a. Security
b. Longevity
c. Reliability
d. Performance

29) 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

30) In the computer networks, the encryption techniques are primarily used for improving the ________

a. Security

b. Performance

c. Reliability

d. Longevity

31) Which of the following statements is correct about the firewall?

a. It is a device installed at the boundary of a company to prevent unauthorized physical access.

b. It is a device installed at the boundary of an incorporate to protect it against the unauthorized access.

c. It is a kind of wall built to prevent files form damaging the corporate.

d. None of the above.

32) When was the first computer virus created?

a. 1970

b. 1971

c. 1972

d. 1969

33) Which of the following is considered as the world's first antivirus program?

a. Creeper

b. Reaper

c. Tinkered

d. Ray Tomlinson

34) 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

35) Which of the following principle of cyber security restricts how privileges are initiated whenever any object or subject is created?

a. Least privilege

b. Open-Design

c. Fail-safe Defaults

d. None of the above

36) 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

37) Which of the following can also consider as the instances of Open Design?

a. CSS
b. DVD Player
c. Only A
d. Both A and B

38) Which one of the following principles states that sometimes it is become more desirable to rescored the details of intrusion that to adopt more efficient measure to avoid it?

a. Least common mechanism
b. Compromise recording
c. Psychological acceptability

d. Work factor

39) 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 cybersecurity principle?

a. Compromise recording
b. Psychological acceptability
c. Complete mediation
d. None of the above

40) 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 behavior of a network look likes so that he/she can spot any changes, breaches in the behavior 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

41) 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

42) 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

43) The term "CHAP" stands for __________

a. Circuit Hardware Authentication Protocols

b. Challenge Hardware Authentication Protocols

c. Challenge Handshake Authentication Protocols

d. Circuit Handshake Authentication Protocols

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

a. Rootkits

b. Trojans

c. Worms

d. Viruses

45) Which of the following malware's type allows the attacker to access the administrative controls and enables his/or her to do almost anything he wants to do with the infected computers.

a. RATs

b. Worms

c. Rootkits

d. Botnets

46) 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

47) Which of the following is just opposite to the Open Design principle?

a. Security through obscurity

b. Least common mechanism
c. Least privileges
d. Work factor

48) 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

49) Which of the following usually considered as the default port number of apache and several other web servers?

a. 20
b. 40
c. 80
d. 87

50) DNS translates a Domain name into ________

a. Hex
b. Binary
c. IP
d. URL

51) 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

52) In the CIA Triad, which one of the following is not involved?

a. Availability
b. Confidentiality
c. Authenticity
d. Integrity

53) In an any organization, company or firm the policies of information security come under__________

a. CIA Triad
b. Confidentiality
c. Authenticity
d. None of the above

54) Why are the factors like Confidentiality, Integrity, Availability, and Authenticity considered as the fundamentals?

a. They help in understanding the hacking process
b. These are the main elements for any security breach
c. They help to understand the security and its components in a better manner
d. All of the above

55) 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

56) Which one of the following is considered as the most secure Linux operating system that also provides anonymity and the incognito option for securing the user's information?

a. Ubuntu
b. Tails
c. Fedora
d. All of the above

57) Which type following UNIX account provides all types of privileges and rights which one can perform administrative functions?

a. Client

b. Guest

c. Root

d. Administrative

58) Which of the following is considered as the first hacker's conference?

a. OSCON

b. DEVON

c. DEFCON

d. SECTION

59) 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

60) Name of the Hacker who breaks the SIPRNET system?

a. John Draper

b. Kevin Mitnick

c. John von Neumann

d. Kevin Poulsen