SKILL BASED ELECTIVE - 1
Network and Information Security

UNIT I: BASICS OF NETWORK

1. How long is an IPv6 address?

a. 32 bits
b. 128 bits
c. 64 bits
d. 128 bits

2. What is the size of the IP version 4?

a. 22 bytes
b. 32 bits
c. 32 bytes
d. 99 bytes

3. Bluetooth is an example of

A. personal area network
B. local area network
C. virtual private network
D. none of the mentioned

4. A _____ set of rules that governs data communication

a. Protocols
b. Standards
c. RFCs
d. None of the mentioned

5. In computer network nodes are

a. the computer that originates the data
b. the computer that routes the data
c. the computer that terminates the data
d. all of the mentioned

6. The first Network was

a. CNNET
b. NSFNET
c. ASAPNET
d. ARPANET

7. The_____ address identifies a process on a host.

a. physical
b. IP
c. port
d. specific

8. The ____ address uniquely defines a host on the Internet.
a. physical
b. IP
c. port
d. specific

9. An unauthorized user is a network _____ issue.

a. Performance
b. Reliability
c. Security
d. All the above

10. A _____ is a data communication system within a building, plant, or campus, or between nearby buildings.

a. LAN
b. MAN
c. WAN
d. none of the above

11. A _____ is a data communication system spanning states, countries, or the whole world.

a. MAN
b. LAN
c. WAN
d. none of the above

12. _____ is a collection of many separate networks.

a. A WAN
b. An internet
c. a LAN
d. None of the above

13. In a type of computer network, what does MAN stands for?

a. Major area network
b. Mini area network
c. Metropolitan area network
d. Micro area network

14. You have shared printers and scanners centrally in a Computer network, what is it called?

a. Data sharing
b. Resource sharing

c. Device sharing
d. Hardware sharing

15. How many layers does OSI have?

a. 4
b. 7
c. 5
d. 6

16. Computer Network is

a. Collection of hardware components and computers
b. Interconnected by communication channels
c. Sharing of resources and information
d. All of the Above

17. What is a Firewall in Computer Network?

a. The physical boundary of Network
b. An operating System of Computer Network
c. A system designed to prevent unauthorized access
d. A web browsing Software

18. What is the meaning of Bandwidth in Network?

a. Transmission capacity of a communication channels
b. Connected Computers in the Network
c. Class of IP used in Network
d. None of Above

19. The Internet is an example of

a. Cell switched network
b. Circuit switched network
c. Packet switched network
d. All of above

20. Which of the following is not the Networking Devices?

a. Gateways
b. Linux
c. Routers
d. Firewalls

21. _____ is a first-generation cellular phone system.

a. AMPS
b. D-AMPS
c. GSM
d. none of the above

22. A _____ is a device that forwards packets between networks by processing the routing information included in the packet.

a. bridge
b. firewall
c. router
d. hub

23. What is the main reason the OSI model was created?

A. To create a layered model larger than the DoD model.
B. So application developers can change only one layer's protocols at a time.
C. So different networks could communicate.
D. So Cisco could use the model.

24. The location of a resource on the internet is given by its?

a. Protocol
b. URL
c. E-mail address
d. ICQ

25. The term HTTP stands for?

a. Hyper terminal tracing program
b. Hypertext tracing protocol
c. Hypertext transfer protocol
d. Hypertext transfer program

26. Which one of the following is the most common internet protocol?

a. HTML
b. NetBEUI
c. TCP/IP
d. IPX/SPX

27. The term FTP stands for?

a. File transfer program
b. File transmission protocol
c. File transfer protocol
d. File transfer protection

28. The term WAN stands for?

a. Wide Area Net
b. Wide Access Network
c. Wide Area Network
d. Wide Access Net

29. How many versions available of IP?

a. 6 version
b. 4 version
c. 2 version
d. 1 version

30. The term LAN stands for?

a. Local Area Net
b. Local Area Network
c. Local Array Network
d. Local Array Net

31. Which performs modulation and demodulation

a. Modem
b. Fiber optic
c. satellite
d. coaxial cable

32. _____ is the most important/powerful computer in a typical network.

a. Desktop
b. Network server
c. Network client
d. Network switch

33. What is a benefit of networking your computer with other computers?

a. Increase in the computer's speed
b. Sharing of cables to cut down on expenses and clutter
c. Sharing of resources to cut down on the amount of equipment needed
d. Increase in the speed of the network

34. Communication between a computer and a keyboard involves _____ transmission.

a. Automatic
b. Half-duplex
c. Full-duplex
d. Simplex

35. The acronym OSI stands for ____ in computer networking.

A. Organization for Standards Institute
B. Open Systems Interconnection
C. Organizing Systems Interconnection
D. Open Systems Interworking

36. _____ is a computer or device that links two similar LANs based on the same protocol.

a. Bridge
b. Router
c. Gateway
d. Switches

37. _____ is a communication computer that connects different types of networks using different protocols.

a. Bridge
b. Router
c. Gateway
d. Switches

38. _____ is a network device that connects two different systems, using direct and systematic translation between protocols.

a. Bridge
b. Router
c. Gateway
d. Switches

UNIT I: NETWORK MEDIA

39. _____ cable consists of two insulated copper wires twisted together.

a. Coaxial
b. Fiber-optic
c. Twisted-pair
d. none of the above

40. _____ cable is used for voice and data communications.

a. Coaxial
b. Fiber-optic
c. Twisted-pair
d. none of the above

41. _____ consists of a central conductor and a shield.

a. Coaxial
b. Fiber-optic
c. Twisted-pair
d. none of the above

42. _____ cables are composed of a glass or plastic inner core surrounded by cladding, all encased in an outside jacket.

a. Coaxial
b. Fiber-optic
c. Twisted-pair
d. none of the above

43. _____ cables carry data signals in the form of light.

a. Coaxial
b. Fiber-optic
c. Twisted-pair
d. none of the above

44. Which transmission media has the highest transmission speed in a network?

a. coaxial cable
b. twisted pair cable
c. optical fiber
d. electrical cable

45. Twisted- pair wire, coaxial cable and fiber optic cable are all examples of _____

a. Guided media
b. Unguided media
c. Both A and B
d. None of these

46. How many pairs of cable in twisted pair cable?

a. 2
b. 4
c. 6
d. 8

47. Which factor makes twisted pair cable better than to fiber optic cable?

a. Cost
b. Signal attenuation
c. Noice resistance
d. Bandwidth range

48. Which factor makes fiber optic cable better than to twisted pair cable?

a. Cost
b. Bandwidth range
c. Robustness
d. Maintenance

49. Which of the following is not a communication media?

a. twisted pair
b. UTP
c. microwave
d. modem

50. _____ is the actual path over which an electrical signal travels as it moves from one component to another.

a. Network media
b. Transmission Media
c. Cable
d. Wireless

UNIT I: VARIOUS OPERATING SYSTEMS

51. Which of the following is not an operating system?

a. Windows
b. Linux
c. Oracle
d. DOS

52. When was the first operating system developed?

a. 1948
b. 1949
c. 1950
d. 1951

53. What is the full name of FAT?

a. File attribute table
b. File allocation table
c. Font attribute table
d. Format allocation table

54. BIOS is used?

a. By operating system
b. By compiler
c. By interpreter
d. By application software

55. Which of the following supports Windows 64 bit?

a. Window XP
b. Window 2000
c. Window 1998
d. None of these

56. Which of the following operating systems does not support more than one program at a time?

a. Linux
b. Windows
c. MAC
d. DOS

57. Who provides the interface to access the services of the operating system?

a. API
b. System call
c. Library
d. Assembly instruction

58. What is Microsoft window?

a. Operating system
b. Graphics program
c. Word Processing
d. Database program

59. Which of the following is an example of a Real Time Operating System?

a. MAC
b. MS-DOS
c. Windows 10
d. Process Control

60. Which windows was introduced to My Computer?

a. Windows 10
b. Windows XP
c. Windows 95
d. Windows 98

61. What program runs first after computer is booted and loading GUI?

a. Desktop Manager
b. File Manager
c. Windows Explorer
d. Authentication

62. Which is the latest version of MS Windows

A. Windows 2007
B. Windows 8.1
C. Windows 2008
D. Windows 10

63. Linux is an _____ operating system

a. Open source
b. Microsoft
c. Windows
d. Mac

64. Main memory of the computer system is also called

a. non volatile
b. volatile
c. reserved
d. large

65. Environment in which programs of the computer system are executed is:

a. operating system
b. nodes
c. clustered system
d. both a and b

66. One megabyte memory storage in the form of bytes is equal to

a. 1024 bytes
b. 1024 kilo bytes
c. 1056 bytes
d. 1058 kilo bytes

67. One that is not a peripheral device of the computer system is

a. keyboard
b. mouse
c. printer
d. register

68. MB memory storage stands for?

a. meta byte

b. Meta data
c. mega byte
d. mega bit

69. One byte memory storage is a collection of

a. characters
b. nibble
c. bits
d. words

70. Operating systems that can be modified and distributed are called

a. close source
b. open source
c. free
d. both a and b

71. The ability of an operating system is

a. multiprocessor
b. multiprogramming
c. clustering
d. both a and b

72. Today's fastest growing mobile phone operating system is

a. Apple's IOS
b. Google's Android
c. Mac OS X
d. Microsoft Windows

73. Android 1.5 is known by the name

a. Cupcake
b. Donut
c. Éclair
d. Froyo

74. Android 1.6 is known by the name

a. Cupcake
b. Donut
c. Éclair
d. Froyo

UNIT 1: Basics of Firewalls on all Platforms including Windows, MacOS and Linux.

75. Firewall is?

a. a hardware
b. a software
c. can be a hardware as well as software
d. can neither be a hardware nor a software

76. Firewalls can be of _____ kinds.

a.1
b.2
c.3
d.4

77. _____ is the kind of firewall is connected between the device and the network connecting to internet.

a. Hardware Firewall
b. Software Firewall
c. Stateful Inspection Firewall
d. Microsoft Firewall

78. _____ is software that is installed using an internet connection or they come by-default with operating systems.

a. Hardware Firewall
b. Software Firewall
c. Stateful Inspection Firewall
d. Microsoft Firewall

79. A firewall protects which of the following attacks?

a. Phishing
b. Dumpster diving
c. Denial of Service (DoS.
d. Shoulder surfing

80. There are _____ types of firewall.

a. 5
b. 4
c. 3
d. 2

81. Packet filtering firewalls are deployed on _____

a. routers
b. switches
c. hubs
d. repeaters

82. The _____ defines the packet filtering firewall rules.

a. Access Control List
b. Protocols

c. Policies
d. Ports

83. Which of the following is / are the types of firewall?

a. Packet Filtering Firewall
b. Dual Homed Gateway Firewall
c. Screen Host Firewall
d. Dual Host Firewall

84. What is a Firewall?

a. A firewall is a program that encrypts all the programs that access the Internet
b. Firewalls are network-based security measures that control the flow of incoming and outgoing traffic
c. A firewall is a program that keeps other programs from using the network.
d. Firewalls are interrupts that automatically disconnect from the internet when a threat appears

85. A firewall is a _____security system

a. Network
b. File
c. Program
d. None of These

86. Firewalls are frequently used to prevent unauthorized internet users from accessing private networks connected to the internet especially

a. Intranets
b. Extranets
c. Both of Above
d. None of These

87. Firewalls are used to protect:

a. Home Networks
b. Corporate Networks
c. Both of Above
d. None of These

88. Firewalls are often categorized as:

a. Network Firewalls
b. Host Based Firewalls
c. Either Network firewalls or Host based firewalls
d. None of These

UNIT II

1. _____ is a weakness that can be exploited by attackers.

a. System with Virus
b. System without firewall
c. System with vulnerabilities
d. System with a strong password

2. A _____ is a software bug that attackers can take advantage to gain unauthorized access in a system.

a. System error
b. Bugged system
c. Security bug
d. System virus

3. A computer _____ is a malicious code which self-replicates by copying itself to other programs.

a. program
b. virus
c. application
d. worm

4. Which of the below-mentioned tool is used for Wi-Fi hacking?

a. Wireshark
b. Nessus
c. Aircrack-ng
d. Snort

5. There are _____ types of scanning.

a. 2
b. 3
c. 4
d. 5

6. _____ scanning is a procedure to identify active hosts on your network.

a. Network
b. Port
c. Vulnerability
d. System

7. _____ scanning is an automatic process for identifying vulnerabilities of the system within a network.

a. Network
b. Port
c. Vulnerability
d. System

8. Which of them is not a standard scanning type or terminology?

a. Network
b. Port
c. Vulnerability
d. System

9. What is the first phase of hacking?

a. Maintaining access
b. Gaining access
c. Reconnaissance
d. Scanning

10. Which type of hacker represents the highest risk to your network?

A. Disgruntled employees
B. Black-hat hackers
C. Grey-hat hackers
D. Script kiddies

11. _____ is unauthorized altering of data before or during entry into a computer system, and then changing it back after processing is done

a. Foot-printing
b. Computer Stalking
c. Theft of passwords
d. Data Diddling

12. A defined way to breach the security of an IT system through vulnerability.

a. Local Exploit
b. Exploit
c. Attack
d. Threat

13. Programs (such as viruses, Trojan horses, and worms. that, when activated, cause harm to information systems

a. Hack value
b. Tiger Team

c. Malicious code
d. Black Hats

14. Is an existence of a software flaw, logic design, or implementation error that can lead to an unexpected and undesirable event executing bad or damaging instructions to the system?

a. Masquerading
b. Vulnerability Research
c. Vulnerability
d. Availability

15. Good guys, who use their hacking skills for defensive purposes.

a. White Hats
b. Threat
c. Grey hats
d. Black Hats

16. _____ is an attempt to get you to share personal information, usually by impersonating a trusted source.

a. Scanning
b. Hardening
c. Local Exploit
d. Social engineering

17. _____ is simple software that records the key sequence and strokes of your keyboard into a log file on your machine.

a. Keylogger
b. Denial of Service
c. Eavesdropping
d. Phishing

18. The _____ in our browser store personal data such as browsing history, username, and passwords for different sites we access.

a. Virus
b. Malware
c. Cookies
d. Phishing

19. _____ is an inspection of the potential points of exploit on a computer or network to identify security holes.

a. Vulnerability scanning
b. Denial of Service
c. Eavesdropping
d. Phishing

20. Unauthorized access to restricted systems or resources is referred as _____

a. Pharming
b. Penetration
c. Phishing
d. None of the Above

21. Sending large numbers of unwanted e-mail messages to a single recipient or to a group of such recipients is termed as _____

a. Logic bomb
b. Mail bombing
c. Time bomb
d. None of the above

22. Malicious modification or destruction of data such as changing information on Web sites is called _____

a. Super zapping
b. Vandalism
c. Spamming
d. None

23. An _____ is a technique that allows hackers to play upon the security vulnerabilities of the software that runs a web site.

a. SQL injection
b. Hacking
c. Scanning
d. All of the above

UNIT III

1. VLAN stands for

a. Virtual LAN
b. Visual LAN
c. Voice LAN
d. None of the Above

2. WPA2 stands for

a. Wi-Fi Privacy Access II
b. Wi-Fi Private Access II
c. Wi-Fi Protected Access II
d. Wi-Fi Privacy Act II

3. What are the types of widely used network architectures?

a. peer-to-peer
b. client/server aka tiered
c. Both a & b
d. None of the above

4. An _____ is a device or software application that monitors a network or systems for malicious activity or policy violations

a. Intrusion detection system
b. Encryption
c. Server
d. None of the above

5. What are the attacks used to penetrate wireless security

a. Brute-forcing
b. Shoulder surfing
c. Remote accessing
d. All the above

6. WEP stands for

a. Wireless encryption protection
b. Wired equivalent privacy
c. Wireless encrypted product
d. Wired encryption protection

7. _____ is a method of remapping an IP address space into another by modifying network address information in the IP header of packets while they are in transit across a traffic routing device.

a. Abstraction
b. Binding
c. Addressing
d. Network Address Translation

8. OSPF stands for _____

a. Open shortest path finder
b. Open shortest path first
c. Other shortest path finder
d. None of the above

9. ICMP stands for

a. internet control message protocol
b. instant connect message protocol
c. internet control message privacy
d. None of the above

10. A type of software application or script that performs tasks on command, allowing an attacker to take complete control remotely of an affected computer

a. DDoS
b. Worm
c. Botnet
d. Trojan horse

11._____ feature blocks other computers from performing operating system fingerprinting in windows 7

a. OS fingerprinting
b. boot-time filtering
c. **fullstealth**
d. None of the above

12. Rules that are applied to the traffic which is coming from the network and the Internet to your computer or device

a. Outbound rules
b. Inbound rules
c. Both a & b
d. None of the above

13. In the Windows Firewall with Advanced Security's Monitoring feature includes

a. The firewall rules that are active
b. The connection security rules that are active
c. Active security associations
d. All of the above

14. How many number of Network Profiles available in Windows 7 firewall

a. 2
b. 3 (public,work/home,domain.
c. 4
d. 5

15. NLA stands for _____

a. Network Location Awareness
b. Network Local Address
c. Network Location Address
d. No Location Address

16. How many chains (set of rules) are available to process the traffic in Linux firewall
a. 4
b. **3 (Input,output,forward)**
c. 1
d. 2

17. What are the actions which the iptables can perform on the traffic in linux

a. ACCEPT
b. DROP
c. REJECT
d. **All of the above**

18. Which one of the following command returns the current firewall status in linux

a. **# firewall-cmd --state**
b. # firewall-cmd --status
c. both a & b
d. None of the above

19. Netcat (nc., is a universal command line tool in Linux that can be used to

a. port scan
b. port forwarding
c. port allocation
d. port binding

20. –A command is used in Linux Iptable to perfom

a. Arithmetic functions
b. Add/Append
c. Both a & b
d. None of the above

21. Precautions to be taken while using Social Networking platforms safely

a. Secure passwords
b. Delete your password and browsing history
c. Careful when integrating your social network accounts
d. All of the above

22. Which of the following do not comes under the three pillars of digital privacy?

a. Communication privacy
b. Individual privacy
c. Family privacy
d. Communication privacy

23. Which of the following is not an appropriate solution for preserving privacy?

a. Use VPN
b. Close all logical ports
c. Do not use malicious sites and torrent sites
d. Use privacy-focussed SE

24. The _____ protects your privacy by bouncing your connection and links around a distributed network over the globe run by volunteers. It gives three layers of anonymity.

a. Private Search Engines
b. VPNs
c. Tor browser
d. Cookie removers

25. _____ allow its users to attach to the internet via a remote or virtual server which preserves privacy.

a. Tor browser
b. Private Search Engines
c. Cookie removers
d. VPNs

26. The data transferred between your device & the server is securely _____ if you're using VPNs.

a. Packed
b. Encrypted
c. Locked
d. Sealed

27. Which of these is a part of network identification?

a. Password
b. UserID
c. fingerprint
d. OTP

28. An algorithm in encryption is called _____

a. Procedure
b. Module
c. Object
d. Cipher

29. Which is not an objective of network security?
a. Identification

b. Lock
c. Access control
d. Identification

30. _____ is a malicious technique of tricking a user into clicking on something different from what the user perceives, thus potentially revealing confidential information

a. Clickjacking
b. Phishing
c. Attack
d. None of the above

UNIT IV

1. Several computers linked to a server to share programs and storage space.

A. Library
B. Network
C. Grouping
D. Integrated system

2. The Internet is

A. A communication system for some states of India
B. A communication system for the Indian government
C. An internal communication system for a business
D. **A large network of networks**

3. What Is the Most Important Activity In System Hacking?

A. Information Gathering
B. Cracking Passwords
C. Escalating Privileges
D. Covering Tracks

4._____ scanning is a procedure to identify active hosts on your network.

A. **Network**
B. Port
B. Vulnerability
D. System

5. Person who gains illegal access to a computer system is known as

A. hacker
B. worm
C. pirate
D. theif

6. Wi-Fi stands for-

A. Wireless Fidelity
B. Wireless LAN
C. Wireless FLAN
D. None of the mentioned

7. What is the primary goal of an Ethical Hacker?

A. Avoiding detection
B. Testing security controls
C. Resolving security vulnerabilities
D. Determining return on investment for security measures

8. The full form of Malware is _____

A. Malfunctioned Software
B. Multipurpose Software
C. **Malicious Software**
D. Malfunctioning of Security

9. What Is the Most Important Activity In System Hacking?

A. Information Gathering
B. Cracking Passwords
C. Escalating Privileges
D. Covering Tracks

10. Networks that are made up of hundreds and sometimes thousands of components are known as

A. Complex Networks
B. Hybrid Networks
C. Component Networks
D. All of the Above

11. Firewalls are used to protect:

A. Home Networks
B. Corporate Networks
C. Both of Above
D. None of These

12. What is a Firewall in Computer Network?

A. The physical boundary of Network
B. An operating System of Computer Network
C**. A system designed to prevent unauthorized access**
D. A web browsing Software

13. --------- helps to block websites, internet browsers, cable companies, and internet service providers from tracking your information and your browser history

A. Privacy
B. Security
C. Hacking
D. Password

14. -------- helps protect you from other people accessing your personal information and other data

A. Privacy
B. Security
C. Hacking
D. Password

15. Malware gets propagated through networks and technologies like?

A. SMS
B. Bluetooth
C. Wireless
D. **All of the above**

16.What are the uses of Malware?

A. Many early infectious programs, including the first Internet Worm, were written as experiments or pranks
B. Today, malware is used primarily to steal sensitive personal, financial, or business information for the benefit of others
C. Malware is sometimes used broadly against government or corporate websites to gather guarded information, or to disrupt their operation in general
D. All of these

17. Which of the following is not a stand-alone program?

A. Trojan
B. Worm
C. Virus
D. Spyware

18. Wireshark is a _____ tool.

A. **network protocol analysis**
B. network connection security
C. connection analysis
D. defending malicious packet-filtering

19. The first computer virus is

A. The famous
B. HARLIE
C. PARAM
D. Creeper

20. A computer virus may be used to –

A. Corrupt data in your computer
B. Log the user's keystrokes
C. Access private data like user id and passwords
D. **All of the above**

21. Which of the following is not Computer Hardware?

A. Antivirus
B. Printer
C. Mouse
D. Monitor

22. A honey pot is an example of what type of software?

A. **Intrusion-detection**
B. Virus
C. Encryption
D. Security-auditing

23. Ideally, what characters should you use in a password to make it strong?

A. Letters and Numbers only
B. Mixed Case (Upper and Lower.
C. Characters Special Characters
D. All of the above

24. Many applications use _____, where two independent factors are used to identify a user.

A. **Two-factor authentication**
B. Cross-site request forgery
C. Cross-site scripting
D. Cross-site scoring scripting

25._____ passwords are next level of security.

A. BIOS
B. CMOS
C. SMOS
D. BOIS

26. Which of the following are forms of malicious attack?

A. Theft of information
B. Modification of data
C. Wiping of information
D. **All of the mentioned**

27. What are the common security threats?

A. File Shredding
B. **File sharing and permission**
C. File corrupting
D. File integrity

28. Why is one time password safe?

A. It is easy to generated
B. It cannot be shared
C. **It is different for every access**
D. It is a complex encrypted password

29. What are the characteristics of Authorization?

A. RADIUS and RSA
B. 3 way handshaking with syn and fin
C. Multilayered protection for securing resources
D. Deals with privileges and rights

30. What forces the user to change password at first login?

A. Default behavior of OS
B. Part of AES encryption practice
C. Devices being accessed force the user
D. Account administrator

UNIT V

1. Network security consists of

A. Protection
B. Detection
C. Reaction
D**. All of the above**

2. Which of the following we should configure your systems and networks as correctly as possible?

A. **Protection**
B. Detection
C. Reaction
D. None of the above

3. The process of verifying the identity of a user.

A. **Authentication**
B. Identification
C. Validation
D. Verification

4. Which of these is a part of network identification?

a. **UserID**
b. Password
c. OTP
d. Fingerprint

5. An algorithm in encryption is called _____

a. Algorithm
b. Procedure
c. **Cipher**
d. Module

6. The information that gets transformed in encryption is _____

a. **Plain text**
b. Parallel text
c. Encrypted text
d. Decrypted text

7. The process of transforming plain text into unreadable text.

a. Decryption
b. **Encryption**
c. Network Security
d. Information Hiding

8. A process of making the encrypted text readable again.

A. **Decryption**
B. Encryption
C. Network Security
D. Information Hiding

9. A small program that changes the way a computer operates.

A. Worm
B. Trojan
C. Bomb
D. **Virus**

10. A program that copies itself.

A. **Worm**
B. Virus
C. Trojan
D. Bomb

11. Which of the following is programs that copy themselves throughout a computer or network?

A. Worms
B. Trojans
C. Viruses
D. Rootkits

12. Which of the following malware do not replicate or reproduce through infection?

A. Worms
B. Trojans
C. Viruses
D. Rootkits

13. Study of creating a d using encryption and decryption techniques.

A. Cipher
B. **Cryptography**
C. Encryption
D. Decryption

14. An attack in which the user receives unwanted amount of e-mails.

A. Smurfing
B. Denial of service
C**. E-mail bombing**

D. Ping storm

15. The protocol used to provide security to e-mails?

A.POP
B.PGP
C.SNMP
D.HTTP

16..... is an example for public key algorithm.

A.RSA
B.DES
C.IREA
D.RC5

17. Decryption and Encryption of data are the responsibility of which of the following layer?

A. Session layer
B. Network layer
C. Transport layer
D. Presentation layer

18. Firewalls are used for.....

A. routing
B. security
C. tunneling
D. congestion control

19..…….. is used to validate the identity of the message sender to the recipient.

A. Encryption
B. Decryption
C. Digital certificate
D. None of these

20. Digital signature needs a

A. Private-key system
B. Shared-key system
C. Public-key system
D. All of them

21. One way to preserve the integrity of a document is through the use of a

A. Eye-Rays
B. Finger Print
C. Biometric
D. X-Rays

22. To Hide Information Inside A Picture, What Technology Is Used?

A. Rootkits
B. Bitmapping
C. Steganography
D. Image Rendering

23. A unique piece of information that is used in encryption.

A. Cipher
B. Plain Text
C. Key
D. Cipher

24. An attack in which the user receives unwanted amount of e-mails.

A. Smurfing
B. Denial of service
C. E-mail bombing
D. Ping storm

25. Firewalls are to protect against

A. Virus Attacks
B. Fire Attacks
C. Data Driven Attacks
D. Unauthorized Attacks

26. Which of the following option is used to protect data and passwords?

A. Authorization
B. Authentication
C. Encryption
D. Non-repudiation

27. What are the forms of password cracking techniques?

A. AttackBrute Forcing
B. AttacksHybrid
C. AttackSyllable
D. All of the above

28. Your password should be?

A. at **least six characters**
B. at least seven characters
C. at least eight characters
D. at most eight characters

29. Why might someone break into (hack. your computer?

A. They don't like you
B. To commit a crime
C. To use it to distribute porn, malicious programs, etc.
D. All of the above

30. What is the virus that spread in computer?

A. It is system software
B. It is a computer program
C. It is a windows tool
D. It is hardware

31. Password cracking in system hacking is of _____ types.

A. Two
B. Three
C. **Four**
D. Five

32. What is not a best practice for password policy?

A. Deciding maximum age of password
B. Restriction on password reuse and history
C. Password encryption
D. Having change password every 2 years

33. A --- allows you to access software and verify your identity with a physical device rather than relying on authentication codes or passwords.

A. hard token
B. Soft token
C. Worm
D. Virus

34. Which of the following is an authentication method?

A. Biometric
B. Password
C. SMS code
D. **All of the above**