CYBER SECURITY

PROTOCOL NAMES:

1. ***Transmission control Protocol (TCP):*** *This is a communication protocol that computers uses to communicate over a network. TCP divides message into stream of packets which are sent and then reassembled at the destination.*

Example: *Examples include peer-to-peer sharing methods like File Transfer Protocol (FTP), Secure Shell (SSH), and Telnet.*

2. ***Internet Protocol (IP):***

Internet protocol is addressing protocol. It is always used together with TCP. IP addresses of packet, routes them through different nodes and networks until it reaches its final destination. TCP/IP is perhaps the most used standard protocol for connecting computer networks.

Example : *Examples include wired networking (e.g., Ethernet), wireless networking (e.g., 802.11ac), and Internet communication (e.g., IP)*

3. ***Internet Address Protocol (IP Address):***

This is the address that identifies a computer on a network using TCP/IP. An IP address contains series of four numbers unique to the computer concerned

Example *: 90.399.424.34. This address is usually supplied by a Internet Service Provider***.**

4. ***Post office Protocol (POP):*** *This is used to receive incoming E-mail .*

   Example : *email programs track retrieved messages, sometimes this process fails, and messages might download again.*

5. ***Simple mail transport Protocol (SMTP)***:

   This protocol is used for sending and distributing outgoing E-Mail .

   Example *: For example, vivek@gmail.com, where "vivek" is the username of the recipient and "gmail.com" is the domain name. If the domain name of the recipient's email address is different from the sender's domain name, then MSA will send the mail to the Mail Transfer Agent (MTA).*

6. File Transfer Protocol (FTP):*This is a system that allows users to transfer files from one computer to another computer. Files that can be transfered may include program files, text files and multimedia files ect. This method of file transfer is faster than that using HTTP.*

   Example *: sharing files like text file.*

7. ***Hyper Text Transfer Protocol (HTTP):****HTTP is used to transfer a hyper text between two or more computers. Hyper text is the text that is coded using the language called HTML. HTML codes are used to create links. This link may be in any format such as text or graphics.*

Eample : *For example, when a URL is entered into the browser, the browser sends an HTTP command to the web server directing it to search and transmit the requested web page.*

8. ***Ethernet:*** *Ethernet is a most popular protocol used for LAN communication. It transfer the information in digital packets. Every computer that uses this protocol contains the Ethernet Network Interface Card (NIC).*

Example : *An example of Ethernet is the cable system that connects the computer network of a small business office.*

9. ***Telnet:****Telnet is a set of rules used to connect one computer to another computer. The process of this connection is called as remote login. The computer who request connection is called local computer, who accept the connection is called remote computer. If you type commands in local computer remote login these commands executed in the remote computer. You can see in your monitor what is the process going on in this remote computer.*

Example : *The establishment of connection and display data on the local computer uses a Telnet server program to* *accept the connection and send responses to requests for information back to the local computer*.

10. *Gopher:Gopher is a sot of rules used to search, retrieve and display documents from remote sites. It is possible to initiate on-line connections with other systems through Goper. It also operates on client/server principal*.

    Example *: browse many different kinds of resources by looking at menus or listings of information available.*

11. ***User Datagram Protocol**: UDP is an alternative to TCP and also works with IP to transmit time-sensitive data. UDP enables low-latency data transmissions between internet applications, so this protocol is ideal for voice over IP or other audio and video requirements. Unlike TCP, UDP doesn't wait for all packets to arrive or organize the packets. Instead, UDP transmits all packets even if some haven't arrived.*

    ***Example :** transmits packets, while TCP transmits, organizes and ensures the packets arrive. While UDP works more quickly than TCP, it's also less reliable.*

12. ***Internet Control Message Protocol (ICMP):*** *ICMP protocol is made to send error messages in a network. It works with the IP protocol.* ***It helps to diagnose network communication issues.*** *ICMP is mainly used to determine whether or not data is reaching its specified destination in the best ways.*

Example : ***Unlike IP, ICMP is a connectionless protocol. To send an ICMP message from one system to another, it is not needed to establish a connection between systems.Generally,*** *ICMP is found on network devices like routers.* ***It is also used in distributed denial-of-service(DDoS) attacks.***

13. ***Address Resolution Protocol (ARP)****):****It maps network addresses to the physical addresses used by a data link protocol.***

Example : ***If Host A wants to transmit data to Host B, which is on the different network, then Host A sends an ARP request message to receive a MAC address for Host B. The router responds to Host A with its own MAC address pretend itself as a destination. When the data is transmitted to the destination by Host A, it will send to the gateway so that it sends to Host B. This is known as proxy ARP****.*

14. Dynamic Host Configuration Protocol (DHCP):

This protocol works on IP networks, assigning IP addresses to devices and hosts connected to the network. ***It also allows them to communicate with each other efficiently.***

Example **:***Some examples of DHCP options are Router (default gateway), DNS Servers, and DNS Domain Name.*

15. Spanning Tree Protocol (STP):

Defined by IEEE 802.1d, this protocol prevents loops on LAN. The STP deals with issues related to networks with bridges. ***It eliminates redundant links and process network changes and failures.****The STP monitors all the links in the network. To find any problem present in the links or a redundant link, it applies the spanning-tree algorithm (STA).*

Example : The STP protocol uses configuration messages as its protocol frames

16. ***Secure Shell (SSH)*** *: It is a network protocol that uses cryptography in order to secure network services over unsecured networks. Many applications like the execution of a comment remotely, access to a remote computer can be secured with SSH.*

Example : *SSH clients and servers can use a number of encryption methods.*

17. ***SSH File Transfer Protocol (SFTP):****The SSH File Transfer Protocol (**SFTP**) also known as secure FTP is used to secure the connection when a file is sent remotely from one system to another*.

Example *: clients and servers can use a number of encryption methods.*

18. ***Domain Name System (DNS)****: IP addresses are of numerical format and hence they are not easily readable or remember-able to humans. DNS is a hierarchical system that converts these IP addresses into a human-readable hostname. The most common vulnerability in DNS is cache poisoning. Here the attacker replaces the legitimate IP address to send the target audience to malicious websites.*

Example : *DNS amplification can also be exploited on a DNS server which permits recursive lookups and uses recursion to amplify the magnitude of the attack*.

19. **Internet Message Access Protocol (IMAP):***It is an Internet email protocol that stores emails on the mail server but allows the end-user to retrieve, see, and manipulate the messages as they were stored locally on the user's devices. Usernames, passwords, and messages can be intercepted .*

    Example : *the email server can be injected with malware, which in turn can be sent to clients using infected attachments.*

20. ***Hyper Text Transfer Protocol Secure (HTTPS):*** *HTTPS is abbreviated as Hyper Text Transfer Protocol Secure is a standard protocol to secure the communication among two computers one using the browser and other fetching data from web server.*

    Example : *HTTP is used for transferring data between the client browser (request) and the web server (response) in the hypertext format, same in case of HTTPS except that the transferring of data is done in an encrypted format. So it can be said that https thwart hackers from interpretation or modification of data throughout the transfer of packets.*

21. ***Character-orientated Protocols (COP)****:Each character has its own meaning in character-orientated protocols. A character may be a data byte or a control byte during transmission. The main COP in use today is known as Bisync or binary synchronous. Each character sent is transmitted using the ASCII code. Control bytes obviously have values in ASCII of between 00 and 1F, whereas data bytes have values between 20 and 7F.*

Example *: For example UART communication.*

22. ***Synchronous Protocol***: *These protocol involve timing information of sender along with the data bytes. This protocol helps receiver to remain synchronization with the sender.*

Example : *Synchronous Protocol These protocol involve timing information of sender along with the data bytes. This protocol helps receiver to remain synchronization with the sender. When the sender has no data to transmit, the sender transmits a sequence of alternating 0s sand 1s to maintain sender/receiver synchronization. This sequence of 0s and 1s is called idle flags. Data bytes are packaged into small chunks called packets including address fields and check-sums.*

23. ***Asynchronous Data Link Control (DLC) Protocols:*** *Asynchronous protocols are used primarily for low-speed data communications between PCs and very small computers. Framing occurs at the byte level, with each byte surrounded by a start bit (a 0 bit) and a*

stop bit (a 1 bit). A parity bit often accompanies each character as well.

Example **:** *Emails, forum comments, corporate intranet, and even Asana or Trello boards serve as examples of asynchronous communication we deal with every day.*

24. **Binary Synchronous Protocol (Bisync or BSC)** **:***Bisync was developed by IBM in 1966 as a character-oriented protocol that frames the data with control codes which apply to the entire set of data. Bisync organizes data into block of up to 512 characters.*

Example: *The receiving device independently calculates the BCC and compares the two calculations***.**

25. **HDLC :** *It can be used for point-to-multipoint connections via the original master-slave modes Normal Response Mode (NRM) and Asynchronous Response Mode (ARM).*

Example : *But they are now rarely used; it is now used almost exclusively to connect one device to another, using Asynchronous Balanced Mode (ABM).*

26. ***Point-to-Point Protocol (PPP):*** *It is a TCP/IP protocol that is used to connect one computer system to another.*

Example : *Computers use PPP to communicate over the telephone network or the Internet.*

27. ***Network Control Protocol (NCP):****It is a set of protocols forming a part of Point − to − Point Protocol (PPP). PPP is a data link layer protocol that is used to transmit multiprotocol data between two directly connected (point-to-point) computers.*

Example : *Post Office Protocol 3, or POP3.*

28. ***IPCP****: In computer networking, Internet Protocol Control Protocol (IPCP) is a Network Control Protocol (NCP) for establishing and configuring Internet Protocol over a Point-to-Point Protocol link. IPCP is responsible for configuring the IP addresses as well as for enabling and disabling the IP protocol modules on both ends of the point-to-point link*.

Example*: IPCP Configuration Options allow negotiatiation of desirable Internet Protocol parameters. IPCP uses the same Configuration Option format defined for LCP Link Control Protocol.*

29. ***LCP****: LCP is considered a data link layer protocol because it works at the data link layer (Layer 2) of* ***the Open System Interconnection networking reference model****.*

Example*: LCP is considered a data link layer protocol because it works at the data link layer (Layer 2) of the Open System Interconnection networking reference model.*

30. SNMP: Simple Network Management Protocol: *snmp is enables* *network admins to monitor network performance, identify network glitches, and troubleshoot them. SNMP protocol is comprised of three components: a managed device, an SNMP agent, and an SNMP manager.*

Example: *This protocol used to manage nodes, like servers, workstations, routers, switches, etc.,*