FUNDAMENTALS OF DATA COMMUNICATION AND NETWORKING:-

Communication is defined as a process in which more than one computer transfers information, instructions to each other and for sharing resources. Or in other words, communication is a process or act in which we can send or receive data. A network of computers is defined as an interconnected collection of autonomous computers. Autonomous means no computer can start, stop or control another computer.

Components of Data Communication

A communication system is made up of the following components:

1. **Message:** A message is a piece of information that is to be transmitted from one person to another. It could be a text file, an audio file, a video file, etc.
2. **Sender:** It is simply a device that sends data messages. It can be a computer, mobile, telephone, laptop, video camera, or workstation, etc.
3. **Receiver:** It is a device that receives messages. It can be a computer, telephone mobile, workstation, etc.
4. **Transmission Medium / Communication Channels:** Communication channels are the medium that connect two or more workstations. Workstations can be connected by either wired media or wireless media.
5. **Set of rules (Protocol):** When someone sends the data (The sender), it should be understandable to the receiver also otherwise it is meaningless. For example, Sonali sends a message to Chetan. If Sonali writes in Hindi and Chetan cannot understand Hindi, it is a meaningless conversation.

Therefore, there are some set of rules (protocols) that is followed by every computer connected to the internet and they are:

- **TCP(Transmission Control Protocol)**: It is responsible for dividing messages into packets on the source computer and reassembling the received packet at the destination or recipient computer. It also makes sure that the packets have the information about the source of the message data, the destination of the message data, the sequence in which the message data should be re-assembled, and checks if the message has been sent correctly to the specific destination.
- **IP(Internet Protocol)**: Do You ever wonder how computer determines which packet belongs to which device. What happens if the message you sent to your friend is received by your father? Scary Right. Well! IP is responsible for handling the address of the destination computer so that each packet is sent to its proper destination.

Type of data communication

As we know that data communication is communication in which we can send or receive data from one device to another. The data communication is divided into three types:

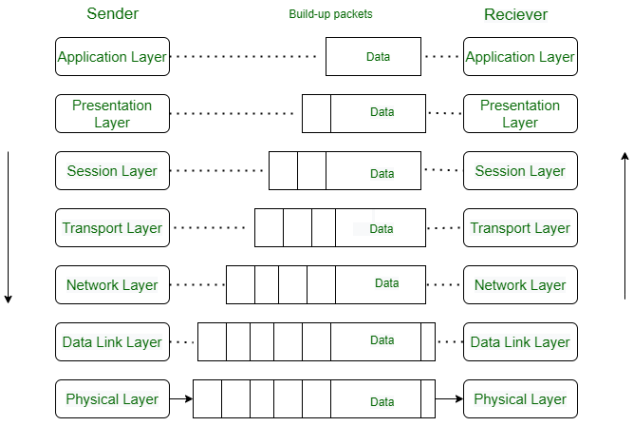
1. **Simplex Communication:** It is one-way communication or we can say that unidirectional communication in which one device only receives and another device only sends data and devices uses their entire capacity in transmission. For example, IoT, entering data using a keyboard, listing music using a speaker, etc.

2. **Half Duplex communication:** It is a two-way communication, or we can say that it is a bidirectional communication in which both the devices can send and receive data but not at the same time. When one device is sending data then another device is only receiving and vice-versa. For example, walkie-talkie.
3. **Full-duplex communication:** It is a two-way communication or we can say that it is a bidirectional communication in which both the devices can send and receive data at the same time. For example, mobile phones, landlines, etc.

NETWORK REFERENCE MODELS: OSI AND TCP/IP MODELS

What is OSI Model?

The OSI model, created in 1984 by ISO, is a reference framework that explains the process of transmitting data between computers. It is divided into seven layers that work together to carry out specialised network functions, allowing for a more systematic approach to networking.

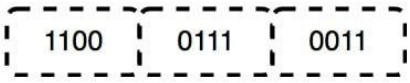


What are the 7 layers of the OSI Model?

The OSI model consists of seven abstraction layers arranged in a top-down order:
1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

Physical Layer – Layer 1

The lowest layer of the OSI reference model is the physical layer. It is responsible for the actual physical connection between the devices. The physical layer contains information in the form of **bits.** It is responsible for transmitting individual bits from one node to the next. When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.



Functions of the Physical Layer

- **Bit synchronization:** The physical layer provides the synchronization of the bits by providing a clock. This clock controls both sender and receiver thus providing synchronization at the bit level.
- **Bit rate control:** The Physical layer also defines the transmission rate i.e. the number of bits sent per second.
- **Physical topologies:** Physical layer specifies how the different, devices/nodes are arranged in a network i.e. bus, star, or mesh topology.
- **Transmission mode:** Physical layer also defines how the data flows between the two connected devices. The various transmission modes possible are Simplex, half-duplex and full-duplex.

Note:

1. *Hub, Repeater, Modem, and Cables are Physical Layer devices.*
2. *Network Layer, Data Link Layer, and Physical Layer are also known as* ***Lower Layers*** *or* ***Hardware Layers****.*

Data Link Layer (DLL) – Layer 2

The data link layer is responsible for the node-to-node delivery of the message. The main function of this layer is to make sure data transfer is error-free from one node to another, over the physical layer. When a packet arrives in a network, it is the responsibility of the DLL to transmit it to the Host using its MAC address.
The Data Link Layer is divided into two sublayers:

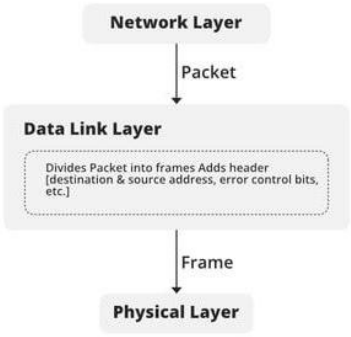
1. Logical Link Control (LLC)
2. Media Access Control (MAC)

The packet received from the Network layer is further divided into frames depending on the frame size of the NIC(Network Interface Card). DLL also encapsulates Sender and Receiver's MAC address in the header.
The Receiver's MAC address is obtained by placing an ARP(Address Resolution Protocol) request onto the wire asking "Who has that IP address?" and the destination host will reply with its MAC address.

Functions of the Data Link Layer

- **Framing:** Framing is a function of the data link layer. It provides a way for a sender to transmit a set of bits that are meaningful to the receiver. This can be accomplished by attaching special bit patterns to the beginning and end of the frame.
- **Physical addressing:** After creating frames, the Data link layer adds physical addresses (MAC addresses) of the sender and/or receiver in the header of each frame.
- **Error control:** The data link layer provides the mechanism of error control in which it detects and retransmits damaged or lost frames.
- **Flow Control:** The data rate must be constant on both sides else the data may get corrupted thus, flow control coordinates the amount of data that can be sent before receiving an acknowledgment.

- **Access control:** When a single communication channel is shared by multiple devices, the MAC sub-layer of the data link layer helps to determine which device has control over the channel at a given time.



Note:
1. *Packet in the Data Link layer is referred to as* ***Frame.***
2. *Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.*
3. *Switch & Bridge are Data Link Layer devices.*

Network Layer – Layer 3

The network layer works for the transmission of data from one host to the other located in different networks. It also takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available. The sender & receiver's IP addresses are placed in the header by the network layer.

Functions of the Network Layer

- **Routing:** The network layer protocols determine which route is suitable from source to destination. This function of the network layer is known as routing.
- **Logical Addressing:** To identify each device inter-network uniquely, the network layer defines an addressing scheme. The sender & receiver's IP addresses are placed in the header by the network layer. Such an address distinguishes each device uniquely and universally.

Note:
1. *Segment in the Network layer is referred to as* ***Packet****.*
2. *Network layer is implemented by networking devices such as routers and switches.*

Transport Layer – Layer 4

The transport layer provides services to the application layer and takes services from the network layer. The data in the transport layer is referred to as *Segments*. It is responsible for the end-to-end delivery of the complete message. The transport layer also provides the acknowledgment of the successful data transmission and re-transmits the data if an error is found.

At the sender's side: The transport layer receives the formatted data from the upper layers, performs **Segmentation**, and also implements **Flow and error control** to ensure proper data transmission. It also adds Source and Destination port numbers in its header and forwards the segmented data to the Network Layer.

Note: *The sender needs to know the port number associated with the receiver's application.*

Generally, this destination port number is configured, either by default or manually. For example, when a web application requests a web server, it typically uses port number 80, because this is the default port assigned to web applications. Many applications have default ports assigned.
At the receiver's side: *Transport Layer reads the port number from its header and forwards the Data which it has received to the respective application. It also performs sequencing and reassembling of the segmented data.*

Functions of the Transport Layer

- **Segmentation and Reassembly:** This layer accepts the message from the (session) layer, and breaks the message into smaller units. Each of the segments produced has a header associated with it. The transport layer at the destination station reassembles the message.
- **Service Point Addressing:** To deliver the message to the correct process, the transport layer header includes a type of address called service point address or port address. Thus by specifying this address, the transport layer makes sure that the message is delivered to the correct process.

Services Provided by Transport Layer

1. Connection-Oriented Service: It is a three-phase process that includes
- Connection Establishment
- Data Transfer
- Termination/disconnection

In this type of transmission, the receiving device sends an acknowledgment, back to the source after a packet or group of packets is received. This type of transmission is reliable and secure.
2. Connectionless service: It is a one-phase process and includes Data Transfer. In this type of transmission, the receiver does not acknowledge receipt of a packet. This approach allows for much faster communication between devices. Connection-oriented service is more reliable than connectionless Service.
Note:
1. *Data in the Transport Layer is called* ***Segments****.*
2. *Transport layer is operated by the Operating System. It is a part of the OS and communicates with the Application Layer by making system calls.*
3. *The transport layer is called as* ***Heart of the OSI*** *model.*
4. ***Device or Protocol Use :*** *TCP, UDP NetBIOS, PPTP*

Session Layer – Layer 5

This layer is responsible for the establishment of connection, maintenance of sessions, and authentication, and also ensures security.

Functions of the Session Layer

- **Session establishment, maintenance, and termination:** The layer allows the two processes to establish, use, and terminate a connection.
- **Synchronization:** This layer allows a process to add checkpoints that are considered synchronization points in the data. These synchronization points help to identify the error so

that the data is re-synchronized properly, and ends of the messages are not cut prematurely and data loss is avoided.
- **Dialog Controller:** The session layer allows two systems to start communication with each other in half-duplex or full-duplex.

Note:

1. *All the below 3 layers(including Session Layer) are integrated as a single layer in the TCP/IP model as the "Application Layer".*
2. *Implementation of these 3 layers is done by the network application itself. These are also known as* ***Upper Layers or Software Layers.***
3. ***Device or Protocol Use :*** *NetBIOS, PPTP.*

Presentation Layer – Layer 6

The presentation layer is also called the **Translation layer**. The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.

Functions of the Presentation Layer

- **Translation:** For example, ASCII to EBCDIC.
- **Encryption/ Decryption:** Data encryption translates the data into another form or code. The encrypted data is known as the ciphertext and the decrypted data is known as plain text. A key value is used for encrypting as well as decrypting data.
- **Compression:** Reduces the number of bits that need to be transmitted on the network.

Note: **Device or Protocol Use:** JPEG, MPEG, GIF

Application Layer – Layer 7

At the very top of the OSI Reference Model stack of layers, we find the Application layer which is implemented by the network applications. These applications produce the data to be transferred over the network. This layer also serves as a window for the application services to access the network and for displaying the received information to the user.

Example: Application – Browsers, Skype Messenger, etc.

Note: *1. The application Layer is also called Desktop Layer.*

2. ***Device or Protocol Use :*** *SMTP*

Functions of the Application Layer

The main functions of the application layer are given below.

- Network Virtual Terminal(NVT): It allows a user to log on to a remote host.
- File transfer access and management(FTAM): This application allows a user to access files in a remote host, retrieve files in a remote host, and manage or control files from a remote computer.
- Mail Services: Provide email service.
- Directory Services: This application provides distributed database sources and access for global information about various objects and services.

Note: *The OSI model acts as a reference model and is not implemented on the Internet because of its late invention. The current model being used is the TCP/IP model.*

Advantages of OSI Model

The OSI Model defines the communication of a computing system into 7 different layers. Its advantages include:

- It divides network communication into 7 layers which makes it easier to understand and troubleshoot.
- It standardizes network communications, as each layer has fixed functions and protocols.
- Diagnosing network problems is easier with the OSI model.
- It is easier to improve with advancements as each layer can get updates separately.

What is TCP/IP?

TCP/IP stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP is also used as a communications protocol in a private computer network -an intranet or extranet.

The entire IP suite -a set of rules and procedures -is commonly referred to as TCP/IP. TCP and IP are the two main protocols, though others are included in the suite. The TCP/IP protocol suite functions as an abstraction layer between internet applications and the routing and switching fabric.

TCP/IP specifies how data is exchanged over the internet by providing end-to-end communications that identify how it should be broken into packets, addressed, transmitted, routed and received at the destination. TCP/IP requires little central management and is designed to make networks reliable with the ability to recover automatically from the failure of any device on the network.

What is the Difference between TCP and IP?

TCP and IP are different protocols of Computer Networks. The basic difference between TCP (Transmission Control Protocol) and IP (Internet Protocol) is in the transmission of data. In simple words, IP finds the destination of the mail and TCP has the work to send and receive the mail. UDP is another protocol, which does not require IP to communicate with another computer. IP is required by only TCP. This is the basic difference between TCP and IP.

TCP/IP is a layered server architecture system in which each layer is defined according to a specific function to perform. All these four TCP IP layers work collaboratively to transmit the data from one layer to another.

- Application Layer
- Transport Layer
- Internet Layer
- Network Interface

Application Layer

Application layer interacts with an application program, which is the highest level of OSI model. The application layer is the OSI layer, which is closest to the end-user. It means the OSI application layer allows users to interact with other software application.

Application layer interacts with software applications to implement a communicating component. The interpretation of data by the application program is always outside the scope of the OSI model.

Example of the application layer is an application such as file transfer, email, remote login, etc.

The function of the Application Layers are

- Application-layer helps you to identify communication partners, determining resource availability, and synchronizing communication.
- It allows users to log on to a remote host
- This layer provides various e-mail services
- This application offers distributed database sources and access for global information about various objects and services.

Transport Layer

Transport layer builds on the network layer in order to provide data transport from a process on a source system machine to a process on a destination system. It is hosted using single or multiple networks, and also maintains the quality of service functions.

It determines how much data should be sent where and at what rate. This layer builds on the message which are received from the application layer. It helps ensure that data units are delivered error-free and in sequence.

Transport layer helps you to control the reliability of a link through flow control, error control, and segmentation or de-segmentation.

The transport layer also offers an acknowledgment of the successful data transmission and sends the next data in case no errors occurred. TCP is the best-known example of the transport layer.

Important functions of Transport Layers

- It divides the message received from the session layer into segments and numbers them to make a sequence.
- Transport layer makes sure that the message is delivered to the correct process on the destination machine.
- It also makes sure that the entire message arrives without any error else it should be retransmitted.

Internet Layer

An internet layer is a second layer of TCP/IP layes of the TCP/IP model. It is also known as a network layer. The main work of this layer is to send the packets from any network, and any computer still they reach the destination irrespective of the route they take.

The Internet layer offers the functional and procedural method for transferring variable length data sequences from one node to another with the help of various networks.

Message delivery at the network layer does not give any guaranteed to be reliable network layer protocol.

Layer-management protocols that belong to the network layer are:

1. Routing protocols
2. Multicast group management
3. Network-layer address assignment.

The Network Interface Layer

Network Interface Layer is this layer of the four-layer TCP/IP model. This layer is also called a network access layer. It helps you to defines details of how data should be sent using the network.

It also includes how bits should optically be signaled by hardware devices which directly interfaces with a network medium, like coaxial, optical, coaxial, fiber, or twisted-pair cables.

A network layer is a combination of the data line and defined in the article of OSI reference model. This layer defines how the data should be sent physically through the network. This layer is responsible for the transmission of the data between two devices on the same network.

Most Common TCP/IP Protocols

Some widely used most common TCP/IP protocol are:

TCP

Transmission Control Protocol is an internet protocol suite which breaks up the message into TCP Segments and reassembling them at the receiving side.

IP

An Internet Protocol address that is also known as an IP address is a numerical label. It is assigned to each device that is connected to a computer network which uses the IP for communication. Its routing function allows internetworking and essentially establishes the Internet. Combination of IP with a TCP allows developing a virtual connection between a destination and a source.

HTTP

The Hypertext Transfer Protocol is a foundation of the World Wide Web. It is used for transferring webpages and other such resources from the HTTP server or web server to the web client or the HTTP client. Whenever you use a web browser like Google Chrome or Firefox, you are using a web client. It helps HTTP to transfer web pages that you request from the remote servers.

SMTP

SMTP stands for Simple mail transfer protocol. This protocol supports the e-mail is known as a simple mail transfer protocol. This protocol helps you to send the data to another e-mail address.

SNMP

SNMP stands for Simple Network Management Protocol. It is a framework which is used for managing the devices on the internet by using the TCP/IP protocol.

DNS

DNS stands for Domain Name System. An IP address that is used to identify the connection of a host to the internet uniquely. However, users prefer to use names instead of addresses for that DNS.

TELNET

TELNET stands for Terminal Network. It establishes the connection between the local and remote computer. It established connection in such a manner that you can simulate your local system at the remote system.

FTP

FTP stands for File Transfer Protocol. It is a mostly used standard protocol for transmitting the files from one machine to another.

Advantages of the TCP/IP model

- It helps you to establish/set up a connection between different types of computers.
- It operates independently of the operating system.
- It supports many routing-protocols.
- It enables the internetworking between the organizations.
- TCP/IP model has a highly scalable client-server architecture.
- It can be operated independently.
- Supports a number of routing protocols.
- It can be used to establish a connection between two computers.

Disadvantages of the TCP/IP model

- TCP/IP is a complicated model to set up and manage.
- The shallow/overhead of TCP/IP is higher-than IPX (Internetwork Packet Exchange).
- In this, model the transport layer does not guarantee delivery of packets.
- Replacing protocol in TCP/IP is not easy.
- It has no clear separation from its services, interfaces, and protocols.

Differences between the OSI and TCP/IP model

OSI Model	TCP/IP model
It is developed by ISO (International Standard Organization)	It is developed by ARPANET (Advanced Research Project Agency Network).
OSI model provides a clear distinction between interfaces, services, and protocols.	TCP/IP doesn't have any clear distinguishing points between services, interfaces, and protocols.
OSI refers to Open Systems Interconnection.	TCP refers to Transmission Control Protocol.
OSI uses the network layer to define routing standards and protocols.	TCP/IP uses only the Internet layer.
OSI follows a vertical approach.	TCP/IP follows a horizontal approach.
OSI model use two separate layers physical and data link to define the functionality of the bottom layers.	TCP/IP uses only one layer (link).
OSI layers have seven layers.	TCP/IP has four layers.
OSI model, the transport layer is only connection-oriented.	A layer of the TCP/IP model is both connection-oriented and connectionless.
In the OSI model, the data link layer and physical are separate layers.	In TCP, physical and data link are both combined as a single host-to-network layer.
Session and presentation layers are not a part of the TCP model.	There is no session and presentation layer in TCP model.
It is defined after the advent of the Internet.	It is defined before the advent of the internet.
The minimum size of the OSI header is 5 bytes.	Minimum header size is 20 bytes.

What is TCP Three-Way HandShake?

Three-Way HandShake or a TCP 3-way handshake is a process which is used in a TCP/IP network to make a connection between the server and client. It is a three-step process that requires both the client and server to exchange synchronization and acknowledgment packets before the real data communication process starts.
Three-way handshake process is designed in such a way that both ends help you to initiate, negotiate, and separate TCP socket connections at the same time. It allows you to transfer multiple TCP socket connections in both directions at the same time.

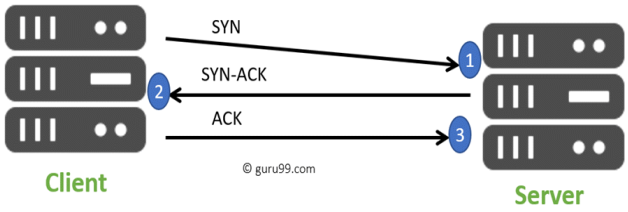
TCP message types

Message	Description
Syn	Used to initiate and establish a connection. It also helps you to synchronize sequence numbers between devices.

Message	Description
ACK	Helps to confirm to the other side that it has received the SYN.
SYN-ACK	SYN message from local device and ACK of the earlier packet.
FIN	Used to terminate a connection.

TCP Three-Way Handshake Process

TCP traffic begins with a three-way handshake. In this TCP handshake process, a client needs to initiate the conversation by requesting a communication session with the Server:



- **Step 1:** In the first step, the client establishes a connection with a server. It sends a segment with SYN and informs the server about the client should start communication, and with what should be its sequence number.
- **Step 2:** In this step server responds to the client request with SYN-ACK signal set. ACK helps you to signify the response of segment that is received and SYN signifies what sequence number it should able to start with the segments.
- **Step 3:** In this final step, the client acknowledges the response of the Server, and they both create a stable connection will begin the actual data transfer process.

CRYPTOGRAPHY:-

Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix “crypt” means “hidden” and suffix “graphy” means “writing”. In Cryptography the techniques which are use to protect information are obtained from mathematical concepts and a set of rule based calculations known as algorithms to convert messages in ways that make it hard to decode it. These algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on internet and to protect confidential transactions such as credit card and debit card transactions.

Techniques used For Cryptography: In today’s age of computers cryptography is often associated with the process where an ordinary plain text is converted to cipher text which is the text made such that intended receiver of the text can only decode it and hence this process is known as encryption. The process of conversion of cipher text to plain text this is known as decryption.

Features Of Cryptography are as follows:

1. **Confidentiality/Privacy:** Information can only be accessed by the person for whom it is intended and no other person except him can access it.
2. **Integrity/Reliability:** Information cannot be modified in storage or transition between sender and intended receiver without any addition to information being detected.
3. **Non-repudiation:** The sender should acknowledge he sent data and not deny it later after transmission.
   Authentication: The identities of sender and receiver are confirmed. As well as destination/origin of information is confirmed.

Encryption Terminology used in Cryptography

Following are some basic terminologies used in encryption:

- **Plain text:** This is the unencrypted message. It does not always need to be text; it can be photos, spreadsheets, or any other information form.
- **Ciphertext:** This is the encrypted information only for the intended individual. Nobody else should be able to access it.
- **Key:** When converting plain text to ciphertext, we use a magic string to encode-decode information. This is called the key. The Key is optional as long as the text has to encode. It can be of short length and can be reused iteratively. But if longer keys are used, security increases since they are challenging to crack.

Types Of Cryptography

In general there are three types Of cryptography:

1. **Symmetric Key Cryptography:** It is an encryption system where the sender and receiver of message use a single common key to encrypt and decrypt messages. Symmetric Key Systems are faster and simpler but the problem is that sender and receiver have to somehow exchange key in a secure manner. The most popular symmetric key cryptography system are Data Encryption System(DES) and Advanced Encryption System(AES).
2. **Hash Functions:** There is no usage of any key in this algorithm. A hash value with fixed length is calculated as per the plain text which makes it impossible for contents of plain text to be recovered. Many operating systems use hash functions to encrypt passwords.
3. **Asymmetric Key Cryptography:** Under this system a pair of keys is used to encrypt and decrypt information. A receiver's public key is used for encryption and a receiver's private key is used for decryption. Public key and Private Key are different. Even if the public key is known by everyone the intended receiver can only decode it because he alone know his private key. The most popular asymmetric key cryptography algorithm is RSA algorithm.

Cryptography tools and techniques

There are many tools and techniques for encoding and decoding data for security purposes. Some of the essential tools and techniques are:

- Secret key cryptography
- Public key cryptography
- Hybrid Cryptography
- Stream Cipher Algorithm
- Block Cipher Algorithm
- Hash Functions

Secret Key Cryptography

It is also known as Symmetric key cryptography. In this technique, the sender and receiver use a single shared key to encrypt and decrypt the information. The algorithms based on this technique are completely streamlined and thus fast in nature. The problem with this technique is that somehow the sender and the receiver have to exchange keys securely. A few types of symmetric cryptography are:

- DES(Data Encryption System)
- RC2
- IDEA
- Blowfish

Public Key Cryptography

It is also known as Asymmetric key cryptography. In this technique, the sender and receiver use a pair of keys to carry on the encryption and decryption of data. The pair of keys is the public key and the private key. For encryption, a public key is used, and a private decryption key is used. Each person stores a private key, and a public key is shared across the network. Even after everyone on the network knows the public key, they cannot decode it. Only the intended user with the private key can decrypt the message. Some of the widely used kinds of asymmetric key cryptography are:

- RSA
- DSA
- PKCs
- Elliptic Curve Technique

Hybrid Cryptography

To achieve advantages of both public and private key cryptographies and nullify or reduce their shortcomings, we use a new technique called hybrid cryptography, a combination of both.
Its working can be explained with an example, Assume that there are two ninjas, Ninja1 and Ninja2, and they want to communicate with secrecy, and the message is long. Since they have a long message, they can not use public-key cryptography because of their slow nature (that is why they are only used in short messages). Here they will use a combination of both. Ninja1 will choose a secret key and encrypt the message using a secret-key(fast) cryptosystem. Then he encrypts this secret key using Ninja2's public key. After which Ninja1 sends the ciphertext and the encrypted key to Ninja2. Ninja2 first uses his private decryption key to decrypt the secret key, and then he uses this secret key to decrypt the ciphertext.

Stream Cipher Algorithm

Stream Cipher algorithm is an algorithm that operates over a stream of information as it passes through the system. Since it can't look ahead, it must be able to keep up with the speed of incoming data. It first uses the key to construct the keystream, a bitstream of the same length as

plain text. The decoding part of this algorithm should be tolerant of missing bits of data. The most common example where these are used is the streaming of audio and video.

Block Cipher Algorithm

It is an algorithm that divides the data into blocks. For example, it divides 64 bits in an 8X8 matrix block and encodes it at once. So, we can define blocks as fixed-size chunks of plain text. Block ciphers are generally very secure and very fast too.

Hash Function

The hash function follows an algorithm that takes an arbitrary length of data input and delivers a fixed data output size. This algorithm does not comprise the usage of any keys. A hash value is calculated as per the plain text, which is fixed in size. This hash value makes it impossible to recover the contents of the plain text, thus making it secure. So, this hash function is used in Operating Systems to encrypt passwords.

Advantages

1. **Access Control:** Cryptography can be used for access control to ensure that only parties with the proper permissions have access to a resource. Only those with the correct decryption key can access the resource thanks to encryption.
2. **Secure Communication:** For secure online communication, cryptography is crucial. It offers secure mechanisms for transmitting private information like passwords, bank account numbers, and other sensitive data over the internet.
3. **Protection against attacks:** Cryptography aids in the defence against various types of assaults, including replay and man-in-the-middle attacks. It offers strategies for spotting and stopping these assaults.
4. **Compliance with legal requirements:** Cryptography can assist firms in meeting a variety of legal requirements, including data protection and privacy legislation.

TYPES OF HACKING

We can define hacking into different categories, based on what is being hacked. These are as follows:

1. **Network Hacking:** Network hacking means gathering information about a network with the intent to harm the network system and hamper its operations using the various tools like Telnet, NS lookup, Ping, Tracert, etc.
2. **Website hacking:** Website hacking means taking unauthorized access over a web server, database and make a change in the information.
3. **Computer hacking:** Computer hacking means unauthorized access to the Computer and steals the information from PC like Computer ID and password by applying hacking methods.
4. **Password hacking:** Password hacking is the process of recovering secret passwords from data that has been already stored in the computer system.

5. **Email hacking:** Email hacking means unauthorized access on an Email account and using it without the owner's permission.

CYBERCRIME

Cybercrime can be defined as “The illegal usage of any communication device to commit or facilitate in committing any illegal act”.
A cybercrime is explained as a type of crime that targets or uses a computer or a group of computers under one network for the purpose of harm.
Cybercrimes are committed using computers and computer networks. They can be targeting individuals, business groups, or even governments.

Who are The Cybercriminals?

A cybercriminal is a person who uses his skills in technology to do malicious acts and illegal activities known as cybercrimes. They can be individuals or teams.
Here are some examples of cybercriminals:
Black hat hackers
Cyberstalkers
Cyber terrorists
Scammers
Cybercriminals who conduct targeted attacks are better to be named Threat Actors.

How do Cybercrimes happen?

Cybercriminals take advantage of security holes and vulnerabilities found in systems and exploit them in order to take a foothold inside the targeted environment.
The security holes can be a form of using weak authentication methods and passwords, it can also happen for the lack of strict security models and policies.

Classifications of Cybercrimes

Cybercrimes in general can be classified into four categories:

1. Individual Cyber Crimes: This type is targeting individuals. It includes phishing, spoofing, spam, cyberstalking, and more.

2. Organisation Cyber Crimes: The main target here is organizations. Usually, this type of crime is done by teams of criminals including malware attacks and denial of service attacks.

3. Property Cybercrimes: This type targets property like credit cards or even intellectual property rights.

4. Society Cybercrimes: This is the most dangerous form of cybercrime as it includes cyber-terrorism.

Most Common Cyber Crimes

1. Phishing and Scam

Phishing is a type of social engineering attack that targets the user and tricks them by sending fake messages and emails to get sensitive information about the user or trying to download malicious software and exploit it on the target system.

2. Identity Theft

Identity theft occurs when a cybercriminal uses another person's personal data like credit card numbers or personal pictures without their permission to commit a fraud or a crime.

3. Ransomware Attack

Ransomware attacks are a very common type of cybercrime. It is a type of malware that has the capability to prevent users from accessing all of their personal data on the system by encrypting them and then asking for a ransom in order to give access to the encrypted data.

4. Hacking/Misusing Computer Networks

This term refers to the crime of unauthorized access to private computers or networks and misuse of it either by shutting it down or tampering with the data stored or other illegal approaches.

5. Internet Fraud

Internet fraud is a type of cybercrimes that makes use of the internet and it can be considered a general term that groups all of the crimes that happen over the internet like spam, banking frauds, theft of service, etc.

Other Types of Cybercrime

1. Cyber Bullying

It is also known as online or internet bullying. It includes sending or sharing harmful and humiliating content about someone else which causes embarrassment and can be a reason for the occurrence of psychological problems. It became very common lately, especially among teenagers.

2. Cyber Stalking

Cyberstalking can be defined as unwanted persistent content from someone targeting other individuals online with the aim of controlling and intimidating like unwanted continued calls and messages.

3. Software Piracy

Software piracy is the illegal use or copy of paid software with violation of copyrights or license restrictions.
Not only software can be pirated but also music, movies, or pictures.

4. Social Media Frauds

The use of social media fake accounts to perform any kind of harmful activities like impersonating other users or sending intimidating or threatening messages. And one of the easiest and most common social media frauds is Email spam.

5. Online Drug Trafficking

With the big rise of cryptocurrency technology, it became easy to transfer money in a secured private way and complete drug deals without drawing the attention of law enforcement. This led to a rise in drug marketing on the internet.

6. Electronic Money Laundering

Also known as transaction laundering. It is based on unknown companies or online business that makes approvable payment methods and credit card transactions but with incomplete or inconsistent payment information for buying unknown products.
It is by far one of the most common and easy money laundering methods.

CLASSIFICATION OF SECURITY ATTACKS

Active attacks:

Active attacks are a type of cybersecurity attack in which an attacker attempts to alter, destroy, or disrupt the normal operation of a system or network. Active attacks involve the attacker taking direct action against the target system or network, and can be more dangerous than passive attacks, which involve simply monitoring or eavesdropping on a system or network.
Types of active attacks are as follows:

- Masquerade
- Modification of messages
- Repudiation
- Replay
- Denial of Service

Masquerade –

Masquerade is a type of cybersecurity attack in which an attacker pretends to be someone else in order to gain access to systems or data. This can involve impersonating a legitimate user or system to trick other users or systems into providing sensitive information or granting access to restricted areas.
There are several types of masquerade attacks, including:

- **Username and password masquerade:** In a username and password masquerade attack, an attacker uses stolen or forged credentials to log into a system or application as a legitimate user.
- **IP address masquerade:** In an IP address masquerade attack, an attacker spoofs or forges their IP address to make it appear as though they are accessing a system or application from a trusted source.
- **Website masquerade:** In a website masquerade attack, an attacker creates a fake website that appears to be legitimate in order to trick users into providing sensitive information or downloading malware.

- **Email masquerade:** In an email masquerade attack, an attacker sends an email that appears to be from a trusted source, such as a bank or government agency, in order to trick the recipient into providing sensitive information or downloading malware.

Modification of messages –

It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorized effect. Modification is an attack on the integrity of the original data. It basically means that unauthorized parties not only gain access to data but also spoof the data by triggering denial-of-service attacks, such as altering transmitted data packets or flooding the network with fake data. Manufacturing is an attack on authentication. For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.

Repudiation –

Repudiation attacks are a type of cybersecurity attack in which an attacker attempts to deny or repudiate actions that they have taken, such as making a transaction or sending a message. These attacks can be a serious problem because they can make it difficult to track down the source of the attack or determine who is responsible for a particular action.
There are several types of repudiation attacks, including:

- **Message repudiation attacks:** In a message repudiation attack, an attacker sends a message and then later denies having sent it. This can be done by using spoofed or falsified headers or by exploiting vulnerabilities in the messaging system.
- **Transaction repudiation attacks:** In a transaction repudiation attack, an attacker makes a transaction, such as a financial transaction, and then later denies having made it. This can be done by exploiting vulnerabilities in the transaction processing system or by using stolen or falsified credentials.
- **Data repudiation attacks:** In a data repudiation attack, an attacker modifies or deletes data and then later denies having done so. This can be done by exploiting vulnerabilities in the data storage system or by using stolen or falsified credentials.

Replay –

It involves the passive capture of a message and its subsequent transmission to produce an authorized effect. In this attack, the basic aim of the attacker is to save a copy of the data originally present on that particular network and later on use this data for personal uses. Once the data is corrupted or leaked it is insecure and unsafe for the users.

Denial of Service –

Denial of Service (DoS) is a type of cybersecurity attack that is designed to make a system or network unavailable to its intended users by overwhelming it with traffic or requests. In a DoS attack, an attacker floods a target system or network with traffic or requests in order to consume its resources, such as bandwidth, CPU cycles, or memory, and prevent legitimate users from accessing it.
There are several types of DoS attacks, including:

- **Flood attacks:** In a flood attack, an attacker sends a large number of packets or requests to a target system or network in order to overwhelm its resources.

- **Amplification attacks:** In an amplification attack, an attacker uses a third-party system or network to amplify their attack traffic and direct it towards the target system or network, making the attack more effective.

Passive attacks:

A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission. The goal of the opponent is to obtain information that is being transmitted. Passive attacks involve an attacker passively monitoring or collecting data without altering or destroying it. Examples of passive attacks include eavesdropping, where an attacker listens in on network traffic to collect sensitive information, and sniffing, where an attacker captures and analyzes data packets to steal sensitive information.

Types of Passive attacks are as follows:

- The release of message content
- Traffic analysis

The release of message content –

Telephonic conversation, an electronic mail message, or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.

Traffic analysis –

Suppose that we had a way of masking (encryption) information, so that the attacker even if captured the message could not extract any information from the message. The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of the communication that was taking place. The most useful protection against traffic analysis is encryption of SIP traffic. To do this, an attacker would have to access the SIP proxy (or its call log) to determine who made the call.

Difference between Active Attack and Passive Attack:

Active Attack	Passive Attack
In an active attack, Modification in information takes place.	While in a passive attack, Modification in the information does not take place.
Active Attack is a danger to **Integrity** as well as **availability**.	Passive Attack is a danger to **Confidentiality**.
In an active attack, attention is on prevention.	While in passive attack attention is on detection.

Active Attack	Passive Attack
Due to active attacks, the execution system is always damaged.	While due to passive attack, there is no harm to the system.
In an active attack, Victim gets informed about the attack.	While in a passive attack, Victim does not get informed about the attack.
In an active attack, System resources can be changed.	While in passive attack, System resources are not changing.
Active attack influences the services of the system.	While in a passive attack, information and messages in the system or network are acquired.
In an active attack, information collected through passive attacks is used during execution.	While passive attacks are performed by collecting information such as passwords, and messages by themselves.
An active attack is tough to restrict from entering systems or networks.	Passive Attack is easy to prohibit in comparison to active attack.
Can be easily detected.	Very difficult to detect.
The purpose of an active attack is to harm the ecosystem.	The purpose of a passive attack is to learn about the ecosystem.
In an active attack, the original information is modified.	In passive attack original information is Unaffected.
The duration of an active attack is short.	The duration of a passive attack is long.
The prevention possibility of active attack is High	The prevention possibility of passive attack is low.
Complexity is High	Complexity is low.

ESSENTIAL TERMINOLOGY

Threat

A cyber threat is a malicious act that seeks to steal or damage data or discompose the digital network or system. Threats can also be defined as the possibility of a successful cyber attack to get access to the sensitive data of a system unethically. Examples of threats include computer viruses, Denial of Service (DoS) attacks, data breaches, and even sometimes dishonest employees.

Types of Threat

Threats could be of three types, which are as follows:

1. **Intentional**Malware, phishing, and accessing someone's account illegally, etc. are examples of intentional threats.
2. **Unintentional**Unintentional threats are considered human errors, for example, forgetting to update the firewall or the anti-virus could make the system more vulnerable.
3. **Natural**Natural disasters can also damage the data, they are known as natural threats.

Vulnerability:

In cybersecurity, a vulnerability is a flaw in a system's design, security procedures, internal controls, etc., that can be exploited by cybercriminals. In some very rare cases, cyber vulnerabilities are created as a result of cyberattacks, not because of network misconfigurations. Even it can be caused if any employee anyhow downloads a virus or a social engineering attack.

Types of Vulnerability

Vulnerabilities could be of many types, based on different criteria, some of them are:

1. **Network**Network vulnerability is caused when there are some flaws in the network's hardware or software.
2. **Operating system**When an operating system designer designs an operating system with a policy that grants every program/user to have full access to the computer, it allows viruses and malware to make changes on behalf of the administrator.
3. **Human**Users' negligence can cause vulnerabilities in the system.
4. **Process**Specific process control can also cause vulnerabilities in the system.

Risk:

Cyber risk is a potential consequence of the loss or damage of assets or data caused by a cyber threat. Risk can never be completely removed, but it can be managed to a level that satisfies an organization's tolerance for risk. So, our target is not to have a risk-free system, but to keep the risk as low as possible.
Cyber risks can be defined with this simple formula**Risk = Threat + Vulnerability**.
Cyber risks are generally determined by examining the threat actor and type of vulnerabilities that the system has.

Types of Risks

There are two types of cyber risks, which are as follows:

1. External External cyber risks are those which come from outside an organization, such as cyberattacks, phishing, ransomware, DDoS attacks, etc.
2. Internal Internal cyber risks come from insiders. These insiders could have malicious intent or are just not be properly trained.

Difference Between Threat, Vulnerability, and Risk

	Threat	Vulnerability	Risks
1.	Take advantage of vulnerabilities in the system and have the potential to steal and damage data.	Known as the weakness in hardware, software, or designs, which might allow cyber threats to happen.	The potential for loss or destruction of data is caused by cyber threats.
2.	Generally, can't be controlled.	Can be controlled.	Can be controlled.
3.	It may or may not be intentional.	Generally, unintentional.	Always intentional.
4.	Can be blocked by managing the vulnerabilities.	Vulnerability management is a process of identifying the problems, then categorizing them, prioritizing them, and resolving the vulnerabilities in that order.	Reducing data transfers, downloading files from reliable sources, updating the software regularly, hiring a professional cybersecurity team to monitor data, developing an incident management plan, etc. help to lower down the possibility of cyber risks.
5.	Can be detected by anti-virus software and threat detection logs.	Can be detected by penetration testing hardware and many vulnerability scanners.	Can be detected by identifying mysterious emails, suspicious pop-ups, observing unusual password activities, a slower than normal network, etc.

Attacks:-

An attack or cyber attack in the context of cybersecurity refers to a malicious or unauthorized action taken by an individual, group, or automated system to compromise, disrupt, or gain unauthorized access to computer systems, networks, data, or services. These actions are often intended to cause harm, steal sensitive information, or exploit vulnerabilities for various purposes such as financial gain, espionage, activism, or sabotage.

Classification Based on Targets:

Web-based Attacks:

Definition: Web-based attacks target vulnerabilities in web applications, websites, or web servers. Attackers exploit weaknesses in web technologies, protocols, or configurations to gain unauthorized access, steal data, or disrupt services.

Examples:

SQL Injection (SQLi): Attackers inject malicious SQL commands into input fields to manipulate databases and extract sensitive information.

Cross-Site Scripting (XSS): Attackers inject malicious scripts into web pages viewed by other users, allowing them to steal session cookies or execute unauthorized actions on behalf of users.

Distributed Denial-of-Service (DDoS): Attackers flood a web server with excessive traffic or requests, making it unavailable to legitimate users.

Impact: Web-based attacks can lead to data breaches, website defacement, service disruption, financial losses, and reputational damage.

System-based Attacks:

Definition: System-based attacks target computer systems, networks, or devices directly. Attackers exploit vulnerabilities in operating systems, software, or network configurations to gain unauthorized access, install malware, or compromise data integrity.

Examples:

Malware Infections: Viruses, worms, Trojans, and ransomware are forms of malware that infiltrate systems to steal data, disrupt operations, or extort money.

Unauthorized Access (Hacking): Attackers exploit weak passwords, misconfigured systems, or software vulnerabilities to gain unauthorized access to systems or networks.

Privilege Escalation: Attackers exploit security weaknesses to elevate their privileges and gain higher levels of access than intended.

Impact: System-based attacks can result in data breaches, system downtime, financial losses, intellectual property theft, and regulatory penalties.

Classification Based on Methods:

Active Attack: Active attacks aim to manipulate system resources or impact their operation.

Passive Attack: Passive attacks aim to extract sensitive information from a system without affecting its resources.

Active Attacks:

Definition: Active attacks involve actions that directly affect the target system or network. Attackers execute malicious activities such as injecting code, exploiting vulnerabilities, or launching denial-of-service attacks.

Examples:

Malware Injections: Attackers inject malicious code into systems to steal data, spy on users, or control infected devices.

Exploiting Vulnerabilities: Attackers exploit software vulnerabilities (e.g., unpatched software, zero-day exploits) to gain unauthorized access or execute malicious actions.

Denial-of-Service (DoS) Attacks: Attackers flood target systems or networks with excessive traffic or requests, disrupting services or making them unavailable.

Impact: Active attacks can cause system disruptions, data loss, financial damages, and reputational harm to organizations and individuals.

Passive Attacks:

Definition: Passive attacks involve monitoring and eavesdropping on network communications to gather sensitive information without altering the data. Attackers intercept and analyze data packets to extract confidential information.

Examples:

Sniffing Attacks: Attackers use network sniffers to capture and analyze data packets transmitted over a network, potentially revealing usernames, passwords, or other sensitive information.

Traffic Analysis: Attackers analyze patterns and volumes of network traffic to infer user behavior, identify vulnerabilities, or target specific data.

Impact: Passive attacks can lead to data leaks, privacy breaches, identity theft, and unauthorized access to confidential information.

Types of Cyberattacks:

Malware attacks: These involve malicious software designed to infiltrate, damage, or control computer systems. Examples include viruses, worms, Trojans, and ransomware.

Phishing attacks: These involve deceiving users into providing sensitive information such as login credentials, credit card numbers, or personal data. Phishing can occur via email, text messages, or fake websites.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks: These aim to make a system or network unavailable by overwhelming it with excessive traffic or requests. DDoS attacks are coordinated and more powerful, often involving multiple compromised devices.

Man-in-the-Middle (MitM) attacks: These involve intercepting and manipulating communication between two parties without their knowledge. The attacker can eavesdrop, modify, or inject malicious content into the communication.

SQL injection: This is a type of web-based attack targeting databases by injecting malicious SQL code into input fields, allowing attackers to access, modify, or delete data.

Cross-Site Scripting (XSS): This is a web-based attack where attackers inject malicious scripts into web pages viewed by other users, allowing them to steal session cookies, redirect users, or deface websites.

Brute-force attacks: These involve attempting multiple combinations of usernames and passwords to gain unauthorized access to accounts or systems.

Social engineering attacks: These exploit human psychology to manipulate individuals into divulging confidential information, performing actions, or compromising security measures.

Exploits:-

Definition:

- An exploit in cybersecurity refers to a specific type of cyber attack that takes advantage of vulnerabilities, bugs, or weaknesses in computer systems, software applications, or networks.
- It is a malicious technique used by attackers to gain unauthorized access, execute arbitrary code, or perform other malicious activities on a targeted system.

Types of Exploits:

1. **Known Exploits:**
   - These are vulnerabilities in software or systems that are publicly known and documented.
   - Once a vulnerability becomes known, software vendors typically release patches to fix the issue and make the exploit unusable.
   - Security vendors also receive information about known exploits to develop protections and detection mechanisms.
   - Organizations such as CERT/CC, CVE, and others maintain lists of known vulnerabilities with unique identification numbers, descriptions, and references.
2. **Unknown (Zero-Day) Exploits:**
   - Zero-day exploits are vulnerabilities that are not known to the software vendor or the public until they are actively exploited by attackers.
   - These exploits are developed and used by cybercriminals or state-sponsored actors before the vendor becomes aware of the vulnerability.
   - Zero-day exploits are highly dangerous because systems are vulnerable without any available patches or protections.
   - Detection of zero-day exploits often occurs when a hacker is observed exploiting the vulnerability, leading to the term "zero-day" as there are zero days of awareness before an attack.
   - Once a zero-day exploit is detected, vendors work to develop patches to correct the vulnerability, and security software may detect and block the exploit and associated malware.

In summary, known exploits are vulnerabilities that are publicly known and can be patched or protected against, while zero-day exploits are vulnerabilities that are exploited before they are known or patched, making them highly dangerous and challenging to defend against until mitigations are developed.

3. **Software Exploits:** These exploits target vulnerabilities in software applications or operating systems. Attackers exploit these vulnerabilities by writing and deploying malicious code that takes advantage of the software weaknesses.
4. **Hardware Exploits:** These exploits target vulnerabilities in computer hardware components such as processors, memory, or firmware. They can be more difficult to detect and mitigate compared to software exploits.

5. **Network Exploits:** These exploits target vulnerabilities in network protocols or services. Attackers exploit weaknesses in network configurations or protocols to gain unauthorized access or launch attacks.

Common Exploits:

1. **Buffer Overflow:** This is a type of software exploit where attackers overwhelm a program's buffer with more data than it can handle, leading to unexpected behavior and potential execution of malicious code.
2. **SQL Injection (SQLi):** This is a web-based exploit targeting databases by injecting malicious SQL code into input fields, allowing attackers to manipulate databases and steal data.
3. **Cross-Site Scripting (XSS):** This is another web-based exploit where attackers inject malicious scripts into web pages viewed by other users, enabling them to steal information or perform unauthorized actions.
4. **Zero-Day Exploits:** These exploits target vulnerabilities that are not yet known to the software vendor or have not been patched. Attackers use zero-day exploits to launch attacks before security patches are available.

Impact of Exploits:

- Exploits can have serious consequences, including data breaches, system compromise, financial losses, reputation damage, and disruption of services.
- They can be used by cybercriminals, hackers, or state-sponsored actors for various purposes such as stealing sensitive information, spreading malware, conducting espionage, or sabotaging systems.

Defense Against Exploits:

- To defend against exploits, organizations and individuals should regularly update software, apply security patches, use firewalls, intrusion detection systems, antivirus software, and practice secure coding practices.
- Security awareness training and conducting regular security assessments (such as vulnerability scanning and penetration testing) are also recommended to identify and mitigate vulnerabilities before they can be exploited.

Difference between Vulnerability and Exploit:

S.No	Vulnerability	Exploit
1.	Vulnerability is a weakness in a system that can be exploited.	Exploit is a tool that can be used to take advantage of a vulnerability.
2.	Vulnerabilities can exist without being exploited.	Exploits are created through the use of vulnerabilities.
3.	Vulnerabilities can be exploited for a	Exploits are often used to execute

S.No	Vulnerability	Exploit
	variety of purposes.	malicious code.
4.	Vulnerabilities can remain open and potentially exploitable.	Exploits are often patched by software vendors once they are made public.
5.	Vulnerability can allow the attacker to manipulate the system	Exploits take the form of software or code which helps us to take control of computers and steal network data
6.	Vulnerability can cause by complexity, connectivity, poor password management, Operating system flaws, Software Bugs, etc.	Exploits are designed to provide super user-level access to a computer system.

Difference between Threat and Attack

Threat	Attack
Threats can be intentional or unintentional.	The attack is intentional.
Threats may or may not be malicious.	The attack is malicious.
Circumstances that can cause damage.	The objective is to cause damage.
Information may or may not be altered or damaged.	The chance for information alteration and damage is very high.
The threat is comparatively hard to detect.	Comparatively easy to detect.
Can be blocked by control of vulnerabilities.	Cannot be blocked by just controlling the vulnerabilities.
Can be initiated by the system itself as well as by outsiders.	An attack is always initiated by an outsider (system or user).
Can be classified into Physical, internal, external, human, and non-physical threatsats.	These can be classified into Viruses, Spyware, Phishing, Worms, Spam, Botnets, DoS attacks, Ransomware, and

Threat	Attack
	Breaches.

CYBER TERRORISM

Cyber terrorism (also known as digital terrorism) is defined as disruptive attacks by recognised terrorist organisations against computer systems with the intent of generating alarm, panic, or the physical disruption of the information system.

The internet can be used by terrorists to finance their operations, train other terrorists, and plan terror attacks. The more mainstream idea of cyber terrorism is the hacking of government or private servers to access sensitive information or even siphon funds for use in terror activities. However, there is currently no universally accepted definition of cyber terrorism.

MALWARE

Malware — or malicious software — is any program or code that is created with the intent to do harm to a computer, network or server. Malware is the most common type of cyberattack, mostly because this term encompasses many subsets such as ransomware, trojans, spyware, viruses, worms, keyloggers, bots, cryptojacking, and any other type of malware attack that leverages software in a malicious way.

Type	Description
Ransomware	In a ransomware attack, an adversary encrypts a victim's data and offers to provide a decryption key in exchange for a payment. Ransomware attacks are usually launched through malicious links delivered via phishing emails, but unpatched vulnerabilities and policy misconfigurations are used as well.
Viruses	A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.
Spyware	Spyware is a type of unwanted, malicious software that infects a computer or other device and collects information about a user's web activity without their knowledge or consent.

Type	Description
Adware	Adware is a type of spyware that watches a user's online activity in order to determine which ads to show them. While adware is not inherently malicious, it has an impact on the performance of a user's device and degrades the user experience.
Trojan	A trojan is malware that appears to be legitimate software disguised as native operating system programs or harmless files like free downloads. Trojans are installed through social engineering techniques such as phishing or bait websites. The zeus trojan malware, a variant, has the goal accessing financial information and adding machines to a botnet.
Worms	A worm is a self-contained program that replicates itself and spreads its copies to other computers. A worm may infect its target through a software vulnerability or it may be delivered via phishing or smishing. Embedded worms can modify and delete files, inject more malicious software, or replicate in place until the targeted system runs out of resources.
Exploits	An exploit is a piece of software or data that opportunistically uses a defect in an operating system or an app to provide access to unauthorized actors. The exploit may be used to install more malware or steal data.
Keylogger	Keyloggers are tools that record what a person types on a device. While there are legitimate and legal uses for keyloggers, many uses are malicious. In a keylogger attack, the keylogger software records every keystroke on the victim's device and sends it to the attacker.
Botnet	Botnet is a network of computers infected with malware that are controlled by a bot herder. The bot herder is the person who operates the botnet infrastructure and uses the compromised computers to launch attacks designed to crash a target's network, inject malware, harvest credentials or execute CPU-intensive tasks.
MALSPAM	Malicious malware (MALSPAM) delivers malware as the malicious payload via emails containing malicious content, such as virus or malware infected attachments.

TYPE OF COMPUTER VIRUSES

File Virus:

This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called a **Parasitic virus** because it leaves no file intact but also leaves the host functional.

Boot sector Virus:

It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded. It infects other bootable media like floppy disks. These are also known as **memory viruses** as they do not infect the file systems.

Macro Virus:

Unlike most viruses which are written in a low-level language(like C or assembly language), these are written in a high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, the macro viruses can be contained in spreadsheet files.

Email Virus:

An email virus is a hidden malicious program sent via email that activates upon opening attachments or clicking infected links. It can damage the user's system, spread to other systems through the victim's address book, and be used to launch spam attacks, overwhelming servers. These viruses often come as executable files with extensions like .exe, .pdf, .dot, .com, .xls, or .scr, and they're crafted to evade user detection.

Multi-variant Virus:

A multi-variant virus in cybersecurity refers to a type of malware that exists in multiple versions or variations, each designed to evade detection by security systems. These variations may include changes in code structure, behavior, encryption keys, or other characteristics, making the virus more difficult to detect and mitigate.

Source code Virus:

It looks for source code and modifies it to include virus and to help spread it.

Polymorphic Virus:

A **virus signature** is a pattern that can identify a virus(a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The functionality of the virus remains the same but its signature is changed.

Encrypted Virus:

In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes.

Browser Hijacker:

As the name suggests this virus is coded to target the user's browser and can alter the browser settings. It is also called the browser redirect virus because it redirects your browser to other malicious sites that can harm your computer system.

Direct Action Virus:

The main perspective of this virus is to replicate and take action when it is executed. When a particular condition is met the virus will get into action and infect files in the directory that are specified in the AUTOEXEC.BAT file path.

Type of Virus	Description
Boot Sector Virus	Attacks the part of the computer that starts up when you turn it on. Boot Sector Virus can also spread through devices like **floppy disks**. Often called **a memory virus.**
File Virus	Attaches to the **end of a file** and **modifies** how a program starts to **run the virus's code first.**
Email Virus	Hides in email messages and activates by **clicking a link**, **opening an attachment**, or **interacting with the email.**
Polymorphic Virus	Changes its form every time it **installs to avoid detection** by antivirus software.
Macro Virus	Activates by running a program capable of executing macros, often found in documents like spreadsheets.
Multipartite Virus	Infects the **computer's boot sector**, **memory,** and **files,** making **it difficult to detect and remove.**
Encrypted Virus	Uses encryption to hide from **antivirus software**, includes a **decryption algorithm** to run before executing.
Stealth Virus	**Modifies detection code**, making it very difficult to detect.
Resident Virus	Saves itself in the computer's memory and can infect other files even

Type of Virus	Description
	after the original program stops.
Direct Action Virus	Tied to an executable file, it activates when the file is opened but does not **delete files** or **affect system speed**; **blocks file access.**
Browser Hijacker Virus	**Changes browser settings** without permission, can **redirect to malicious sites.**

The first virus for MS-DOS, called “Brain,” appeared in 1986.

SOME INDICATIONS OF A MALWARE ATTACKS

1. **Sluggish Performance:** If your device suddenly starts running slower than usual, it could be a sign of malware consuming system resources.
2. **Pop-up Ads:** Constant pop-up ads appearing on your device, especially when you're not using a web browser, may indicate malware.
3. **Unexplained Data Usage:** Malware often communicates with remote servers, leading to increased data usage that you can't account for.
4. **Strange Behavior:** If your device starts behaving oddly, like apps crashing frequently or settings changing without your input, malware could be the culprit.
5. **Unwanted Programs:** If you notice unfamiliar apps or programs installed on your device without your knowledge, they might be malicious.
6. **Battery Drain:** Malware running in the background can cause excessive battery drain, even when you're not actively using your device.
7. **Security Warnings:** Messages or notifications about security issues, especially from unfamiliar sources, could indicate a malware attack.
8. **Unusual Network Activity:** Monitoring your network traffic can reveal if there's unusual or suspicious activity that might be linked to malware.
9. **Missing Files:** Malware sometimes deletes or hides files on your device, so if you notice files missing without explanation, it's a red flag.
10. **Ransom Demands:** In extreme cases, ransomware will lock your device or encrypt your files, demanding payment for their release.

DIFFERENCE BETWEEN ANTIVIRUS AND ANTIMALWARE

Antivirus	Antimalware
Antivirus is a software program that	Antimalware is a software program that protects the

Antivirus	Antimalware
protects the computer system from viruses.	computer systems from all malware i.e. viruses, trojans, worms, etc.
Antivirus does not update its rules frequently.	Antimalware updates its rules frequently so that malware detection is easy.
Antivirus protects from predictable danger.	Antimalware protects from unpredictable danger.
Antivirus is comparatively less costly.	Antimalware It is more costly.

DENIAL OF SERVICE –

Denial of Service (DoS) is a type of cybersecurity attack that is designed to make a system or network unavailable to its intended users by overwhelming it with traffic or requests. In a DoS attack, an attacker floods a target system or network with traffic or requests in order to consume its resources, such as bandwidth, CPU cycles, or memory, and prevent legitimate users from accessing it.
There are several types of DoS attacks, including:

- **Flood attacks:** In a flood attack, an attacker sends a large number of packets or requests to a target system or network in order to overwhelm its resources.
- **Amplification attacks:** In an amplification attack, an attacker uses a third-party system or network to amplify their attack traffic and direct it towards the target system or network, making the attack more effective.

To prevent DoS attacks, organizations can implement several measures, such as:

- Using firewalls and intrusion detection systems to monitor network traffic and block suspicious activity.
- Limiting the number of requests or connections that can be made to a system or network.
- Using load balancers and distributed systems to distribute traffic across multiple servers or networks.
- Implementing network segmentation and access controls to limit the impact of a DoS attack.

DDOS(DISTRIBUTED DENIAL OF SERVICE)

A DDoS attack uses multiple servers and Internet connections to flood the targeted resource. A DDoS attack is one of the most powerful weapons on the cyber platform. When you come to know about a website being brought down, it generally means it has become a victim of a DDoS attack. This means that the hackers have attacked your website or PC by imposing heavy traffic. Thus, crashing the website or computer due to overloading.

Types of DDoS attacks:

1. Volumetric Attacks:

- Most common DDoS attack type.
- Overloads the network/server with heavy traffic, exceeding processing capabilities.
- Leads to network bandwidth loss and denial of service.

2. Protocol Attacks:

- Exploit TCP connection vulnerabilities (three-way handshake).
- Prevent handshake completion, leaving ports busy and unavailable.
- Overwhelms server with multiple requests, shutting down services.

3. Application Attacks:

- Target victim applications at Layer 7 (application layer).
- Slow, appear as legitimate user requests initially.
- Victim becomes unable to respond, threatening as they are harder to detect.

4. Fragmentation Attacks:

- Exploit datagram fragmentation process vulnerabilities.
- Divide IP datagrams into smaller packets, then reassemble.
- Fake data packets make reassembly impossible, disrupting communication.

How do DDoS Attacks Work?

The logic of a DDoS attack is very simple, although attacks can be highly different from each other. Network connections consist of various layers of the OSI model. Various types of DDoS attacks focus on particular layers. Examples are illustrated below:

Layer-3: Network layer – Attacks are known as Smurf Attacks, ICMP Floods, and IP/ICMP Fragmentation.

Layer-4: Transport layer – Attacks include SYN Floods, UDP Floods, and TCP Connection Exhaustion.

Layer-7: Application layer – HTTP-encrypted attacks.

1. What is a DoS attack?

DoS Stands for Denial of service attack. This attack is meant to shut down a machine or network, due to which users are unable to access it. DoS attacks accomplish this by flooding the target with traffic or sending it information that triggers a crash.

2. What is a DDoS attack?

DDoS Stands for Distributed Denial of service attack. In a DDoS attack, the attacker tries to make a particular service unavailable by directing continuous and huge traffic from multiple end systems.

3. What are the different types of DoS attacks?

Types of DOS Attacks are:

Buffer overflow attacks

Ping of Death or ICMP flood

Teardrop Attack

Flooding Attack

1. DOS Attack is a denial of service attack, in this attack a computer sends a massive amount of traffic to a victim's computer and shuts it down. Dos attack is an online attack that is used to make the website unavailable for its users when done on a website. This attack makes the server of a website that is connected to the internet by sending a large number of traffic to it.

2. DDOS Attack means distributed denial of service in this attack dos attacks are done from many different locations using many systems.

Difference between DOS and DDOS attacks:

DOS	DDOS
DOS Stands for Denial of service attack.	DDOS Stands for Distributed Denial of service attack.
In Dos attack single system targets the victim system.	In DDoS multiple systems attacks the victims system..
Victim PC is loaded from the packet of data sent from a single location.	Victim PC is loaded from the packet of data sent from Multiple location.
Dos attack is slower as compared to DDoS.	DDoS attack is faster than Dos Attack.
Can be blocked easily as only one system is used.	It is difficult to block this attack as multiple devices are sending packets and attacking from multiple locations.
In DOS Attack only single device is used with DOS Attack tools.	In DDoS attack,The volumeBots are used to attack at the same time.

DOS	DDOS
DOS Attacks are Easy to trace.	DDOS Attacks are Difficult to trace.
Volume of traffic in the Dos attack is less as compared to DDos.	DDoS attacks allow the attacker to send massive volumes of traffic to the victim network.
Types of DOS Attacks are: 1. Buffer overflow attacks 2. Ping of Death or ICMP flood 3. Teardrop Attack 4. Flooding Attack	Types of DDOS Attacks are: 1. Volumetric Attacks 2. Fragmentation Attacks 3. Application Layer Attacks 4. Protocol Attack.

INTRUSION DETECTION SYSTEM

Definition of IDS:

- An Intrusion Detection System (IDS) is a security tool that actively monitors network or system traffic for suspicious activities, policy violations, or potential cyber threats.
- It operates by analyzing incoming and outgoing data packets, looking for patterns or behaviors that deviate from established norms or indicate malicious intent.
- IDS aims to detect and alert administrators to potential security incidents, providing early warning and facilitating timely response and mitigation efforts.

Working of Intrusion Detection System(IDS)

- An IDS (Intrusion Detection System) monitors the traffic on a computer network to detect any suspicious activity.
- It analyzes the data flowing through the network to look for patterns and signs of abnormal behavior.
- The IDS compares the network activity to a set of predefined rules and patterns to identify any activity that might indicate an attack or intrusion.
- If the IDS detects something that matches one of these rules or patterns, it sends an alert to the system administrator.
- The system administrator can then investigate the alert and take action to prevent any damage or further intrusion.

Classification of IDS:

1. Network Intrusion Detection System (NIDS):

- NIDS monitors network traffic at strategic points within the network infrastructure, such as routers, switches, or dedicated appliances.
- It analyzes data packets traversing the network segment, looking for signs of malicious activity, unauthorized access attempts, or abnormal traffic patterns.

2. Host Intrusion Detection System (HIDS):

- HIDS operates on individual host machines or devices, monitoring activities and events specific to the host's operating system, applications, and services.
- It tracks system calls, file integrity, logins, process activities, and other host-related events to detect unauthorized changes, malware infections, or suspicious behaviors.

3. Protocol-based Intrusion Detection System (PIDS):

- PIDS focuses on monitoring and analyzing specific network protocols, such as HTTP, HTTPS, FTP, SMTP, etc., for signs of malicious or abnormal protocol usage.
- It inspects protocol headers, payloads, and interactions between clients and servers to detect anomalies, protocol violations, or potential attacks targeting specific protocols.

4. Application Protocol-based Intrusion Detection System (APIDS):

- APIDS is specialized in monitoring and securing application-specific protocols and interactions, such as database communications (e.g., SQL), middleware communications, or custom application protocols.
- It understands the semantics of application-level protocols, detecting unauthorized data accesses, injection attacks, or abnormal application behaviors.

5. Hybrid Intrusion Detection System:

- Hybrid IDS combines multiple detection approaches (e.g., NIDS, HIDS, PIDS, APIDS) to provide a comprehensive and layered defense strategy.
- By integrating host-based and network-based monitoring, along with protocol-specific or application-specific analysis, hybrid IDS offers a more holistic view of the network environment and enhances detection capabilities.

Detection Methods of IDS:

1. Signature-based Method:

- Signature-based IDS relies on predefined signatures or patterns of known attacks, malware, or malicious behaviors.
- It compares network traffic, system activities, or file contents against a database of signatures, triggering alerts when matches are found.
- While effective against known threats, signature-based IDS may struggle with detecting new or evolving threats for which signatures are not yet available.

2. Anomaly-based Method:

- Anomaly-based IDS establishes a baseline of normal behavior by monitoring network traffic, system activities, or user behaviors over time.
- It uses statistical analysis, machine learning algorithms, or heuristic techniques to identify deviations or anomalies from the established baseline.

- Anomaly-based IDS is particularly useful for detecting unknown or zero-day attacks, as it focuses on detecting unusual or suspicious activities that do not conform to typical patterns or behaviors.

INTRUSION PREVENTION SYSTEM

- IPS, also known as Intrusion Detection and Prevention System (IDPS), is a network security application.
- It monitors network or system activities for malicious behavior, identifies threats, collects information, and attempts to block or stop attacks.
- IPS is an enhancement of Intrusion Detection Systems (IDS), providing real-time response capabilities.
- It records events, notifies administrators, produces reports, and uses response techniques to prevent attacks.
- Response techniques include blocking malicious traffic, changing security settings, or altering attack content.

How Does an IPS Work?

An IPS works by analyzing network traffic in real-time and comparing it against known attack patterns and signatures. When the system detects suspicious traffic, it blocks it from entering the network.

Types of IPS

- **Network-Based IPS:** A Network-Based IPS is installed at the network perimeter and monitors all traffic that enters and exits the network.
- **Host-Based IPS:** A Host-Based IPS is installed on individual hosts and monitors the traffic that goes in and out of that host.

Classification of Intrusion Prevention System (IPS):

Intrusion Prevention System (IPS) is classified into 4 types:

- **Network-based intrusion prevention system (NIPS):** It monitors the entire network for suspicious traffic by analyzing protocol activity.
- **Wireless intrusion prevention system (WIPS):** It monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.
- **Network behavior analysis (NBA):** It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.
- **Host-based intrusion prevention system (HIPS):** It is an inbuilt software package which operates a single host for doubtful activity by scanning events that occur within that host.

Detection Method of Intrusion Prevention System (IPS):

- **Signature-based detection:** Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.
- **Statistical anomaly-based detection:** Anomaly based IDS monitors network traffic and compares it against an established baseline. The baseline will identify what is normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured.
- **Stateful protocol analysis detection:** This IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.

Comparison of IPS with IDS:

The main difference between Intrusion Prevention System (IPS) with Intrusion Detection Systems (IDS) are:

- Intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.
- IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
- IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.
- When IDS detects intrusion it only alerts network administration while Intrusion Prevention System(IPS) blocks the malicious packets before it reaches to destination.

IDS vs. IPS

Most organizations have either an IDS or an IPS, and many have both as part of their security information and event management framework.

	IDS	IPS
NAME	Intrusion detection system	Intrusion prevention system
DESCRIPTION	A system that monitors network traffic for suspicious activity and alerts users when such activity is discovered.	A system that monitors network traffic and alerts for suspicious activity, like an IDS, but also takes preventative action against suspicious activity.
LOCATION	A host-based intrusion detection system is installed on the client computer. A network-based intrusion detection system resides on the network.	Located between a company's firewall and the rest of its network.
USE	Warns of suspicious activity taking place, but it doesn't prevent it.	Warns of suspicious activity taking place and prevents it.
FALSE POSITIVE	IDS false positives are usually just a minor inconvenience. Although the IDS incorrectly labels legitimate traffic as malicious, it does not prevent the traffic from entering the network.	IPS false positives can be more serious. When an IPS mistakes legitimate traffic for a threat, it stops the legitimate traffic from entering the network, which could impact any part of the organization, not just the IT team.

SNOOPING

- Snooping, in a security context, is unauthorized access to another person's or company's data. The practice is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission.

- Snooping refers to unauthorized access to someone else's data.
- It can involve casually observing or actively monitoring data on a computer or network.
- Examples include watching someone type, using keyloggers to capture keystrokes and passwords, and monitoring communications data.
- Keyloggers are software programs that capture keystrokes, including sensitive information like passwords and login details.
- Snooping can be used maliciously by hackers for identity theft or accessing protected resources.
- Some companies also use snooping tools to monitor employees' computer and internet usage for productivity and security reasons.
- The rise of remote work has led to increased use of remote snooping tools by employers.

Different types of electronic snooping methods and tools

Although snooping has a negative connotation in general, in computer technology, snooping can refer to any program or utility that performs a monitoring function. Thus, the types of snooping methods and tools can vary widely, including the following:

- keylogger
- man-in-the-middle network snooping
- packet capture or sniffer
- employee performance monitoring
- telephone wiretaps
- audio/video surveillance

What is the difference between snooping and spoofing?

The terms *snooping* and *spoofing* are often used interchangeably. However, this is incorrect. Snooping is a form of eavesdropping with the purpose of learning information that is not intended to be visible or shared. Spoofing, on the other hand, is a method used to make an electronic device or network look like it is a trusted source. A spoofed device is used to gain the trust of a remote device, user or service so that it can freely share information. While the two terms are used to refer to activities to gain unauthorized access to information, they use different tactics to accomplish that goal.

How to prevent electronic snooping attacks

There are several methods users can practice to help reduce the chance of electronic snooping. Some common examples are the following:

- Avoid using public Wi-Fi networks.
- Use secure Wi-Fi authentication techniques.

- Conduct rogue Wi-Fi access point searches.
- Keep antivirus software updated.
- Use strong passwords, and change them frequently.
- Use encryption when transmitting and storing sensitive data.
- Know your surroundings, and turn computer screens away from surveillance cameras.
- Deploy network monitoring and prevention tools, such as firewalls, virtual private networks (VPNs) and anti-Address Resolution Protocol/domain name system spoofing services.
- Segment networks so that secure communications flow through specific portions of the network that can be better protected from spoofing attacks.

EAVESDROPPING ATTACK:

An eavesdropping attack, also known as a wiretapping or listening attack, is a popular cyberattack in networking. In this attack, **an attacker intercepts and listens to communications between two parties without their knowledge or consent.**

An eavesdropping attack can be performed by physically tapping into a communication line or wire. Additionally, the attackers can use specialized software or hardware to intercept as well as decode wireless communication.

Eavesdropping attacks are a big threat to the integrity and confidentiality of the data. It allows an attacker to gather sensitive information, such as login credentials, financial data, or personal conversations, without the victim's knowledge. Furthermore, attackers can use the extracted information for various malicious purposes, such as identity theft, extortion, or espionage.

Eavesdropping can be passive or active:

- **Passive eavesdropping** — A hacker detects the information by listening to the message transmission in the network.
- **Active eavesdropping** — A hacker actively grabs the information by disguising himself as friendly unit and by sending queries to transmitters. This is called probing, scanning or tampering.

** Data encryption is the best countermeasure for eavesdropping.*

General Steps to Launch an Eavesdropping Attack:

- Identify target and gather information about communication systems and vulnerabilities.
- Choose an attack method (e.g., intercepting unsecured networks, using malware, hardware devices).
- Execute chosen method, intercept communication, analyze and extract valuable information.

Variants of Eavesdropping Attacks:

- **Man-in-the-middle (MITM):** Intercepts and relays messages between parties, altering communication.

- **Sniffing:** Captures and decodes wireless communication to gather information or gain unauthorized access.
- **Physical wiretapping:** Taps into communication lines to intercept messages.
- **Eavesdropping on public Wi-Fi:** Intercepts communication on unencrypted public Wi-Fi networks.
- **Malware-based eavesdropping:** Uses malware to intercept and transmit sensitive information.

Prevention Techniques:

- **Encryption:** Uses algorithms like AES and RSA to encrypt communication, making it difficult for attackers to intercept.
- **Virtual Private Networks (VPNs):** Creates secure, encrypted connections to prevent interception.
- **Secure communication protocols (e.g., HTTPS, SFTP, SSH):** Uses encryption and security measures to protect communication.
- **Firewalls:** Controls network traffic to prevent unauthorized access.
- **Network segmentation:** Divides networks into isolated segments to prevent access to sensitive information.
- Educating employees and users about risks and secure communication methods.

KEYLOGGER (KEYSTROKE LOGGER OR SYSTEM MONITOR)

A keylogger, sometimes called a keystroke logger, is a type of surveillance technology used to monitor and record each keystroke on a specific device, such as a computer or smartphone. It can be either hardwareor software-based. The latter type is also known as system monitoring software or keyboard capture software.

Why are keyloggers used?

Keyloggers are often used as a spyware tool by cybercriminals to steal personally identifiable information, login credentials and sensitive enterprise data.

That said, some uses of keyloggers could be considered ethical or appropriate in varying degrees. For instance, keyloggers can also be used for the following reasons:

- By employers to observe employees' computer activities.
- By parents to supervise their children's internet usage.
- By device owners to track possible unauthorized activity on their devices.
- By law enforcement agencies to analyze incidents involving computer use.

Types of keyloggers:

1. **Hardware-based Keyloggers:**
   - Small devices that connect between the keyboard and computer.
   - They are designed to blend in with regular computer cabling, making them easy to hide.
   - Require physical access to the computer for installation.
2. **Software-based Keyloggers:**
   - Don't require physical access and can be downloaded purposefully or through malware.
   - Two main types:
     - **User mode keyloggers:** Use Windows API to intercept keyboard and mouse movements, requiring active monitoring by the attacker.
     - **Kernel mode keyloggers:** Work with higher privileges, are more complex, and can modify the internal Windows system through the kernel.

** Some keylogging software can also perform additional actions like running other applications, injecting malicious scripts, or memory injection.*

FIREWALL

A firewall is a tool that monitors incoming and outgoing network traffic and can detect and prevent suspicious packets of data on the basis of predefined rules, letting only genuine traffic gain entry into your private network. The most basic way to add additional security between a system and malicious attacks is to install a firewall.

You can use firewalls in both business and home settings. They are an essential part of network security. Most operating systems include a basic firewall. Using a third-party firewall application, on the other hand, provides better protection.

Different types of firewalls

There are many different types of firewalls, depending on their operation. Some of the most common firewalls are:

Packet filtering firewalls

Packet filtering firewalls are the most traditional type of network layer firewall. A static firewall is another name for this firewall. This firewall monitors incoming and outgoing packets and allows them to pass or fail based on the source and destination IP addresses, ports, and protocols. Packet filtering firewalls are quick, inexpensive, and effective. However, the security they offer is fundamental. Because these firewalls cannot analyze the content of data packets, they cannot protect against malicious data packets originating from trusted source IPs.

Some of the benefits and drawbacks of this type of firewall are:

Advantages	Drawbacks
Low resource consumption	IP spoofing is possible

More affordable	There is no user authentication
Filtering headers is quick and efficient	There is no payload.

Stateful inspection firewalls

You can use this type of firewall to control how data packets pass through a firewall. These firewalls can determine whether a packet belongs to a specific session or not. It only allows communication if the session between two endpoints is perfectly established; otherwise, it will block communication. Even though these security requirements offer advanced security, they consume many system resources and can significantly slow down traffic. As a result, they are vulnerable to DoS attacks. This kind of firewall is also known as dynamic packet filtering.

Some of the benefits and drawbacks of this type of firewall are:

Advantages	**Drawbacks**
It records the entire session	It takes a lot of resources.
Examines packet headers and payloads	There is no user authentication support
Provides more control	DoS attacks are possible

Circuit-level gateways

A circuit-level gateways firewall operates at the OSI model's session layer, monitoring TCP (Transmission Control Protocol) connections and sessions. Their foremost objective is to guarantee the safety of the established connections. Circuit-level gateways are inexpensive, simple, and have little impact on network performance. Their incapability to check the content of data packets, however, renders them an insufficient security solution on their own. A data packet containing malware can easily avoid a circuit-level gateway if it has a valid TCP handshake.

Some of the benefits and drawbacks of this type of firewall are:

Advantages	**Drawbacks**
Cost-efficient	There is no content filtering
Avoid exposing your address	There is no application layer security
Examine TCP handshakes	Requires software modifications

Proxy firewalls

You must use a proxy device to implement a proxy firewall, also known as an application-level gateway. Instead of an outsider directly accessing your internal network, the proxy server intercepts the message whenever a client requests to connect to a web page. The proxy transmits the message to the web server while posing as the client. This conceals the client's location and identity, cloaking them from any restrictions or possible threats.

Some of the benefits and drawbacks of this type of firewall are:

Advantages	**Drawbacks**
Protects client data such as geolocation	Performance may suffer
Maintain user anonymity	Not all network protocols are supported
Protects against various attacks	Additional configuration is required to ensure

	overall encryption

Next-generation firewalls

A next-generation firewall goes beyond the capabilities of a traditional, stateful firewall. A traditional firewall typically provides stateful inspection of incoming and outgoing network traffic; however, a next-generation firewall includes features such as integrated prevention systems, application awareness and control, and cloud-delivered threat intelligence.

Some of the benefits and drawbacks of this type of firewall are:

Advantages	**Drawbacks**
Deep inspection is integrated	Requires a lot of system resources
Upgrades happen automatically	Expensive in comparison to other options
Keep track of network traffic from Layer 2 to Layer 7	Integration with existing security management systems may necessitate additional configuration.

Software firewall

A software firewall protects our computers. If you have multiple devices, you must install the software on each one. Because it must be compatible with the host, you must configure it individually for each. This type of firewall can safeguard our system against external threats such as unauthorized access, malicious attacks, etc. The firewall alerts you to the danger of opening a specific email or attempting to access an insecure website.

Some of the benefits and drawbacks of this type of firewall are:

Advantages	**Drawbacks**
Simple to set up or reconfigure	Requires a lot of system resources
Suitable for personal or domestic use	Not suitable for situations where response times are critical
Less expensive in comparison to other options	It can be challenging to remove or uninstall a software firewall completely

Hardware firewall

A hardware firewall is a physical piece of equipment that filters traffic to and from a computer, similar to a server. Usually, a network cable is plugged directly into a computer or server, but with a hardware firewall, the cord is connected directly into the firewall first. This firewall inspects outbound and inbound network traffic because all network links pass through it. As a result, access controls and other security policies are enforced. This is also known as an Appliance Firewall.

Some of the benefits and drawbacks of this type of firewall are:

Advantages	**Drawbacks**
Allows for faster response times	More expensive than a software firewall
Can handle increased traffic loads	Installation is difficult
Less vulnerable to attacks	Upgrading is quite difficult

Cloud firewall

These firewalls can control the flow of information between external domains and your internal system. A cloud firewall, as opposed to traditional firewalls, filters data at the cloud level. These firewalls helps to combat today's advanced threats and safeguard your operation's data.

Some of the benefits and drawbacks of this type of firewall are:

Advantages	Drawbacks
Simple to deploy and scale as needed	Expensive in comparison to other options
There is no hardware involved	The availability is contingent on the availability of the cloud infrastructure
In the event of an issue, you can take snapshots and quickly recover to the desired state	Operating enhanced security features can cause the network to slow down

---

BOTS

Bots are automated software programs that conduct internet-based tasks. They can be developed for a variety of objectives, both good and bad. Search engines utilize good bots, such as web crawlers, to index web pages. Malicious bots, on the hand, are designed to do destructive tasks such as propagating malware, stealing, or initiating assaults.

Features

- Bots are automated software programs that can do activities without the need for human involvement, saving time and effort.
- **Efficiency:** Bots can do jobs faster than humans, enhancing efficiency in a variety of activities.
- **Scalability:** Bots can easily be expanded to do enormous volumes of activities at the same time, making them ideal for repetitive or high-volume processes.
- **Accuracy:** Bots are trained to execute tasks precisely, reducing mistakes that can occur when humans are involved.

Advantages

- **Increased Productivity:** Bots may automate repetitive and monotonous work, freeing up people to focus on more difficult and strategic duties, resulting in increased overall productivity.
- **Savings:** By automating operations, bots can minimize labour costs associated with manual execution, particularly for jobs that take a long time or involve huge amounts of data.
- **Time Efficiency:** Bots can execute jobs significantly faster than humans, allowing for speedier reaction times and increased efficiency in a variety of processes.
- Bots conduct jobs consistently, adhering to present rules and processes, and are not impacted by factors like as weariness or emotions, which can lead to deviations in human execution.

Disadvantages

- **Lack of Adaptability:** Bots are programmed to do certain activities according to predetermined rules. They may struggle with activities that need adaptation or complicated decision-making in response to changing conditions.
- **Programming Dependence:** Bots are constrained to the capabilities and limits established during programming. Without human interaction, they may be unable to manage unforeseen events or tasks outside of their predefined scope.
- Bots have the potential to be used maliciously, such as propagating malware, participating in fraudulent operations, executing cyberattacks, and providing security hazards to persons and organizations.
- **Impersonal Interactions:** Interacting with bots can often lack the human touch and personalisation that clients need, thus harming user experience and satisfaction.

BOTNETS

Botnets are infected computer networks, often known as zombies or bots. These machines have been infected with malware, allowing a botmaster to remotely control them. The botmaster has the ability to send orders to the botnet and coordinate their activities for different nefarious activities. Botnets are frequently used in distributed denial-of-service (DDoS) assaults, spam email distribution, cryptocurrency mining, and other types of cybercrime.

Features

- Botnets are controlled by a centralized command and control (C&C) server or a botmaster. This enables the botmaster to send orders to the whole botnet at the same time.
- Botnets may grow in size from a few hacked computers to millions of infected devices throughout the world. This vast network gives enormous power and resources for conducting coordinated strikes.
- Botnets are built to be durable and avoid discovery or disruption. To make it difficult for security measures to detect and neutralise them, they frequently use tactics like as encryption, peer-to-peer communication, and frequent changes in C&C servers.

Advantages

- Botnets allow fraudsters to undertake coordinated assaults using a large number of compromised devices. This gives them a lot of computational power and bandwidth, which they may use to launch distributed denial-of-service (DDoS) assaults, overwhelm target servers, and disrupt internet services.
- Botnets may be used to send spam emails or to carry out phishing campaigns. Botnets may produce and distribute a large amount of malicious emails by sharing the workload over numerous hacked machines, boosting the spread of malware, or duping victims into disclosing critical information.

Disadvantages

- Botnets are mostly employed for nefarious purposes, inflicting harm to individuals, businesses, and organizations. These actions range from service disruption to financial losses, data breaches, and privacy violations.
- Most jurisdictions make it unlawful to create, control, or use botnets. If detected and punished, engaging in such actions can result in serious legal repercussions, including fines and jail.

ZOMBIES

Individual machines infected with malware and controlled by a botmaster within a botnet are referred to as zombies in the context of cybersecurity. These infected machines might have been hacked by visiting malicious websites, opening infected email attachments, or falling prey to social engineering assaults. When a computer is infected, it becomes a member of the botnet and may be used to carry out harmful operations.

Features

- **Compromised State:** Computers that have been compromised by malware, which often acquires control of the system without the user's knowledge or agreement, are referred to as zombies.
- **Remote Control:** Once infected, zombies are placed under the command and control of a botmaster, who may remotely manipulate and use their resources for a variety of malevolent purposes.
- **Unwanted Activities:** Zombies can be used to perform distributed denial-of-service (DDoS) assaults, disseminate malware or spam, conduct phishing campaigns, and participate in botnet-driven criminality.
- **Silent Operation:** Zombies frequently remain dormant or function silently in the background, undetected by the user. This enables the botmaster to maintain control of them discretely and carry out destructive acts unnoticed.

Advantages

- Botnets may leverage the combined power of a large number of hacked machines, allowing for more effective coordinated assaults.
- Botnets may quickly grow by infecting more machines, giving a greater pool of resources for various cybercriminal actions.
- Botnets provide the botmaster with some anonymity because their orders are routed across several infected machines, making it difficult to pinpoint the source.
- Botnets can be built with redundant command and control (C&C) infrastructure, allowing them to survive even if some nodes are destroyed or hacked.

Disadvantages

- Botnet construction, control, and usage are all unlawful. Botnet-related acts can result in serious legal penalties.
- Botnets are typically used for nefarious purposes, such as initiating DDoS attacks, spreading malware, stealing personal information, or sending spam emails, all of which cause harm to persons, organisations, and networks.
- Infected systems within a botnet endure diminished performance as a result of the botnet's increased processing and network resources. This can cause system slowdowns, instability, and hardware damage.
- Botnets represent substantial security dangers to people and organisations alike. They can exploit computer weaknesses, resulting in data breaches, financial loss, and reputational harm.

Difference between Bots, Botnets, and Zombies

Point of Comparison	Bots	Botnets	Zombies
Definition	Automated software programs	Networks of infected computers	Malware infiltrated individual computers
Purpose	Perform automatic chores, whether good or bad.	Controlled by a central command server	A botmaster controls it remotely.
Communication	It is possible to communicate with a command server.	Inter-botnet communication	N/A – Avoid communicating within a network.
Infection Method	Infected by malware or social engineering techniques	Malware infection, followed by replication via a self-propagation or command and control servers	Infected by malware or other techniques of exploitation
Botmaster/Bot Herder	Controls and manages the bots	Controls and commands the botnet	N/A – No central control
Size	Individual instances	The number of people might range from a few to millions.	Individual instances within a botnet
Persistence	It is possible that it will remain on the system until it is deleted.	Remains connected to the botnet may.	May remain on the system until removed.
Botnet Size and Reach	Individual bot	Can span globally	N/A – A single infected computer
Examples	Web crawlers, chatbots	Mirai, Zeus, Necurs, Emotet, Conficker	Infected computers used in DDoS attacks,

			spamming, etc.

WEB APPLICATION BASED THREATS

SQL Injection

A SQL injection attack is executed when an attacker injects malicious code into an application's database through user input fields. These types of attacks can accomplish many different things. Two of the most common outcomes include allowing the attacker to gain unauthorized access to sensitive data stored in the database. Depending on what data the database is storing, the attack could get access to passwords, financial information, and personal data. The second outcome could be the manipulation or deletion of data. For instance, a user may be able to execute a **DROP TABLE** or **DROP DATABASE** command.

You can mitigate this with the following steps:

- Validate user input.
- Use output encoding, which involves converting special characters such as < and > into their HTML entity equivalents, to prevent them from being interpreted as HTML code.
- Use prepared statements, parameterized queries, or stored procedures instead of dynamic SQL whenever possible.

Most languages and frameworks have recommended ways of handling form input. By combing frontend and backend standards to prevent SQL injection from happening, your application can increase its security against this type of threat.

SQL Injection Attacks

- SQL injection attacks use a series of malicious SQL queries to directly manipulate the database.
- An attacker can use a vulnerable web application to bypass normal security measures and obtain direct access to the valuable data.
- SQL injection attacks can often be executed from the address bar, from within application fields, and through queries and searches.

Cross-Site Scripting (XSS)

Cross-site scripting (XSS) attacks involve injecting malicious code or a malicious script into a website. The website then executes the script, allowing the attacker to steal sensitive user data, like session tokens and cookies, or perform other actions.

There are two main types of XSS attacks: reflective and stored. Reflective XSS attacks involve injecting malicious code into a website that is immediately executed. Stored XSS attacks involve injecting malicious code into a website that is stored and executed at a later time.

If successful, a cross-site scripting attack can result in the theft of user session IDs, website defacement, and redirection to malicious sites, thereby enabling phishing attacks.

You can mitigate this with the following steps:

- Validate user input.
- Use output encoding techniques.
- Use auto-sanitization libraries such as OWASP AntiSamy.
- Implement a content security policy.

Similar to the recommendation for SQL injection, using modern web frameworks generally tends to steer developers towards secure coding practices to avoid XSS and similar attacks.

Cross-Site Request Forgery (CSRF)

Cross-site request forgery (CSRF) is a type of attack that involves tricking a victim into performing an action on a website without their knowledge. This can be done by injecting a malicious link or form into a website that the victim is already authenticated on.

When the victim clicks the link or submits the form, the action is performed on their behalf, potentially leading to data loss or unauthorized access.

You can mitigate this with the following steps:

- Leverage CSRF protections already built into the framework you are using, if applicable.
- Use CSRF tokens. These are unique, randomized values associated with a user's session and are included in forms and links to verify the authenticity of the request.
- Use SameSite cookies. These are a type of cookie that is only sent with requests to the same origin as the cookie's creation. This can help prevent attackers from being able to send requests on behalf of a victim, as they would not have access to the victim's SameSite cookies.

Drive-by attack

- Drive-by download attacks are a standard method of spreading malware. Hackers search for insecure websites and plant a malicious script into HTTP or PHP code on one among the pages. This script might install malware directly onto the pc of somebody who visits the site, or it'd re-direct the victim to a site controlled by the hackers. Drive-by downloads can happen when visiting a website or viewing an email message or a pop-up window. Unlike many other types of cyber security attacks, a drive-by doesn't rely on a user to do anything to actively enable the attack — you don't need to click a download button or open a malicious email attachment to become infected. A drive-by download can cash in of an app, operating system or web browser that contains security flaws thanks to unsuccessful updates or lack of updates.
- To protect yourself from drive-by attacks, you would like to stay your browsers and operating systems up to date and avoid websites which may contain malicious code. stick with the sites you normally use — although keep in mind that even these sites are often hacked. Don't keep too many unnecessary programs and apps on your device. The more plug-ins you have, the more vulnerabilities there are which will be exploited by drive-by attacks.

Command Injection

Command injection is an attack in which the goal is execution of arbitrary commands on the host operating system via a vulnerable application. Command injection attacks are possible when an

application passes unsafe user supplied data (forms, cookies, HTTP headers etc.) to a system shell. In this attack, the attacker-supplied operating system commands are usually executed with the privileges of the vulnerable application. Command injection attacks are possible largely due to insufficient input validation.

This attack differs from Code Injection, in that code injection allows the attacker to add their own code that is then executed by the application. In Command Injection, the attacker extends the default functionality of the application, which execute system commands, without the necessity of injecting code.

Code Injection vs. Command Injection

Code injection is a generic term for any type of attack that involves an injection of code interpreted/executed by an application. This type of attack takes advantage of mishandling of untrusted data inputs. It is made possible by a lack of proper input/output data validation.

A key limitation of code injection attacks is that they are confined to the application or system they target. If an attacker can inject PHP code into an application and execute it, malicious code will be limited by PHP functionality and permissions granted to PHP on the host machine.

Command injection typically involves executing commands in a system shell or other parts of the environment. The attacker extends the default functionality of a vulnerable application, causing it to pass commands to the system shell, without needing to inject malicious code. In many cases, command injection gives the attacker greater control over the target system.

Command Injection Attacks

- **Shell Injection**:
  - An attacker tries to craft an input string to gain shell access to a web server.
  - Shell Injection functions include system(), StarProcess(), java.lang.Runtime.exec(), System.Diagnostics.Process.Start(), and similar APIs.
- **HTML Embedding**:
  - This type of attack is used to deface websites virtually. Using this attack, an attacker adds an extra HTML-based content to the vulnerable web application.
  - In HTML embedding attacks, user input to a web script is placed into the output HTML, without being checked for HTML code or scripting.
- **File Injection**:
  - The attacker exploits this vulnerability and injects malicious code into system files.

Command Injection Example

1. An attacker enters malicious code (account number) with a new password.
2. The last two sets of numbers are the banner size.
3. Once the attacker clicks the submit button, the password for the account 1036 is changed to "newpassword".
4. The server script assumes that only the URL of the banner image file is inserted into that field.
5. Poor input validation at server script was exploited in this attack that uses database INSERT and UPDATE record command.

Directory Traversal

Directory traversal, also known as path traversal or directory climbing, is a vulnerability in a web application server caused by a HTTP exploit.

The exploit allows an attacker to access restricted directories, execute commands, and view data outside of the web root folder where application content is stored.

By manipulating input parameters or file paths, an attacker can navigate through the file system and gain unauthorized access to sensitive files or directories.

How Does Directory Traversal Work?

Directory traversal attacks manipulate variables that reference file paths within web applications. The attacker modifies the path variables to move upwards in the directory structure or to traverse to different directories. This is typically done using specific sequences like `../` or `..\` in Unix and Windows systems, respectively.

An attacker might use the sequences in a URL or input field in an attempt to trick the server into returning a file from outside of the document's root directory.

Example: `http://website.com/../../etc/passwd`

Requesting a URL like the example above attempts to have the server return a sensitive system file.

Attacks stemming from directory traversal can be damaging if they're used to display system files or download sensitive information. It can allow an attacker to view, edit, or execute arbitrary files on the server's file system, leading to a potential compromise of the server.

What are the Risks of Directory Traversal?

Directory traversal poses three significant threats to the security and integrity of web servers and applications:

- Directory traversal can lead to unauthorized access of sensitive information stored in files outside of the web root directory. This could include: system files, configuration files, or even user data. The unauthorized access of confidential data is a direct breach of privacy and can lead to information theft.
- Attackers can read and also modify or delete critical files, causing serious system malfunctions or service disruptions. This can lead to significant downtime, loss of productivity, and even financial loss.
- Successful directory traversal attacks can provide attackers with the ability to carry out damaging attacks. For instance, gaining access to certain system files can provide valuable information about the server's structure, configuration, and the security measures that are in place. Taken together, this is information that can be used to construct more sophisticated attacks in the future.

Buffer Overflow

Buffer overflow is a software coding error or vulnerability that can be exploited by hackers to gain unauthorized access to corporate systems.

Also known as a buffer overrun, buffer overflow occurs when the amount of data in the buffer exceeds its storage capacity. That extra data overflows into adjacent memory locations and corrupts or overwrites the data in those locations.

What Is a Buffer Overflow Attack?

A buffer overflow attack takes place when an attacker manipulates the coding error to carry out malicious actions and compromise the affected system. The attacker alters the application's execution path and overwrites elements of its memory, which amends the program's execution path to damage existing files or expose data.

Buffer Overflow Consequences:

Impact: System crashes, loss of access control, exploitation of other vulnerabilities, and potential security service subversion.

Types of Buffer Overflow Attacks:

- **Stack-based:** Overwriting stack data, including return pointers, to control program flow.
- **Heap-based:** Flooding memory space beyond current operations, more complex than stack-based attacks.
- **Format string:** Exploiting input data processing to execute code, read stack data, or cause application faults.

Phishing

Phishing is a type of cyberattack that uses email, SMS, phone, social media, and social engineering techniques to entice a victim to share sensitive information — such as passwords or account numbers — or to download a malicious file that will install viruses on their computer or phone.

Common phishing attacks include:

Type	Description
Spear Phishing	Spear-phishing is a type of phishing attack that targets specific individuals or organizations typically through malicious emails. The goal of spear phishing is to steal sensitive information such as login credentials or infect the targets' device with malware.
Whaling	A whaling attack is a type of social engineering attack specifically targeting senior or C-level executive employees with the purpose of stealing money or information, or gaining access to the person's computer in order to execute further cyberattacks.
SMiShing	Smishing is the act of sending fraudulent text messages designed to trick individuals into sharing sensitive data such as passwords, usernames and credit card numbers. A smishing attack may involve cybercriminals pretending to be your bank or a shipping service you use.

Type	Description
Vishing	Vishing, a voice phishing attack, is the fraudulent use of phone calls and voice messages pretending to be from a reputable organization to convince individuals to reveal private information such as bank details and passwords.

Spoofing

Spoofing is a technique through which a cybercriminal disguises themselves as a known or trusted source. In so doing, the adversary is able to engage with the target and access their systems or devices with the ultimate goal of stealing information, extorting money or installing malware or other harmful software on the device.

Spoofing can take different forms, which include:

Type	Description
Domain Spoofing	Domain spoofing is a form of phishing where an attacker impersonates a known business or person with fake website or email domain to fool people into the trusting them. Typically, the domain appears to be legitimate at first glance, but a closer look will reveal subtle differences.
Email Spoofing	Email spoofing is a type of cyberattack that targets businesses by using emails with forged sender addresses. Because the recipient trusts the alleged sender, they are more likely to open the email and interact with its contents, such as a malicious link or attachment.
ARP Spoofing	Address Resolution Protocol (ARP) spoofing or ARP poisoning is a form of spoofing attack that hackers use to intercept data. A hacker commits an ARP spoofing attack by tricking one device into sending messages to the hacker instead of the intended recipient. This way, the hacker gains access to your device's communications, including sensitive data.

WIRELESS NETWORK

Wireless networking uses radio frequency connections to connect network nodes. This type of networking enables devices to connect to the network while roaming within its coverage area. Wireless networks are a famous home, business, and telecommunications network solution.
Wireless networking is a more cost-effective and affordable way to set up an Internet network system. It is because there is no need for a cable, allowing all family members to use their devices in any house area. And with wireless networking, you can connect other devices to the network in seconds.

Wired and wireless networks differ mainly because of a single aspect. And that distinction is that wired networks use cables to connect devices, such as laptops, computers, mobiles, etc., to the Internet.

Examples of Wireless Networking

Wireless networking is an essential part of today's communications, and its new forms will be a central part of robots, drones, self-driving cars, and other emerging technologies. Some common examples of wireless networking include:

- Television and Radio Broadcasting
- Satellite Communication
- Radar
- AM radio
- Bluetooth
- Paging
- Terrestrial microwave networks
- FM radio
- HD radio
- SiriusXM satellite radio
- Cordless Phones
- Radio Frequency Identification (RFID)
- Cell phone networks
- Wireless sensor networks
- Explore free networking courses

Working of Wireless Network

Radio frequency technology is connected to radio wave propagation within the electromagnetic spectrum and is used to power wireless networks. When an RF current is applied to an antenna, an electromagnetic field is created that can spread throughout space.

A wireless network's core is a system known as an access point (AP). The primary function of an access point is to broadcast a wireless signal that computers detect and tune into. As wireless networks generally connect to wired networks, access points frequently serve as a gateway to the resources of a wired network, such as an Internet connection.

To connect to an access point and join a wireless network, computers must have wireless network adapters. Generally, computers have these adapters built into the device. Still, if not, almost any computer or notebook can be made wireless-capable by attaching an add-on adapter to an empty expansion slot, USB port, PC card slot, etc.

Types of Wireless Networks

There are mainly four types of standard wireless networks such as wireless local-area network (WLAN), wireless personal area network (WPAN), wireless metropolitan-area network (WMAN), and wireless wide-area network (WWAN).

1. Wireless Local-Area Network (WLAN):

- Connects devices in fixed locations like homes or offices.
- Can range from small-scale home networks to large enterprise networks.
- Commonly used for in-home WiFi setups and small business networks.

2. Wireless Personal Area Network (WPAN):

- Links electronic devices within a user's immediate vicinity, typically up to 10 meters.
- Examples include Bluetooth connections between smartphones and accessories.

3. Wireless Metropolitan Area Network (WMAN):

- Spans cities, small geographic areas, campuses, or business districts.
- Larger than LANs, covering several square miles based on organizational needs.
- Utilized by telephone companies for city-wide cable TV networks.

4. Wireless Wide-Area Network (WWAN):

- Spans large geographic areas like cities, states, or countries.
- Contains smaller networks (LANs or MANs) within its structure.
- Enables communication across long distances, connecting localized networks.
- Examples include cellular networks and the Internet.

5. Wireless Sensor Network (WSN):

- An infrastructure-less network with numerous wireless sensors.
- Monitors system, environmental, and physical conditions.
- Used for surveillance, threat detection, and environmental monitoring purposes.
- Faces challenges with limited energy resources in battery-powered sensors for extended operation.

Advantages of Wireless Networking:

- **Increased Efficiency:** Faster data transfer enhances communication and productivity.
- **Connectivity and Availability:** Users can stay connected on the go, minimizing downtime.
- **Flexibility:** Enables remote work and new working styles like WFH.
- **Savings:** Cost-effective installation due to minimal cabling, suitable for buildings with restrictions.
- **Device Connectivity:** Easy addition or removal of devices without cable limitations.
- **New Possibilities:** Enables the introduction of new products/services, seen in public spaces like airports and hotels.

Disadvantages of Wireless Networking:

- **Security Concerns:** Vulnerable to unauthorized access, requiring robust security measures.
- **Coverage Challenges:** May face coverage gaps or 'black spots' in some buildings.
- **Transmission Speeds:** Wireless speeds can be slower and less efficient than wired connections.
- **Installation Issues:** Potential interference from other wireless devices or electromagnetic sources.

WI-FI STANDARDS

Wireless standards are a set of services and protocols that dictate how your Wi-Fi network (and other data transmission networks) acts.

The most common wireless standards you will encounter are the IEEE 802.11 Wireless LAN (WLAN) & Mesh.

There are many different types of Wi-Fi standards. Your router, laptop, tablet, smartphone, and smart home devices use different wireless standards to connect to the internet. Wireless standards change every few years, too. Updates bring faster internet, better connections, more simultaneous connections, and so on—but the sheer number of wireless standards and specifications is confusing, to say the least.

A Brief History of Wireless Standards

IEEE Standard	Wi-Fi Alliance Name	Year Released	Frequency	Maximum Data Rate
802.11a	Wi-Fi 1	1999	5GHz	54Mbps
802.11b	Wi-Fi 2	1999	2.4GHz	11Mbps
802.11g	Wi-Fi 3	2003	2.4GHz	54Mbps
802.11n	Wi-Fi 4	2009	2.4GHz & 5GHz	600Mbps
802.11ac	Wi-Fi 5	2014	2.4GHz & 5GHz	1.3Gbps
802.11ax	Wi-Fi 6	2019	2.4GHz & 5GHz	10-12Gbps
802.11ax-2021	Wi-Fi 6E	2021	2.4GHz, 5GHz, & 6GHz	10-12Gbps
801.11be	Wi-Fi 7	2024/2025	2.4GHz, 5GHz, & 6GHz	40Gbps

WIRELESS ACCESS POINT

A Wireless Access Point (WAP) is a networking device that allows connecting the devices with the wired network. A Wireless Access Point (WAP) is used to create the WLAN (Wireless Local Area Network), it is commonly used in large offices and buildings which have expanded businesses.

A wireless AP connects the wired networks to the wireless client. It eases access to the network for mobile users which increases productivity and reduces the infrastructure cost.

Advantages of WAP:

- **Increased User Access:** Supports 50-100+ users/devices compared to routers (10-20).
- **Broader Transmission Range:** Covers 100-300 meters, ideal for large offices/buildings.
- **Flexible Networking:** Adapts to diverse wireless devices and network setups.
- **Mobility:** Allows users to move freely while connected.

Disadvantages of WAP:

- **High Cost:** Expensive due to enterprise scale, leading some to use cheaper home routers.
- **Poor Stability:** Relies on air transmission, susceptible to obstacles and slower than wired networks.
- **Less Secure:** Radio wave transmission can be intercepted by hackers.
- **Limited Range:** Impacted by physical barriers, interference, and environmental conditions.
- **Bandwidth Limitations:** May experience reduced speed and reliability.

Applications of WAP:

- **Creating WLANs:** Extends network coverage for large enterprises.
- **Connectivity Expansion:** Allows more users to connect easily in offices.
- **Public Access:** Provides LANs in public places like coffee shops, airports.
- **Wireless Printing:** Connects printers to networks for convenient printing.
- **Cloud Services:** Facilitates device connections to cloud services for data backup and synchronization.

CELLULAR WIRELESS NETWORKS

Cellular network is an underlying technology for mobile phones, personal communication systems, wireless networking etc. The technology is developed for mobile radio telephone to replace high power transmitter/receiver systems. Cellular networks use lower power, shorter range and more transmitters for data transmission.

Features of Cellular Systems

Wireless Cellular Systems solves the problem of spectral congestion and increases user capacity. The features of cellular systems are as follows –

- Offer very high capacity in a limited spectrum.
- Reuse of radio channel in different cells.
- Enable a fixed number of channels to serve an arbitrarily large number of users by reusing the channel throughout the coverage region.
- Communication is always between mobile and base station (not directly between mobiles).
- Each cellular base station is allocated a group of radio channels within a small geographic area called a cell.
- Neighboring cells are assigned different channel groups.
- By limiting the coverage area to within the boundary of the cell, the channel groups may be reused to cover different cells.
- Keep interference levels within tolerable limits.
- Frequency reuse or frequency planning.

ATTENUATION

- **Definition:** Attenuation refers to the gradual weakening of a signal as it travels through a medium like air, water, or a cable. This weakening occurs due to factors like distance, obstacles, and interference.
- **Causes:** The main causes of attenuation include signal absorption by the medium, scattering of the signal, and reflection or refraction at boundaries.
- **Impact:** Higher levels of attenuation result in weaker signals reaching the receiver, which can lead to slower data transmission rates, increased error rates, or complete signal loss.
- **Mitigation:** To mitigate attenuation, various techniques are used, such as using signal repeaters or amplifiers to boost signal strength, optimizing antenna placement for better signal propagation, and using higher-quality cables with lower signal loss.

ANTENNA

- **Definition:** An antenna is a device used to transmit or receive electromagnetic waves, such as radio waves or microwaves. It converts electrical signals into electromagnetic waves for transmission or vice versa for reception.
- **Types:** There are various types of antennas, each designed for specific purposes. For example, dipole antennas are commonly used for radio broadcasting, Yagi antennas for directional communication, and patch antennas for Wi-Fi routers.
- **Function:** Antennas work based on the principle of electromagnetic radiation. They capture electrical signals from a transmitter and convert them into radio waves for transmission. Similarly, they receive incoming radio waves and convert them back into electrical signals for the receiver.
- **Applications:** Antennas are used in communication systems (radio, TV, cellular networks), radar systems, satellite communication, Wi-Fi routers, and RFID systems.

MICROWAVE

- **Definition:** Microwaves are a type of electromagnetic radiation with wavelengths ranging from about one meter to one millimeter. They are used in various applications due to their ability to penetrate obstacles like clouds and rain.
- **Applications:** Microwaves are commonly used in microwave ovens for cooking food, radar systems for aircraft navigation and weather monitoring, communication networks (microwave links) for long-distance data transmission, and satellite communication for TV broadcasting and telecommunication.
- **Advantages:** One of the key advantages of microwaves is their ability to travel long distances without significant signal degradation, making them ideal for point-to-point communication and long-range wireless links.

- **Safety Concerns:** High-power microwaves can be harmful to human health, causing tissue heating and potential damage, so they must be used with proper safety measures and shielding.

JAMMING

- **Definition:** Jamming refers to the deliberate interference or disruption of wireless communication signals to disrupt normal operations or prevent authorized access.
- **Techniques:** Jamming can be achieved using various techniques, such as transmitting noise or interference signals on the same frequency as the target signal, using high-power transmitters to overwhelm the receiver, or employing frequency-hopping or spread spectrum techniques to evade detection.
- **Purposes:** Jamming is used for both legal and illegal purposes. In military applications, it is used for electronic warfare to disrupt enemy communication and radar systems. In civilian applications, it can be used to prevent unauthorized use of radio-controlled devices or to disrupt wireless networks.
- **Countermeasures:** To counter jamming, techniques such as frequency agility (changing frequencies rapidly), spread spectrum modulation, signal filtering, and using directional antennas to minimize interference are employed.

SSID (SERVICE SET IDENTIFIER)

- **Definition:** SSID is a unique identifier that distinguishes one wireless network from another. It is used to identify and connect to specific Wi-Fi networks.
- **Usage:** When connecting to a Wi-Fi network, users need to enter the correct SSID to access the network. SSID settings are managed through the router's administration interface.
- **Security:** While SSID hiding can be used as a basic security measure, it's not a foolproof method as SSIDs can still be discovered using network scanning tools. Stronger security measures like WPA/WPA2 encryption and network authentication are recommended.
- **Configuration:** Network administrators can configure SSID names, visibility (hidden or broadcast), and security settings (encryption type, passphrase) through the router's settings interface.

BLUETOOTH

- **Definition:** Bluetooth is a wireless technology standard used for short-range communication and data exchange between devices.
- **Applications:** Bluetooth is commonly used in wireless headphones, speakers, computer peripherals (keyboards, mice), smartphones, IoT devices, and automotive systems for hands-free calling and audio streaming.

- **Features:** Bluetooth offers low power consumption, ease of use, and compatibility with a wide range of devices. Different versions of Bluetooth (e.g., Bluetooth 4.0, Bluetooth 5.0) offer improved speed, range, and connectivity features.
- **Usage:** Users can pair Bluetooth-enabled devices to establish a wireless connection, allowing for data transfer, audio streaming, and device control functionalities.

WI-FI HOTSPOTS

- **Definition:** Wi-Fi hotspots are locations where wireless internet access is provided through a wireless local area network (WLAN).
- **Types:** Hotspots can be public (e.g., cafes, airports, hotels) or private (set up by individuals or organizations for specific users).
- **Access:** Users can connect to hotspots using Wi-Fi-enabled devices like smartphones, laptops, or tablets. They typically require authentication (e.g., entering a password) for access.
- **Security:** Public hotspots may pose security risks, so users should use VPNs (Virtual Private Networks) or other encryption methods for secure browsing and data protection.
- **Benefits:** Hotspots provide convenient internet access on the go, enabling users to stay connected outside their homes or offices. They are commonly found in public spaces, transportation hubs, and commercial establishments, offering wireless connectivity to customers, guests, and employees.

WIFI

Wi-Fi (Wireless Fidelity) is the **wireless networking** technology that connects devices to the internet. It is the trademark created by the Wi-Fi Alliance. This organization allows using the 'Wi-Fi Certified' term only for products that have successfully completed interoperability certification training.

Features of WiFi

- WiFi establishes an **internet** connection for the individual as well as public use.
- The indoor and outdoor Wi-Fi range is dependent upon the environment.
- Wi-Fi networks encrypt the radio signal through WPA encryption.
- It uses Physical Data Link Layer (PDLL) to operate.
- WiFi operates similarly to LAN without the need for wired connections such as wires and cables.

Uses of Wi-Fi

- Helps devices to exchange information with one another by creating a netwotk.
- Find application in wireless mesh networks.
- Helps in using the Internet of Things devices.
- Acts as a hotspot to offer temporary access to Wi-Fi enabled devices so that they do not know about the details of main network.

- Enables VoWi-Fi to call anyone, even in areas where there is no mobile network.
- Acts as positioning system to recognize the area of a device by detecting the placement of Wi-Fi hotspots.
- Constructs simple wireless connections called Point to Point networks to connect two locations that cannot be accessed through the wire.

For the transmission of WiFi signal, the following three media are available:

- **Ethernet(802.3) connection/ Base station:** This is the main host network which provides network connection to the router.
- **Access point:** It accepts wired Ethernet connection and then converts the wired connection into a wireless connection. It then extends the connection as radio waves.
- **Accessing devices:** These are the physical devices on which Wifi is enabled and on which we surf the internet.

WIRELESS ATTACKS

1. War Driving:

- **Definition:** WarDriving, knew as **Access Point Mapping** War driving is the act of searching for Wi-Fi networks while driving around in a vehicle, typically with a laptop or mobile device equipped with Wi-Fi scanning tools.
- **Purpose:** The goal of war driving is to identify and map out wireless networks, including their SSIDs, security settings, and signal strengths.
- **Techniques:** War drivers use tools like NetStumbler, Kismet, or Wireshark to detect nearby Wi-Fi networks and analyze their vulnerabilities.
- **Risk:** War driving can pose a security risk as it allows attackers to identify open or poorly secured networks, which can be exploited for unauthorized access or data interception.

2. War Walking:

- **Definition:** War walking is similar to war driving, but instead of driving, the attacker walks around on foot with a portable device to scan for Wi-Fi networks.
- **Purpose:** War walking is used to discover and map out Wi-Fi networks in specific locations, such as urban areas, office complexes, or public spaces.
- **Tools:** Attackers use tools like WiFi Analyzer, inSSIDer, or similar apps on smartphones or handheld devices for scanning and mapping networks.
- **Security Implications:** War walking can reveal security vulnerabilities in wireless networks, especially if networks are poorly secured or use outdated encryption protocols.

3. War Flying:

- **Definition:** War flying involves using an aircraft or drone equipped with Wi-Fi scanning equipment to detect and analyze wireless networks from the air.

- **Purpose:** War flying allows attackers to cover larger areas and identify wireless networks in remote or difficult-to-access locations.
- **Tools:** Attackers may use specialized equipment mounted on aircraft or drones, such as high-gain antennas and GPS systems, to conduct war flying.
- **Risk:** War flying poses a significant security risk as it enables attackers to identify Wi-Fi networks from long distances and potentially target networks that are not visible from the ground.

4. War Chalking:

- **Definition:** War chalking involves marking physical surfaces, such as walls or pavements, with symbols or codes to indicate the presence and characteristics of nearby wireless networks.
- **Purpose:** War chalking was historically used by hackers and enthusiasts to share information about Wi-Fi networks in public spaces, such as cafes, libraries, or parks.
- **Symbols:** Common war chalking symbols include SSID names, encryption types (WEP, WPA), signal strength indicators, and network accessibility (open or secured).
- **Security Concerns:** While war chalking is less common today due to increased security awareness and advancements in Wi-Fi technology, it can still pose a security risk by disclosing network information to potential attackers.

5. Bluejacking:

- **Definition:** Bluejacking is a type of wireless attack that involves sending unsolicited messages or data to Bluetooth-enabled devices, such as smartphones, tablets, or laptops.
- **Purpose:** Bluejacking is often used for harmless pranks or social engineering, such as sending funny messages or promotional content to nearby Bluetooth devices.
- **Technique:** Attackers use Bluetooth-enabled devices or apps that allow them to discover nearby devices and send messages without pairing or establishing a connection.
- **Security Implications:** While bluejacking is usually benign, it highlights the potential vulnerabilities of Bluetooth technology, such as unauthorized access and data interception. It also underscores the importance of Bluetooth device security settings and awareness.

Piggybacking is the unauthorized use of someone else's Wi-Fi network without their permission. It involves connecting to a network that is not owned or provided by the individual or device attempting to access it. This can occur by exploiting weak security measures such as open networks, default passwords, or vulnerabilities in Wi-Fi protocols.

HOW TO SECURE WIRELESS NETWORKS

- **Strong Passwords:** Use complex, unique passwords for your Wi-Fi network to prevent unauthorized access.
- **Encryption:** Enable WPA2 or WPA3 encryption to secure data transmitted over the network.

- **Update Firmware:** Regularly update your router's firmware to patch security vulnerabilities.
- **Disable WPS:** Disable Wi-Fi Protected Setup (WPS) as it can be exploited by attackers.
- **Guest Network:** Set up a separate guest network with limited access for visitors.
- **Firewall:** Enable firewall settings on your router to block unauthorized connections.
- **SSID Broadcasting:** Disable SSID broadcasting to make your network less visible to potential attackers.
- **MAC Filtering:** Use MAC address filtering to only allow specified devices to connect to your network.
- **Network Monitoring:** Use network monitoring tools to detect and respond to suspicious activity.
- **Physical Security:** Secure your router in a physically safe location to prevent unauthorized access to the device.

PROXY SERVER

The **proxy server** is a computer on the internet that accepts the incoming requests from the client and forwards those requests to the destination server. It works as a gateway between the end-user and the internet. It has its own IP address. It separates the client system and web server from the global network.

In other words, we can say that the proxy server allows us to access any websites with a different IP address. It plays an intermediary role between users and targeted websites or servers. It collects and provides information related to user requests. The most important point about a proxy server is that it does not **encrypt traffic**.

There are two main purposes of proxy server:

- To keep the system behind it anonymous.
- To speed up access to a resource through caching.

Types of Proxy Servers

There are many types of proxy servers available. The two most common types of proxy servers are **forward** and **reverse proxy servers**. The other proxy server has its own feature and advantages. Let's discuss each in detail.

1. **Open or Forward Proxy Server:** It is the most widely recognized type of intermediary worker that is gotten to by the customer. An open or forward proxy server refers to those sorts of intermediaries that get demands from web clients and afterward peruse destinations to gather the mentioned information. After collecting the data from the sites, it forwards the data to the internet users directly. It bypasses the firewall made by authorities. The following image shows forward proxy configuration.

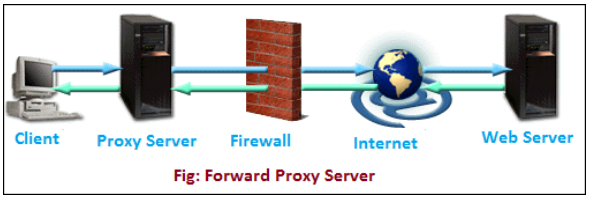


Fig: Forward Proxy Server

2. **Reverse Proxy Server:** It is a proxy server that is installed in the neighborhood of multiple other internal resources. It validated and processes a transaction in such a way that the clients do not communicate directly. The most popular reverse proxies are **Varnish** and **Squid**. The following image shows the reverse proxy configuration.

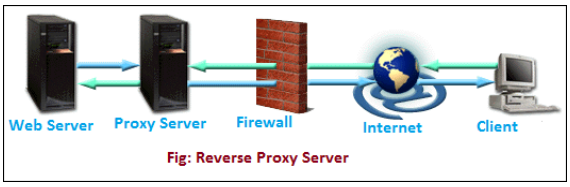


Fig: Reverse Proxy Server

Advantages of Proxy Server

- It improves the security and enhances the privacy of the user.
- It hides the identity (IP address) of the user.
- It controls the traffic and prevents crashes.
- Also, saves bandwidth by caching files and compressing incoming traffic.
- Protect our network from malware.
- Allows access to the restricted content.

Working of Proxy Server

As we have discussed above, the proxy server has its own IP address and it works as a gateway between the client and the internet. The client's computer knows the IP address of the proxy server. When the client sends a request on the internet, the request is re-routed to the proxy. After that, the proxy server gets the response from the destination or targeted server/site and forwards the data from the page to the client's browser (Chrome, Safari, etc.).

PROXY CHAIN

A proxy chain, also known as a proxy cascade or proxy relay, is a series of proxy servers that are used sequentially to route internet traffic through multiple intermediary servers before reaching the final destination. Here's a detailed explanation:

1. **Initial Request:** When a user initiates an internet request (e.g., browsing a website), it first goes through the client's local network settings, which may include a configured proxy server.
2. **First Proxy Server:** The request is then forwarded to the first proxy server in the chain. This server acts as an intermediary between the client device and the internet.
3. **Intermediate Proxies:** If the first proxy server is part of a proxy chain, it forwards the request to the next proxy server in the chain. This process continues until the request reaches the final proxy server before exiting to the internet.
4. **Final Proxy Server:** The last proxy server in the chain forwards the request to the target website or server on the internet.

5. **Response Path:** The response from the target server follows a similar path in reverse, passing through each proxy server in the chain before reaching the client device.

Benefits of Proxy Chains:

1. **Anonymity:** Enhances user anonymity by hiding the origin IP address, making tracing difficult.
2. **Access Control:** Bypasses content restrictions and accesses blocked websites by routing traffic through different proxies.
3. **Load Balancing:** Distributes internet traffic across multiple proxies, balancing server loads and improving performance.

Considerations and Risks:

1. **Latency:** Additional proxy servers may introduce latency, slowing down browsing or data transfer.
2. **Security:** Risks include data exposure to interception or manipulation if proxy servers are not secure.
3. **Configuration Complexity:** Setting up and managing a proxy chain requires technical configuration and maintenance.

TELNET

This software links personal computer to a network server and converts data into the plain text. Basically, it is used for remote login for a system. It makes modifications and control of the server easier.

FTP

FTP is used for transferring of web pages and used for downloading the files from other different servers. Basically, it is used for transferring the files from one system to another system more reliably and efficiently.

SSH OR SECURE SHELL

SSH or Secure SHell is now only major protocol to access the network devices and servers over the internet. SSH was developed by SSH Communications Security Ltd., it is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.

- It provides strong authentication and secure communications over insecure channels.
- SSH runs on port 22 by default; however it can be easily changed. SSH is a very secure protocol because it shares and sends the information in encrypted form which provides confidentiality and security of the data over an un-secured network such as internet.
- Once the data for communication is encrypted using SSH, it is extremely difficult to decrypt and read that data, so our passwords also become secure to travel on a public network.
- SSH also uses a public key for the authentication of users accessing a server and it is a great practice providing us extreme security. SSH is mostly used in all popular operating systems like Unix, Solaris, Red-Hat Linux, CentOS, Ubuntu etc.

- SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker who has managed to take over a network can only force ssh to disconnect. He or she cannot play back the traffic or hijack the connection when encryption is enabled.
- When using ssh's slogin (instead of rlogin) the entire login session, including transmission of password, is encrypted; therefore, it is almost impossible for an outsider to collect passwords.

SECURE SOCKET LAYER (SSL)

It is a networking protocol which gives secure transmission in a non-secure network. SSL requires a certificate and works on the Public Key Encryption. SSL is implemented in various operations of networked environment such as web browsing, messaging, emails and other protocols like FTP. (copy)

SMTP

SMTP (Simple Mail Transfer Protocol) is a protocol for managing Internet's electronic mail. It is an application layer protocol. It uses TCP due to its reliable data transfer service. TCP establishes SMTP connections at port 25. SMTP uses persistent connections. The same TCP connection can be used to send multiple emails, once the connection has been established. Only 7-bit ASCII content is to be directly sent. Other content needs to be encoded to 7-bit ASCII and then decoded at the receiving end.

HYPERTEXT TRANSFER PROTOCOL (HTTP)

- HyperText Transfer Protocol (HTTP) is a protocol using which hypertext is transferred over the Web.
- Due to its simplicity, HTTP has been the most widely used protocol for data transfer over the Web but the data (i.e. hypertext) exchanged using HTTP isn't as secure as we would like it to be.
- In fact, hyper-text exchanged using HTTP goes as plain text i.e. anyone between the browser and server can read it relatively easily if one intercepts this exchange of data.
- The acronym for Hypertext Transfer Protocol is HTTP.
- The web server delivers the desired data to the user in the form of web pages when the user initiates an HTTP request through their browser. Above the TCP layer lies an application layer protocol called HTTP. It has given web browsers and servers certain standard principles that they can use to talk to one another.
- Because each transaction on the HTTP protocol is carried out independently of the others and without reference to the history, the connection between the web browser and the server ends after the transaction is finished. This makes HTTP a stateless protocol.

Advantages of HTTP

- Because there are fewer connections running at once, it delivers reduced CPU and memory utilization.

- It allows requests and answers to be pipelined via HTTP.
- Because there are fewer TCP connections, it provides less network congestion.
- During the first stage of connection establishment, handshakes are exchanged. Because there is no handshaking, it provides lower latency for subsequent requests.
- Without terminating the TCP connection, it reports problems.

Disadvantages of HTTP

- It is applicable to point-to-point connections.
- It isn't mobile-friendly.
- It is not capable of being pushed.
- It uses far too many words.
- It doesn't provide trustworthy exchange (in the absence of retry mechanism).
- When the client receives all the data it requires, the connection is not terminated. Therefore, the server won't be accessible during this time.

HYPERTEXT TRANSFER PROTOCOL SECURE (HTTPS)

- Hypertext Transfer Protocol Secure (HTTPS) is an extended version of the Hypertext Transfer Protocol (HTTP). It is used for secure communication.
- In HTTPS, the communication protocol is encrypted using Transport Layer Security.
- HTTPS stands for Hypertext Transfer Protocol Secure.
- While HTTP guarantees data security, the HTTP protocol does not provide data security.
- As a result, HTTPS can be defined as a secure variant of the HTTP protocol. Data can be transferred using this protocol in an encrypted format.
- In most cases, the HTTPS protocol must be used while entering bank account information.
- The HTTPS protocol is mostly utilised in situations when entering login credentials is necessary. Modern browsers like Chrome distinguish between the HTTP and HTTPS protocols based on distinct markings.
- HTTPS employs an encryption mechanism called Secure Sockets Layer (SSL), also known as Transport Layer Security, to enable encryption.

Advantages of HTTPS

- Provides in-transit data security.
- Shields your website from data breaches, phishing, and MITM attacks.
- Increases the visitors' trust to your website.
- Eliminates the "NOT Secure" alerts.
- Assist you in raising your website's ranking.

Disadvantages of HTTPS

- When switching to HTTPS, an SSL certificate needs to be bought. Even though website hosts often give SSL certificates, these should be renewed annually by paying a charge.
- Encrypting and decrypting data across HTTPS connections requires a lot of computation.
- There will be issues with caching some information over HTTPS. Public caching of those that previously took place won't happen again.
- Certain proxy servers and firewalls prevent users from accessing HTTPS websites. Both deliberate and inadvertent actions might result from this.

- If there are configuration issues, HTTP will be used by your website to obtain files rather than HTTPS.

POP3

POP 3 stands for Post Office Protocol Version 3. POP3 protocol is used to provide access to the mail inbox that is stored in the email server. POP3 protocol can download and delete messages. Once the POP3 client has established a connection with the mail server it can easily retrieve all the messages from the server. The user can access the messages locally even if the user is offline. Every time the client needs to check manually for new messages as POP3 Protocol provides the feature of real-time synchronization. Various email applications such as Microsoft Outlook, Apple Mail, Gmail supports POP3 protocol.
When a message is sent, SMPT is used to transfer it from the client to the server and ultimately to the server of the recipient. However, the Message Access Agent facilitates the transmission of the message from the receiving server to the host server. POP3 and IMAP are the two types of protocols that are included in the Message Access Agent.
POP3 Ports
POP3 makes use of two network ports. They are:

- **Port 110:** Port 110 is a default TCP port used by POP3. But It has a disadvantage that it does not support encrypted communication.
- **Port 995:** Port 995 is majorly used for more secure applications. Port 995 is a TLS or SSL port used to provide more security.

DNS

An application layer protocol defines how the application processes running on different systems, pass the messages to each other.

- DNS stands for Domain Name System.
- DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
- DNS is required for the functioning of the internet.
- Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
- DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
- DNS is a TCP/IP protocol used on different platforms. The domain name space is divided into three different sections: generic domains, country domains, and inverse domain.

Generic Domains

- It defines the registered hosts according to their generic behavior.
- Each node in a tree defines the domain name, which is an index to the DNS database.
- It uses three-character labels, and these labels describe the organization type.

Label	Description
com	Commercial Organizations
edu	Educational institutions
gov	Government institutions
org	Nonprofit Organizations

Country Domain

The format of country domain is same as a generic domain, but it uses two-character country abbreviations (e.g., us for the United States) in place of three character organizational abbreviations.

Inverse Domain

The inverse domain is used for mapping an address to a name. When the server has received a request from the client, and the server contains the files of only authorized clients. To determine whether the client is on the authorized list or not, it sends a query to the DNS server and ask for mapping an address to the name.

Differences between TELNET and FTP

S.NO	TELNET	FTP
1.	TELNET stands for TELecommunication NETwork.	FTP stands for File Transfer Protocol.
2.	TELNET is used to access command line interface of a remote server.	FTP is used for uploading & downloading the files.
3.	TELNET uses port 23.	FTP uses ports 20 and 21.
4.	TELNET uses only one connection.	FTP establish two connections, one is for control command and another is for data transfer.
5.	Remote Login is necessary in TELNET.	Remote Login is not necessary in FTP.
6.	It does not provide high security, it provides only general security.	It provides high security than TELNET.
7.	It is used for remote login into a system.	It is used for transferring the files from one system to another system.
8.	It is a connection oriented protocol.	It is also a connection oriented protocol.

S.NO	TELNET	FTP
9.	Telnet is mainly used for translating NVT from data and converting it to the acknowledged form.	While FTP is mainly used for transferring of data between client and server.
10.	TELNET has become more or less outdated.	FTP is a popular tool.
11.	TELNET is not as widely used for web diagnostics.	FTP is used for uploading and downloading web files.

Differences between SSH and TELNET

1. SSH is **more secure** compared to Telnet
2. SSH **encrypts the data** while Telnet sends data in plain text
3. SSH uses a **public key for authentication** while Telnet does not use any authentication
4. SSH adds a bit more **overhead** to the bandwidth compared to Telnet
5. Telnet has been all but replaced by SSH in almost all uses
6. SSH and Telnet commonly serves the same purpose
7. SSH allows for remote command execution while Telnet does not support this feature.
8. SSH relies on external terminal emulation software while Telnet includes built-in terminal emulation.

Differences between SSH and SSL

S.No	SSH	SSL
1.	SSH stands for Secure Shell.	SSL stands for secure socket layer.
2.	It is cryptographic tunneling protocol and has a username/password authentication system.	It does not have a username/password authentication system like SSH.
3.	It works on the port number 22.	It works on the port number 443.
4.	It completely depends on the network tunneling.	It is asynchronous as it depends on the certificates.
5.	It works on three-stage process for server and client authentication processes.	While SSL usually works on X.509 digital certificates for server and client authentication.

S.No	SSH	SSL
6.	It encrypts the communication between two computers over the internet.	It encrypts the communication between browser and server.
7.	It is appropriate and effective for securely executing commands across the internet.	It is best suited for securely transferring critical data like in credit cards and banking.
8.	It provides data confidentiality by using symmetric key algorithms.	It adopts a combination of both symmetric and asymmetric encryption algorithms to provide data privacy.
9.	SSH is basically a cryptographic network protocol.	SSL is basically is a security protocol.
10.	SSH protects against DNS spoofing, data manipulation, IP source routing, data sniffing during transmission etc.	

Differences between SMTP and HTTP

SMTP	HTTP
SMTP is used for mail services.	HTTP is mainly used for data and file transfer.
It uses port 25.	It uses port 80.
It is primarily a push protocol.	It is primarily a pull protocol.
It imposes a 7-bit ASCII restriction on the content to be transferred.	It does not impose a 7-bit ASCII restriction. Can transfer multimedia, hyperlinks, etc.
SMTP transfers emails via Mail Servers.	HTTP transfers files between the Web server and the Web client.
SMTP is a persistent type of TCP connection.	It can use both Persistent and Non-persistent.
Uses base64 encoding for authentication.	Uses different methods of authentication such as basic, digest, and OAuth.

SMTP	HTTP
Does not support session management or cookies.	Supports session management and cookies to maintain state.
Has a smaller message size limit compared to HTTP.	Has a larger message size limit compared to SMTP.
Requires authentication for sending emails.	Does not require authentication for browsing web pages.
Supports both plain text and encrypted communication (SMTPS or STARTTLS).	Supports both plain text and encrypted communication (HTTPS).

Differences between HTTP and HTTPS

HTTP	HTTPS
HTTP stands for HyperText Transfer Protocol. In HTTP, URL begins with “http://”.	HTTPS for HyperText Transfer Protocol Secure. In HTTPs, URL starts with “https://”.
HTTP uses port number 80 for communication.	HTTPs uses 443 port number for communication.
HTTP is considered to be unsecure.	HTTPs is considered as secure.
HTTP works at Application Layer. In HTTP, Encryption is absent. HTTP does not require any certificates. HTTP does not improve search ranking	HTTPS works at Transport Layer. Encryption is present in HTTPS. HTTPS needs SSL Certificates. HTTPS helps to improve search ranking
HTTP faster than HTTPS	HTTPS slower than HTTP
HTTP does not use data hashtags to	While HTTPS will have the data before

HTTP	HTTPS
secure data.	sending it and return it to its original state on the receiver side.
In HTTP Data is transfer in plaintext.	In HTTPS Data transfer in ciphertext.
HTTP Should be avoided.	HTTPS Should be preferred.
Search engines do not favour the insecure website.	Improved reputation of the website in search engine.
HTTP Does not require SSL/TLS or Certificates	HTTPS Requires SSL/TLS implementation with Certificates.
In HTTP Users ar worried about their data.	In HTTPS Users are confident about the security of their data.

Differences between SMTP and POP3

For sending and receiving messages, we use two protocols one is SMTP (Simple Mail Transfer Protocol) and another is POP3 (Post Office Protocol version 3). They are also called as PUSH and POP protocols respectively. They are agents, Message Transfer Agent, and Message Access Agent respectively to send and retrieve the messages.

S.NO	SMTP	POP3
1.	SMTP stands for Simple Mail Transfer Protocol.	POP3 stands for Post Office Protocol version 3.
2.	It is used for sending messages.	It is used for accessing messages.
3.	The port number of SMTP is 25, 465, and 587 for secured connection (TLS connection).	The port number of POP3 is 110 or port 995 for SSL/TLS connection.
4.	It is an MTA (Message Transfer Agent) for sending the message to the receiver.	It is MAA (Message Access Agent) for accessing the messages from mailbox.
5.	It has two MTAs one is client MTA	It has also two MAAs one is client MAA

S.NO	SMTP	POP3
	(Message Transfer Agent) and second one is server MTA (Message Transfer Agent).	(Message Access Agent) and another is server MAA(Message Access Agent).
6.	SMTP is also known as PUSH protocol.	POP3 is also known as POP protocol.
7.	SMTP transfers the mail from sender's computer to the mail box present on receiver's mail server.	POP3 allows to retrieve and organize mails from mailbox on receiver mail server to receiver's computer.
8.	It is implied between sender mail server and receiver mail server.	It is implied between receiver and receiver mail server.

Port Number

- HTTP (Hypertext Transfer Protocol): Port 80
- HTTPS (Hypertext Transfer Protocol Secure): Port 443
- FTP (File Transfer Protocol): Port 20 and 21
- SSH (Secure Shell): Port 22
- Telnet: Port 23
- SMTP (Simple Mail Transfer Protocol): Port 25 and currently port 587
- DNS (Domain Name System): Port 53
- POP3 (Post Office Protocol version 3): port 110: default, non-encrypted port; and port 995: for secure connection

---

PASSWORD

A password is an authentication method used for computer accounts and websites. They are strings of characters used for user authentication in computing.

A strong password has multiple layers of complexity, making it difficult for someone to crack it. Weak passwords can be broken quite easily, which means they offer very little security protection.

Users tend to choose simple passwords that are easy to remember; however, this also makes them easier to crack by hackers or other nefarious users who may want to get into your account or system.

What Is a Strong Password?

A strong password is difficult to crack. It has multiple layers of complexity and is hard to guess.

A password should contain different characters (letters, numbers, and symbols). It should be at least 12 characters long and contain a combination of capital and lowercase letters, and at least one number.
A strong password should never contain a person's name, birth date, address, etc. A strong password should be difficult for anyone to guess, even a computer.

What is a Weak Password?

A weak password has very little complexity and is easily guessable. It usually consists of easy-to-remember words found in the dictionary.
Weak passwords are usually short and easy to crack.
Those who use weak passwords are at a higher risk of having their accounts hacked. They are also less likely to be able to use the strongest security features available on the internet.
The best way to avoid using a weak password is to create a strong password.

Tips for Creating Strong Passwords

1. Length.
2. Mix It Up.
3. Avoid Obvious Words.
4. Avoid Personal Info.
5. Make It Random.
6. Use a Password Manager.

DIFFERENT TYPES OF PASSWORDS

1. Biometric Passwords:

- Biometric passwords use unique biological characteristics such as fingerprints, facial recognition, iris scans, or voiceprints for authentication.
- These passwords are highly secure as they are based on individual physical traits that are difficult to replicate.
- Biometric passwords are commonly used in smartphones, access control systems, and high-security environments.

2. Pattern-based Graphical Passwords:

- Pattern-based graphical passwords use patterns or gestures drawn on a graphical interface instead of alphanumeric characters.
- Users create a unique pattern by connecting predefined points or shapes on a grid or screen.
- These passwords are visually intuitive, easy to remember, and can be more secure than traditional text-based passwords if implemented correctly.

STRONG PASSWORD TECHNIQUES

- Strong password techniques involve creating passwords that are complex, lengthy, and difficult for attackers to guess or crack.
- These passwords typically include a mix of uppercase and lowercase letters, numbers, symbols, and avoid common words or predictable patterns.
- Examples of strong password techniques include using passphrases, combining unrelated words, incorporating special characters, and avoiding personal information.

Strong password techniques are strategies used to create passwords that are highly secure and resistant to various forms of attacks, such as brute-force attacks, dictionary attacks, and social engineering. Here's an elaboration on strong password techniques:

- **Complexity:** Strong passwords are complex, meaning they include a mix of different character types such as uppercase letters, lowercase letters, numbers, and special symbols (e.g., !, @, #, $, %, ^, &).
- **Length:** Longer passwords are generally more secure than shorter ones. A recommended minimum length for strong passwords is typically 12 characters, but longer passwords, such as 16 characters or more, provide even greater security.
- **Avoiding Predictability:** Strong passwords should avoid using easily guessable information such as common words, phrases, or personal information (e.g., names, birthdays, addresses). Using random combinations of characters is more secure.
- **Passphrases:** Passphrases are a type of strong password that consists of multiple words or a sentence. They are easier to remember than random strings of characters and can still be highly secure if they include a mix of words, numbers, and symbols.
- **Randomness:** Strong passwords should be as random as possible, meaning they should not follow a predictable pattern or sequence. Avoiding repeating characters, consecutive numbers or letters, and common password structures (e.g., "123456" or "password") enhances security.
- **No Reuse:** It's crucial not to reuse passwords across multiple accounts or services. Each account should have a unique, strong password to prevent a security breach on one platform from compromising others.
- **Regular Updates:** It's good practice to update passwords regularly to minimize the risk of them being compromised over time. Changing passwords at least every 3-6 months is a common recommendation.
- **Password Managers:** Consider using a reputable password manager to generate, store

---

Types of Passwords Attack

- Non-electric attacks
- Online attacks
- Offline attacks

Non-electric Attacks: A non-electric attack is a type of attack that uses chicanery to get sensitive information of users or perform actions through which the security of a network will be compromised.

- **Social Engineering:** Tricking individuals into divulging sensitive information or performing actions that compromise security.
- **Shoulder Surfing:** Observing someone's password as they enter it, typically in public or shared spaces.
- **Spidering:** Gathering information from various sources to build a customized list of potential passwords.

Online Attacks:

- **Guess:** Attempting to guess passwords based on personal information or common patterns.
- **Brute Force Attack:** Trying all possible combinations of characters until the correct password is found.
- **Dictionary Attack:** Using a pre-built list of common words or phrases to guess passwords.
- **Phishing:** Deceiving users into revealing their passwords through fake emails, messages, or websites.
- **Malware:** Using malicious software to steal passwords or gain unauthorized access.

Offline Attacks:

- **Offline Cracking:** Attempting to crack hashed passwords obtained from compromised systems or databases.
- **Rainbow Table Attack:** Using precomputed tables of hashed passwords to quickly match and reveal plaintext passwords.
- **Network Analyzers:** Intercepting and analyzing plaintext passwords sent over networks to gain unauthorized access.
- **Mask Attack:** Tailoring attacks based on known patterns or criteria to reduce the search space and speed up password cracking.

STEPS TO STAY SECURE IN DIGITAL WORLD

- **Have a Strong Password:** Use complex combinations of letters, numbers, and symbols in your passwords and avoid easily guessable information.
- **Encrypt Your Data:** Utilize encryption tools or software to protect sensitive data stored on your devices and ensure secure communications over the internet.
- **Security Suite Software:** Install reputable antivirus and anti-malware software to detect and prevent malicious threats, and keep it updated regularly.
- **Firewall Setup:** Enable and configure firewalls on your devices and network router to monitor and control incoming and outgoing traffic.
- **Update Operating System (OS):** Keep your OS, applications, plugins, and drivers updated with the latest security patches and software updates.