What is TCP/IP:

the TCP / IP using one example, so TCP is like the bus full of data and IP is the driver who will give bus the direction so that the bus will reach where it has to go.

TCP vs. IP: What is the Difference?

TCP and IP are separate protocols that work together to ensure data is delivered to its intended destination within a network. IP obtains and defines the address — the IP address — of the application or device the data must be sent to.

How Does TCP/IP Work?

It breaks messages into packets to avoid having to resend the entire message in case it encounters a problem during transmission. Packets are automatically reassembled once they reach their destination. Every packet can take a different route between the source and the destination computer, depending on whether the original route used becomes congested or unavailable.

Data Link Layer

The datalink layer defines how data should be sent, handles the physical act of sending and receiving data, and is responsible for transmitting data between applications or devices on a network. This layer is same as physical & data link layer of the **OSI** model.

Internet Layer

The internet network level protocol (IP,ARP,ICMP) handle machine to machine communications.

The internet layer is responsible for sending packets from a network and controlling their movement across a network to ensure they reach their

destination. It provides the functions and procedures for transferring data sequences between applications and devices across networks.

Transport Layer

The transport layer is responsible for providing a solid and reliable data connection between the original application or device and its intended destination. This is the level where data is divided into packets and numbered to create a sequence. The transport layer then determines how much data must be sent, where it should be sent to, and at what rate. It ensures that data packets are sent without errors and in sequence and obtains the acknowledgment that the destination device has received the data packets.

TCP/IP defines two protocol at this layer **UDP** & **TCP**

UDP (User Datagram Protocol) is connectionless protocol.

UDP is used for application that requires quick but necessarily reliable delivery.

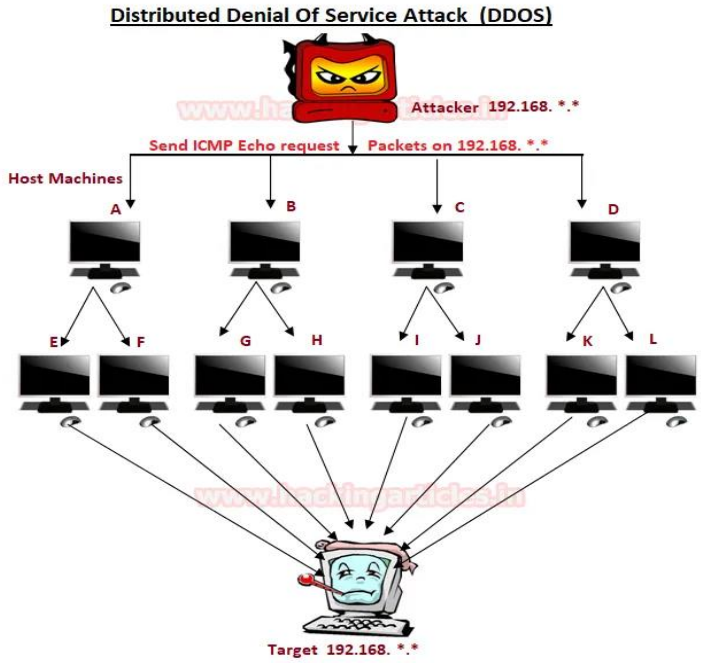
Application Layer

The application layer refers to programs that need TCP/IP to help them communicate with each other. This is the level that users typically interact with, such as email systems and messaging platforms. It combines the session, presentation, and application layers of the OSI model.

What is DOS/DDOS Attack

A **denial-of-service attack** (DoS attack) is a cyber-attack where the attacker looks to make a machine or network resource unavailable to its deliberated users by temporarily or indefinitely services of disturbing a host connected to the Internet. Denial of service is usually accomplished by flooding the targeted machine or resource with excessive requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled

Basically, the attacker machine either sends infinite request packets to the target machine without waiting for a reply packet form the target network or uses bots (host machines) to send request packet on the target machine. Let study more above it using given below image, here you can observe 3 Phases where **Attacker machine** is placed at the **Top** while **Middle** part holds **Host machine** which is controlled by the attacker machine and at **Bottom**, you can see **Target** machine.



DOS/DDOS Categories

Volume Based Attack: The attack's objective is to flood the bandwidth of the target networks by sending ICMP or UDP or TCP traffic in per bits per second.

Protocol-Based Attack: This kind of attack focus actual target server resources by sending packets such TCP SYN flood, Ping of death or Fragmented packets attack per second to demolish the target and make it unresponsive to other legitimate requests.

Application Layer Attack: Rather than attempt to demolish the whole server, an attacker will focus their attack on running applications by sending request per second, for example, attacking WordPress, Joomla web server by infinite request on apache to make it unresponsive to other legitimate requests.

How does Email work?

Step-by-Step Process of Sending an Email

Composing the Email

When you compose an email, you create a message by entering the recipient's email address, a subject line, and the body of the message. You can also attach files or images. Once ready, you click "send."

Connecting to the SMTP Server

After hitting "send," your email client communicates with the SMTP server, which is responsible for sending your email. This connection is typically secured using TLS (Transport Layer Security) to protect the data.

Verifying Sender's Information

The SMTP server verifies the sender's email address to ensure it is valid and authorized to send emails. This step helps in preventing spam and unauthorized use.

Finding the Recipient's Email Server

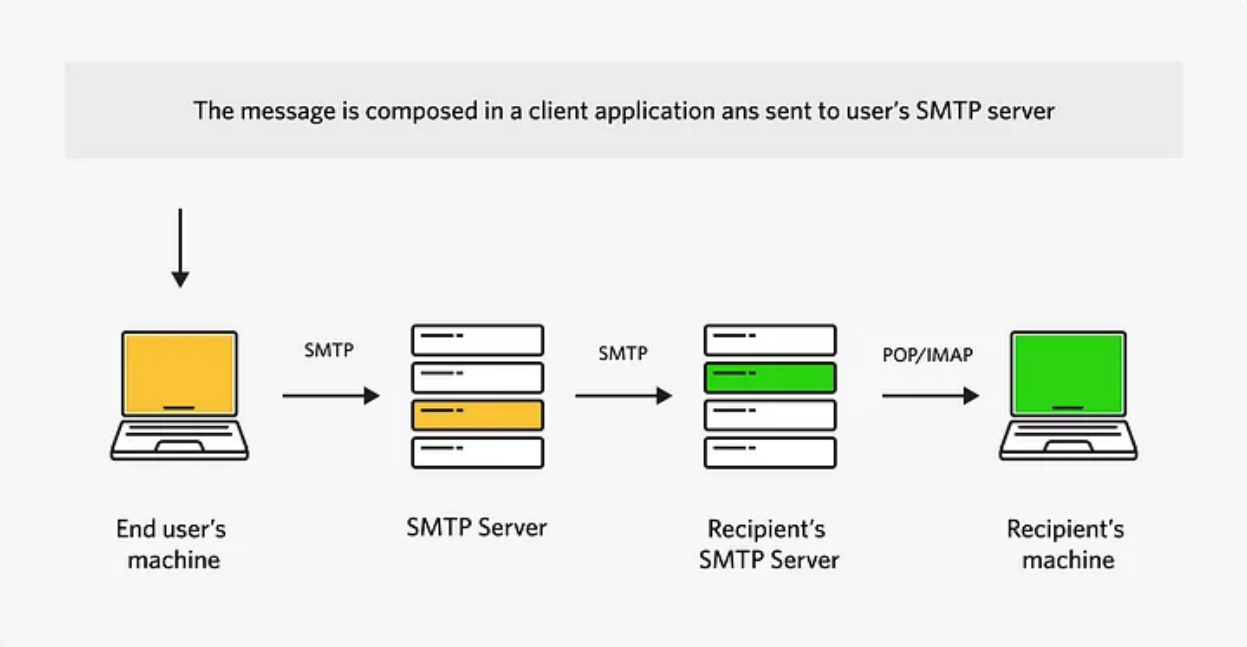
The SMTP server uses the Domain Name System (DNS) to locate the recipient's email server. DNS translates the recipient's email domain into an IP address, guiding the SMTP server to the correct destination.

Sending the Email to the Recipient's Server

The SMTP server forwards the email to the recipient's email server. If the recipient's server is temporarily unavailable, the SMTP server will retry several times before giving up and sending a delivery failure notification.

Storing the Email

The recipient's email server receives the email and stores it in the recipient's mailbox. It may also perform spam and virus checks to ensure the email's safety.



What is Firewall?

Firewall is system designed to prevent unauthorized access from entering a private network by filtering the information comes from internet. Lets take an example for understanding, When you visits your friends home(society) at a entry gate security guard ask us where u have to go and all if your friend permits then and then you can go. Here security guard acts as a firewall.

Man In middle:-

When an attacker intercepts communications between two parties who believe their interaction is secure.

Common examples:

An attacker establishes a free Wi-Fi in a Starbucks, a user connects to the network to check their bank balance and the attacker collects their username/password when they authenticate. The user and the bank are unaware.