Data study

Protocol

- TCP (Transmission Control Protocol): one of the most widely used network layer protocols. TCP ensures that packets of data are delivered reliably and in the correct order to the destination. It does this by establishing a connection between the sender and the receiver, and by using acknowledgments, retransmissions, and flow control mechanisms. TCP is suitable for applications that require high reliability and accuracy, such as web browsing, email, and file transfer.
- UDP (User Datagram Protocol): another common network layer protocol. UDP does not guarantee the delivery or the order of packets, and it does not establish a connection between the sender and the receiver. It simply sends packets of data as fast as possible, without waiting for acknowledgments or retransmissions. UDP is suitable for applications that require speed and efficiency, such as video streaming, online gaming, and voice over IP.
- ICMP (Internet Control Message Protocol): a network layer protocol that is used for diagnostic and error reporting purposes. ICMP sends and receives messages that indicate the status and problems of the network, such as ping requests, echo replies, destination unreachable, time exceeded, and parameter problem. ICMP helps to troubleshoot and maintain the network by providing feedback and information.
- Datagram or packet a piece of data which is small part of the whole data
- The header of a data packet contains information that allows for the actual transmission of the data packet. Sender IP, receiver IP, checksum, type of data packet,size of data packet, ID for resemble, etc.
- Payload: data can be image , video ,text, audo.
- Trailor: not all data packet contain it. Signal of end of packet. Usually consist of additional error checking.
- Packet type:
    - Data: the packet that contains acutal data such as text, vieo, image
    - Control: These packets are not primarily used to transfer actual application data. Instead, they are involved in managing, controlling, and ensuring the proper operation of the network. These packets serve to maintain the network's integrity, troubleshoot, manage traffic flow, and handle error detection.
- TCP and UDP are in Transport layer
- IP (internet protocol) found in network layer

- HTTP: hypertext, transfer protocol in application layer. Used for communicatin between web browser and web server
- FTP: file transfer protocol, in application layer used for transferring file between lient and a server over a network. Example uploading or downloading file between devices
- SMTP(Simple Mail Transfer Protocol) email transmission, a protocol for sending and receiving email message across the network.

- DNS (Domain Name System) is a hierarchical and decentralized naming system that translates human-readable domain names into IP addresses
    - Utilizes a distributed database system to store and manage domain name information
    - Employs a client-server model, with DNS clients querying DNS servers to resolve domain names
- The application layer is the top layer in network models, enabling communication between applications on different systems. It includes crucial protocols like HTTP for web browsing, FTP for file transfer, SMTP for email, and DNS for domain name resolution. These protocols define how applications exchange data, specifying formats and rules for communication. They rely on lower-layer protocols for data delivery and play a vital role in everyday internet activities like browsing websites, sending emails, and sharing files.

IOC (Indictor of compromise): is a piece of evidence or data that suggests that a security breach, compromise, or malicious activity has occurred or is occurring within a network or system. When an IoC is "detected," it means that some form of suspicious or malicious activity has been identified, potentially signaling that an attacker has gained unauthorized access to systems or data.

Attack type:

DDoS (Distributed Denial of Service) Attack: is designed to overwhelm a network, service, or server with a flood of traffic to make it **unavailable** to legitimate users
The attacker **take control a large number of devices** (computers, IoT devices, servers) to send massive amounts of traffic to a target system or server, either by making requests to a server or by exploiting vulnerabilities.
The goal is to **overload** the server, causing it to become **unresponsive** or **crash**, denying legitimate users access to the service or website.

Intrusion Attack (Unauthorized Access):

These attacks are aimed at gaining control over a system to steal, modify, or destroy data, or to use the system for malicious purposes.