Networking Fundamentas & Exploits

Most modern computers operate on a network. A network is a collection of computers (nodes) that allow for the communication and sharing of data between them.

Networks allow things like: - File sharing - Multiplayer games - Administration control over multiple computers - The internet - More…

In order to communicate with other computer, they need to have a “name” assigned to them.

One of the most common naming protocols is called IP Adress (Internet Protocol Address).

IP Adresses are 32-bit numbers that are used to identify a computer on a network. (Think of it as a phone number)

When a computer talks to another computer, it needs to know the IP adress of the other computer.

Internet Protocol has two versions in use (IPv4 and IPv6). IPv4 is the most common one.

IPv4 uses a 4 byte identifier for its adress. This means that there are 2^32 possible IP adresses.

A private network is a local network that can only be seen by that network.

Reserved address blocks: - 10.0.0.0 - 10.255.255.255 - 172.16.0.0 - 172.31.255.255 - 192.168.0.0 - 192.168.255.255

Internet traffic is routed through a series of routers. Routers are devices that forward traffic from one network to another.

It does so through NAT (Network Address Translation).

NAT provides a way to take a single IP Address connected to the internet to service a lot of private ip adresses.

Computers use packets as units of data and their control information

Networking Devices operate on a 7 later model called OSI (Open Systems Interconnection)

This is a conceptual model that standarizes computing communications

The security principle it follows is called Abstraction.

A packet that is generated by a program and desires to communicate with another passes through all seven layers of the OSI model.

Layer 1: Physical Layer

- Handles the actual transfer of information via a physical medium (wires, cables, etc)

Two types of connections: - Wireless: TRansmission of data via radio waves (WLAN: Wireless LAN) - Wired: Transmission of data via wires (Ethernet, USB, etc)

Layer 2: Data Link Layer

- Interface between two physical devices. Connects two physical nodes and allows for data transfer between them.
- MAC: Media Access Control determines privileges between phyisical layer, checks for errors in physical transfer, manages frames and more

A frame is a container for a packet. It contains information about total packets being sent, the packet number, and the packet itself.

In order for devices to communicate with each other in this layer, they need privilege access.

All physical network devices have a MAC adress (kinda like ip adress, but a different protocol)

MAC adreses use 0-9 and A-F (hexadecimal)

Example: 00, 1A, 3F, F1, 4C, C6

The first 3 are the Organizationally Unique Identifier (OUI) which is assigned to the manufacturer of the device. The last 3 are the Network Interface Controller (NIC) which is assigned to the device itself.

Layer 3/4: Network/Transfer Layer: Manges the transfer of variable length packets between computers on a network.

This is where IP and IP Adresses are used. More Abstract networking now, addresses can change

These layers can be refered to as TCP/IP

These layers deal with getting packets from source to destination, splitting up larger packets into smaller packets, and reassembling packets at the destination.

At these layers, a connection is established between two computers on a network. This is done with a TCP handshake. A TCP handshake is a process which estabishes and verifies a connection between two computers

First packet -> SYN (Synchronize Sequence Numbers) Second packet -> SYN-ACK (Synchronize Sequence Numbers and Acknowledge) Third packet -> ACK (Acknowledge)

Layer 5/6/7: Application/Session/Presentation Layer

These next layers deal with applications.