Network Security

Date
Page

Layer 1:- (Physical layer)

① **Repeater** :- Repeater are network devices operating at Physical layer of the OSI model that amplify or regenerate an incoming signal before retransmitting it.

⊙ It work on Physical layer.

let say we create 200m LAN & connect different devices & if any signal moves on this LAN till 200m only signal after 200m gets weak it means strength get weak & signal gets corrupted. Then we use repeater to regenerates the signal strength.

Types of Repeater :

① Analog Repeater } A/c type of signal they are regenerate
Digital Repeater }

② Wired & Wireless → A/c type of network

③ local & Remote → A/c to domain of length.

Advantages :-

① They are easy to install & easily to extend length ~~they~~ & coverage are of network.

② They are cost - effective.

③ Help in forwarding messages from device A to B.

④ Repeater not required any processing overhead.

⑤ They can connect signal using different type of cables.

Disadvantages :-

⑤ It cannot connect dissimilar network.

② They cannot differentiate b/w actual signal & noise.

③ They cannot reduce network traffic or congestion.

④ Most network have limitation upon the no. of repeaters that can be deployed.

(2) HUB :-

- A Hub is a layer 1 device and operate at the physical network of the OSI model.
- Since, it works in the physical layer, it mainly deals with the data in the form of bits & electrical signals.
- A Hub is mainly used to create a network & connect devices on the same devices only.
- Hub forwards the incoming messages to the other devices without checking for any error or processing. It only knows the device is connected to one of its port.
- When data packets arrive at one of the port of Hub, it imply copies the data to every port. it means Hub broadcast messages.
- Transmission mode is Half Duplex.
- Hubs are Passive devices, they don't have any software associate with it.
- Ports of Hub devices → 4/12.

Types of HUB :-

(1) Active HUB: It amplify & regenerate the incoming signal before Broddcasting them.

(2) Passive HUB: It connect node in a star configuratio by connecting wiring from nodes. It also Broadcast the signal onto the network without amplifying the signal.

(3) Intelligent HUB:
These are active HUB that provide additional network management facilities.

Layer 2 : (Data - link layer)

① Switch :-

Switch is a layer 2 network connected device and it works on both Physical & Data-link layer & it interprets the data in the form of data frames. It act as a multiport bridge in the network. They connect device in a network & used Packet-switching to send, receive or forward data packets or data frames over the network.

- It supports Unicast, Multicast & Breadcast Communication
- Ports of Switch → 24/28
- It perform error before forwarding data to the destined port.
- Transmission mode is Full-Duplex.

Types of Switch :-

(I) Unmanaged Switch
(II) Managed Switch
(III) LAN Switch
(IV) POE (Power Over Ethernet) Switch.

② Bridge :

- Bridge is a layer 2 network-connecting device. It works on Physical and Data-link layer of the OSI model. In Physical layer, it act as a repeater and while in Data-link layer it check the MAC address of the data frames for its transmission.
- Used for filtering the signals. It means it can discards the faulty data frames & will allow only the error-less data frames in the network.
- It also maintain the table containing the physical addresses of all the devices in the network.

Types of Bridge :

① Transport Bridge : Bridge work as a transmission medium b/w two devices.

② Routing Bridge : Routing Bridge have their unique identify. They can be easily identify by the network devices.

layer 3 :-

(i) Router :

- Router is a layer 3 network connected devices. It works on Physical, Data-link & Network layer. It is an inter-networking device which can connect devices of different network.
- It can connect two Physically & logically different network devices with each other.
- It is used to connect & route the traffic. In other words, a router is the gateway of network.
- Router maintain a routing table using the Routing Algorithm.
- When a data packet is received at a router, it first check the IP address, if the IP address is same as the networks IP address, it receives the data packet, else it forwards the data packet to the destination IP address using Routing table.

Firewall :-

- A Firewall is a device that filter all traffic between the protected or less trustworthy network. The purpose of a firewall is to help untrusted things outside the protected environment.

- It can be hardware or software device which monitors all incoming & outgoing traffic based on defined set of security rules.
- It accepts, reject or drop that specific traffic.

accept : allow the traffic
reject : block the traffic but reply with unreachable error
drop : block the traffic with no reply.

- A firewall is a network access control device that design to deny all traffic which are not protected or less trustworthy.

Types of Firewall :-

1. Packet filtering
2. Stateful Inspection Firewall (Circuit)
3. Proxy Firewall
4. Personal Firewall.

Different Types of Network layer Attacks :-

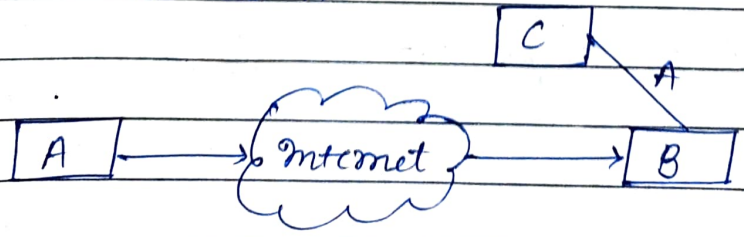
1. Active Attack :

Attack to alter the network.

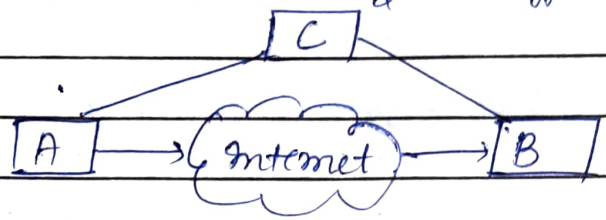
Active attacks involves some modification of the data stream or creation of false statements.

Types :-

(i) Masquerade : This attack takes place when one entity pretend to be other entity. C pretend to be A.



(II) Modification of message: It means that some some part of the message is modify or that message is delayed or recorder to produce an unauthorized effect.

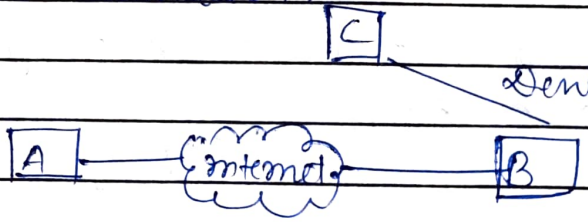


(III) Repudiation: This attack is either done by sender or receiver. It means sender or valver deny the message. The sender or receiver can deny later, that she has not send or receive the message.

(IV) Replay: It involves the passive capture and its subsequently transmission to produce an atthosized effect.

(V) DOS (Denial of Service): It prevent the normal use of communication facilities. This attack may have specific target.

eg An entity may send message directly to a particular destination.



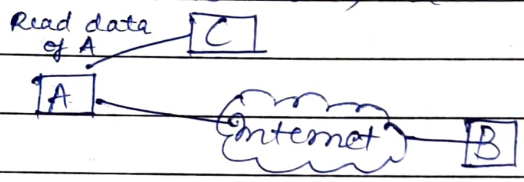
Denial of Service (Overload server by sending false requests).

(2) Passive Attack :

- A passive Attack attempts to learn or make use of information from the system but does not affect system resources.
- Passive attack are in the nature of case dropping or monitoring of transmission.

Types :-

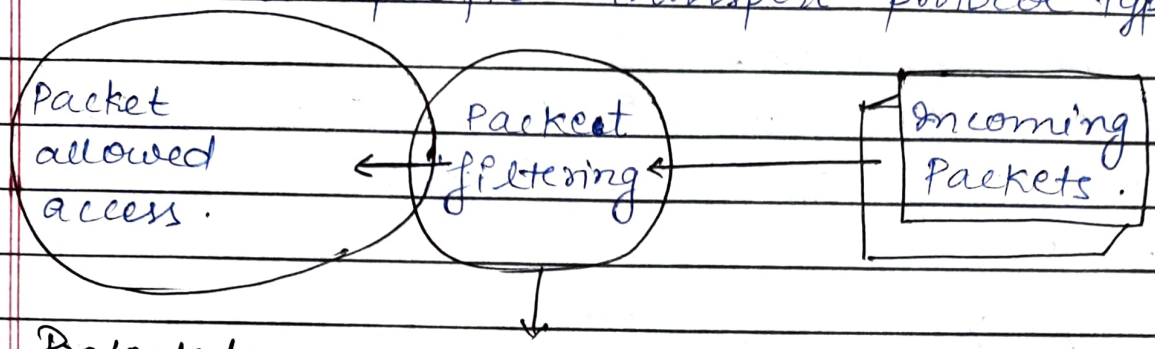
(i) Release of message content
(ii) Traffic Analysis is used to analysis the address.
(i) Telephonic conversation, electronic mail, transfessed file.



Types of Network layer attacks :-

(i) Eaves dropping
(ii) Data Modification
(iii) IP address spoffing
(iv)
(v) Compromise attack
(vi) Man-in middle attack
(vii) Packet sniffer attack
(viii) Fishing or DNS spoffing
(ix) DOS attack
- Three types : Simple DOS
  coordinated DOS
  Distributed DOS attack.

Packet filter firewall which work on network layer & control access the packet on the basis of packets address or specific transport protocol type.



So we will apply set of rules on each packet and based on the outcome, decide to either forward or discard the packet.

Stateful Packet filtering firewall :-
(or circuit)

- This is situated on layer 3 and 4 of OSI model keep track of the state of network connection
- Stateful firewall examine the content of each packet with regards to their placement within the packet series.
- It is created by TCP / UDP (Table)

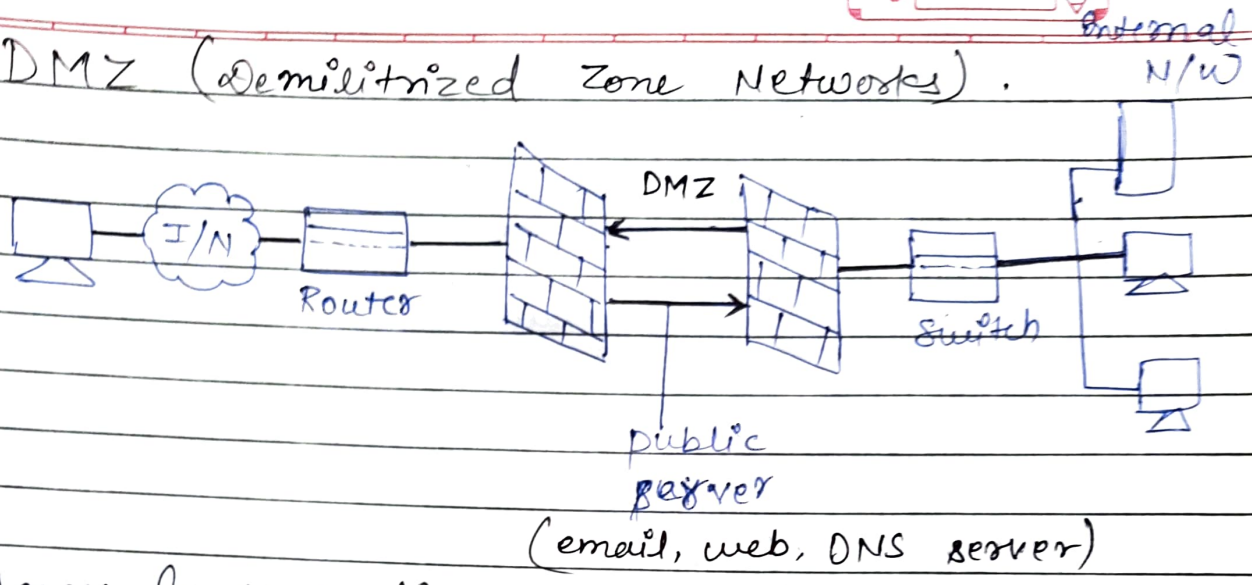
Appⁿ Proxy firewall :-

Appⁿ layer ~~Proxy~~ firewall simulates the proper effect of an appⁿ so that appⁿ received only request to act properly

Personal firewall :-

eg. window firewall, TCP wrappers, IP chang, IP Table

DMZ (Demilitrized Zone Networks).



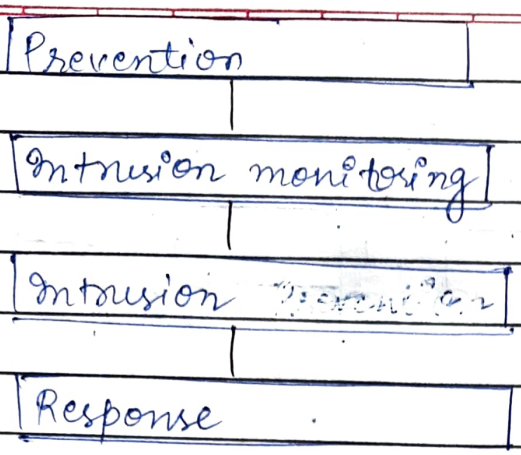
Access Control list :-

Before firewall activity we can use access control list Because firewall security well performed by ACL All are list which contains some list that determine whether access should be granted or denied to a particular address.
Access and Denied these two are permit by ACL.

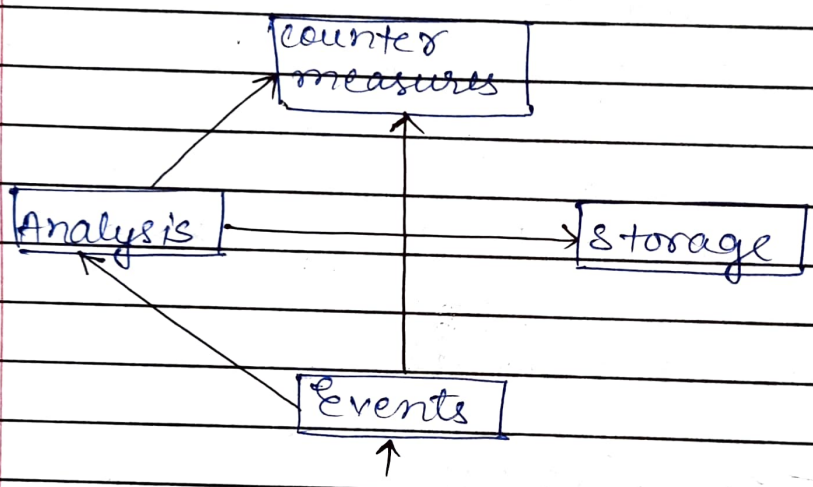
IDS. (Intrusion Detection System).

It is a process of monitoring the events occuring in a computer system or network and analysing them for sign of intrusion.
Intrusion can be defined as set of actions that attempt to comprimises the integrity and ability of resources
Eg Car alarm

Infrastructure -



Model of IDS



IDS
Once the Intrusions has been detected, issues alert notifying admin of the threat.
On the next steps -
Undertaken either by admin or IDS itself

Benefits	Host	Network
Deterrence	Strong for insider Weak for outsider	Weak for insider strong for outsider
Detection	Strong insider detection.	Weak insider detection strong outsider
Response	Weak real ~~tg~~	Strong response against outside attack
Damage Assesement	Excellent for determining extent for comprimse	Very weak damage assisment capabilities
Attack Anticipation	Good at trending & detecting suspicious behaviour pattern	None.