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 :-

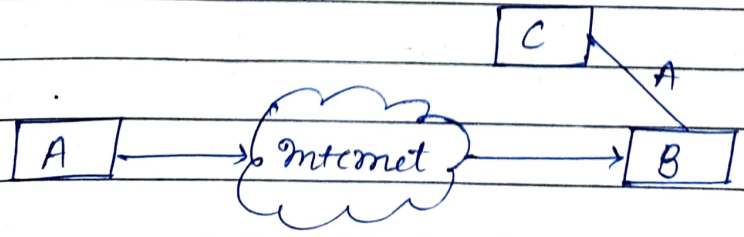
1. Active Attack :

Attack to alter the network.

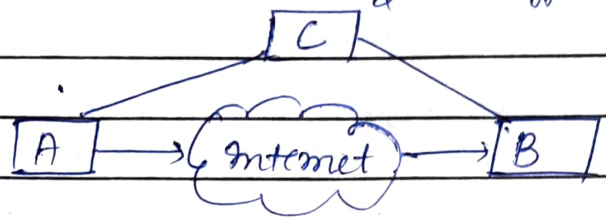
Active attacks involves some modification of the data stream or creation of false statements.

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.

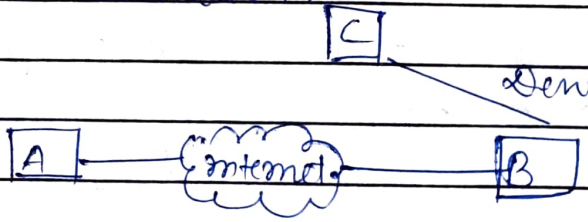


(III) Repudiation: This attack is either done by sender or receiver. It means sender or valver deny the message. The sender or receiver can deny later, that she has not send or receive the message.

(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.



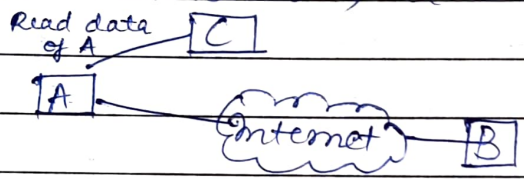
Denial of Service (Overload server by sending false requests).

(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.

→ Firewalls :- → It is a combination of hardware and software device which monitors and control the incoming and outgoing traffic based on pre-defined rules.

→ It acts like a barrier

→ Host based
which is inside our computer system (software based)

Network based
which is for all the whole network. Scans the whole network (hardware based)

→ Two categories :

i) Packet Filtering Firewall.

→ Operates on layer 4 (Transport layer)

→ Checks IP header, TCP header
(IP address) (Port Number)

→ Can block a IP address, Can block Full Network

→ Can block a Service (http, ftp)

ii) Access Control list.

→ It is used to filter the Traffic in Network infrastructure

→ It reduces Network traffic

→ Network admin can block the unknown accessing

→ Two types, Numbered - we use Specific no to apply this ACL

→ ~~Two levels~~

→ Supports two types of filtering

Standard ACL

Can filter only on the Source IP address inside a pocket

Extended ACL

Can filter on both Sou and Destination IP addre inside a pocket.

→ Inbound and outbound Connection

→ DMZ -: → Demilitorized zone is a high security area which comprises of hosts that provides services to the users outside the internal LAN. [Web server, Mail server etc]

→ It uses two firewall

One is b/w External network & DMZ

Other " " DMZ and Internal network

→ One big advantage of DMZ is that, it provides an additional layer security to an ~~organi~~ organization's LAN, an external attacker ~~may~~ can only access the hosts in DMZ and not to any other internal network.

→ Audit Rule -: It is basically a record or a database which consists of all the information of the messages or data packets that has been exchanged like the date, time, location and IP addresses.

Intrusion Detection System -:

Intruder - It is a person who tries to gain on unauthorized access to a system or a network

An intruder can:

- Corrupt the whole data
- Retrieve / Steal the information
- Imbalance the whole network environment

Two types:

Outside Intruder (Masquerade), Unauthorized user

Inside Intruder (Misfeasor), Authorized user

II is more harmful than OI, because it is very much difficult to detect or identify them.

Intrusion - An unauthorized access by an intruder

IDS: → It is a system which continously monitors the network traffic and all the data packets that are moving inside the network. and checks for any suspicious content

→ Checks whether the network resources or privileges are not being misused

→ Works at backend and as soon as it detects any suspicious activity, it sends an alert signal / message to the Network Admin.

→ Two types -:

i) NIDS, → Network based

→ Monitors, Capture and analyze Network traffic

→ Detects malicious data present into packets

→ If it finds any Malicious data, it monitors, captures and Matches that traffic (packet) to library of known attack [Analysis part]

ii) HIDS, → Host Based

→ Installed on individual host or device on network

→ It monitors the data packets from the device only and alerts admin if any suspicious activity is detected

→ How it detects ?

Snapshot

Existing System → Previous System

(Running System) (Initial / Ideal System)

If SS is Same → OK

If SS is not Same → Suspicious activity detected

(Some files may be deleted or modified)

→ Two Detection Methods -:

i) Signature Based IDS, → It matches the pattern

→ Creates a database of all the known attack patterns

→ Cannot identify a new attack

ii) Anomaly Based IDS, → It detects Deviation

→ Whenever someones deviates from its natural behaviour /role / domain, AIDS detects that intrusion / deviation

Network Security

* Comparison of IDS with Firewalls :-

→ Installing IDS and firewall offers cyber-security sol^n to protect n/w.

→ IDS is a passive monitoring device that helps detects threat and generate alerts. An IDS provides no protection to the end-point

→ Firewall is an active protective device that is more like IPS. It performs analysis of the metadata of the n/w packets and helps block/allow the traffic based on some pre-set rules.
This creates a boundary on which some types of traffic or protocols cannot pass.

* Adv. of IDS :-

(i) It keeps a check on routers, firewalls, key servers and files and uses its database to raise the alarm & send notifications.

(ii) Offers centralized management for the correlation of the attack.

(iii) It analyzes diff. attacks, identifies their patterns and helps the administrator to organize and implement effective control.

(iv) Acts as additional layer of protection for the company.

* Disadv. / Challenges of IDS :-

(i) Ensuring Effective Deployment :-

→ Deploying IDS can be tricky, and if not done properly it may create vulnerabilities for critical assets.

(ii) Understanding and Investigating Alerts :-
→ IDS alerts gives very little info. which is sometimes hard to investigate.
→ also, investigating the IDS alerts can be time and resource-intensive, which may require additional info. to identify the seriousness of the attack.

(iii) Managing a High Volume of Alerts :-
→ Since, there is vast majority of attacks are generated by IDS, it may put burden on internal teams to identify each of them.

(iv) Knowing How to Tackle Threats :-
→ Sometimes a home IDS gives false alarms, so ~~loop~~ cyber security team needs to be updated with latest updates in IDS and key domains of cyber security.

* IPS (Intrusion Prevention System) :-
→ IPS is also known as Intrusion Detection and Prevention System.
→ Major function of IPSs are to identify malicious activity, collect info. about this activity ~~and~~, report it and attempt to block or stop it.
→ IPSs are ~~often~~ contemplated as augmentation of IDS because both operate n/w traffic and system activities for malicious activity.
→ IPS typically record info. related to observed events, notify security administrators/

and produce reports.
→ May IPS also respond to threats by attempting to prevent it from succeeding.
→ They use various response techniques which involve the IPS stopping the attack itself.

* Classification :-
4-types

1. Network-Based Intrusion Prevention System (NIPS) :-
→ It monitors the entire network for suspicious traffic by analyzing protocol activity

2. Wireless IPS (WIPS) :-
→ It monitors wireless network for suspicious traffic by analyzing wireless networking protocols.

3. Network Behaviour Analysis (NBA) :-
→ It examines n/w traffic to identify threats that generates unusual traffic flows, such as distributed denial of service attacks, specific form of malware & policy violations.

4. Host-Based IPS (HIPS) :-
→ It is an inbuilt s/w package which operates a single host for doubtful activity by scanning events that occur within that host.

* Detection Method of IPS :-

1. Signature-Based Detection :-
→ It operates packets in n/w and compares with pre-built and predefined attack patterns known as signatures.

2. Statistical anamaly-based Detection :-
→ It monitors n/w traffic and compares it against an established baseline.
→ The baseline will identify what is normal for that n/w and what protocols are used.
→ However, it may raise a false alarm if the baseline is not intelligently configured.

3. ~~Stateful protocol analysis detection~~ :-

3. Policy-Based detection :-
→ It requires system administrators to configure security policies based on an organization's security policies and n/w infrastructure.
→ If any activity breaks a defined security policy, an alert is triggered and sent to the admin.

* Comparison of IPS with IDS :-
→ IDS is more of a alerting system that lets an organization know if anamalous or malicious activity is detected.
The IPS takes this detection one step further and shuts down the n/w before access can be gained or to prevent further movement in a n/w.

* Audit Trail :-

→ Audit trail keeps track of different action that took place for an activity in an chronological order.

→ Therefore, the audit trail records :-

- Who : user or appl° program and a transaction no.
- When : Date and Time
- Where : location of user
- What : Data that is being worked upon or is modified.

→ e.g, when checkout from the counter of a market after shopping, the bill is type of audit trail, where we fill all necessary info.

* Why Audit Trail :-

→ Audit Trail is one of the most essential thing for any company or organization as they keep track of all the things and any chaos / irregularity in the future can be rectified.

→ It enhances security of an organization.

→ It makes an organization trustworthy.

→ All types of industries and organizations makes it mandatory to maintain an audit trail as they deal with sensitive info. and data.

* Types of Audit Trail :-

1 External audits :-

→ An external audit is an independent examination of the financial statements prepared

by the organization.

→ External audits are performed by CPA (certified public accountants) firms hired by a business. to ensure correctness and accuracy of accounting records maintained by a company.

2. Internal Audits :-

→ They are performed within the organization, one department performs audit for other department

→ This helps in growth of an organization and take actions for further growth and steps do avoid upcoming risk.

3. Internal Revenue Service (IRS) Audit :-

→ Performed do avoid any tax violations.

→ It is a type of external audit performed on organizations that are accused guilty of providing wrong tax data.

* Advantages :-

1. Fraud Preventions.
2. Easy verification
3. Maintaining Financial History.
4. Easy recovery.

* Disadvantages :-

1. Maintainance cost :-

→ extra maintainance that it requires, hiring of CA, cost of memory etc.

2. Security threats :-

→ The audit teams are taken care of but if fall in hands of a attack all data of a company will be leaked.

→ Malware -: Malware is a malicious software design-ed to break into, damage or gain authorized acces to a computer system without the owner's consent.

→ It attacks on our Client, Server or whole network

→ Six Types -:

i) VIRUS. Vital Information Resources Under Seige is a type of malicious software or program that corrupts our various files inside the System (~~Faster shortcuts, delete~~)

→ It replicates itself (a human force is needed).

→ First virus was [Boot Sector Virus ('BRAIN') (on Windows)
Creeper (on Networks)
ELK-Cloner (on PC's)

ii) WORM, Write Once Run Many is also a type of virus

→ It is self-replicating (Does not need any human force)

→ It overloads the Hard disk and RAM's space of Computers due to which System becomes slow and it hangs

iii) TROJAN HORSE, It is a ~~tag~~ fake Software which pretends to be useful but it is not, and when we download it, it infects our system

~~→ Mainly found in Banking sectors~~

→ They have Root kits

↓

they are the software packages which modifies the host's OS so that the mal-ware is hidden from the user, i.e. Concealed.

iv) R

iv) Phising. It generally clones a website and creates a duplicate one

→ It mainly hacks our login credentials (ID's, Passwords etc)

v) Ransomware, Once it is installed in the system it ~~hacks~~ encrypts or kidnaps the data and then they asks for ransoms

→ The ransoms are mostly asked to paid virtually through bitcoins so that the developer cannot get caught

→ It is mainly happens in Government sectors

vi) Spyware. It basically tracks our online activities. whenever we download any application from an open source, these spywares may also get installed (as they are very small)

→ The pop-up ads we get while watching a video etc are also a types.

IPS :- → IPS stands for Intrusion Prevention System

→ Designed to prevent malicious threats and activities detected by IDS in the network.

→ Unlike IDS, IPS not only detects the malicious activity but it takes action (in addition to notifying the administrator)

→ The IPS may drop a packet from the suspicious traffic, or release further traffic from that particular IP.