Network Security

UNIT-1 (Syllabus)

→ Networking Devices (layer 1,2,3)
→ Different types of network attacks
→ Firewall, ACL, Packet Filtering
→ DMZ, Audit Rule
→ Intruder IDS, IPS
→ Malware

→ **Networking Devices** -:

→ NIC (Network Interface Card), without this card networking cannot be done, it is attached on the backside of our system. Also known as Ethernet Card or LAN card

→ It converts parallel data stream into serial data stream and vice versa. Two Types i) Media Specific
ii) Network Design Specific

=> Types of Networking Devices :

① **Hubs** - → It operates at Physical layer.

→ It is a Networking device that is used to connect multiple systems in a single LAN network.

→ When Hub receives any signal on its port, it forwards the signal from all ports except on the port on which the signal arrived.

→ Two types i) Active HUB
ii) Passive HUB

Scanned by TapScanner

(2) Bridges → → It operates at Data Link layer

→ It divides a larger network int Smaller segments

→ It has a per port collision domain, means if there is a collision at one port, other ports will not get affected.

→ Three types i) local Bridge
ii) Remote Bridge
iii) Wireless Bridge

(3) Switches - → It operates at data link layer

→ It is a networking devices (like Hub and Bridge) that is used to connect multiple Systems in a LAN segment.

→ It receives data signal ~~and~~ in the form of Fromes

→ Supports three methods of Switching
i) Store and Forword
ii) Cut and Through
iii) Fragment Free

(4) Repeaters - → It is a networking device, which regenerates the signal over the same network to its origi -nal strength

→ It operates at Physical layer

→ It is a 2 port device

→ It does not amplifies the signal

Scanned by TapScanner

(5) Routers -: → It is a networking device which forwa -rds data packets from one logical network segment to another

→ It transfers data in the form of packets

→ It operates at Network layer.

→ It has a routing table which keeps record of path of data packets as they move across the network.

(6) Gateways - → It is networking device which acts as a passage to connect two networks together that may work upon different networking modules

→ It can operate at any network layer

→ It is more complex than switch or router.

→ Network Attacks -:

1.) Active attack - It attempts to alter the system resour -ces, it involves modification of data stream or creation of false statement. Five types

i) Masquerade, this attack takes place when one entity pretends to be some different entity.

ii) Modification of messages, It means that some portion of a message is altered or reodered to produce an unauthorized effect

iii) Refudiation, This attack is done by the sender or receiver, they can deny later that they have send/ received a message.

Scanned by TapScanner

iv) Replay. It involves the passive capture of message and then resend it to produce an unauthorized effect.

v) Denial of Service. This attack may have a specific target, it involves disruption of an entire network by disabling it or overloading it by messages

2.) Passive attack → It involves the monitoring of messages

→ It attempts to learn or make use of the information from the system but does not affect the system resources. Two types:

i) Release of message content, This type of attack occurs when the attacker reads the content of the message that has been sent.

ii) Traffic analysis, In this attack, the attacker may not get the exact information from the message, but he could determine the pattern of the message exchanged.

Scanned by TapScanner

→ 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

Scanned by TapScanner

→ ~~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.

Scanned by TapScanner

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

Scanned by TapScanner

→ 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

Scanned by TapScanner

→ 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

Scanned by TapScanner

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.

Scanned by TapScanner