

Security Practice & System Security:-

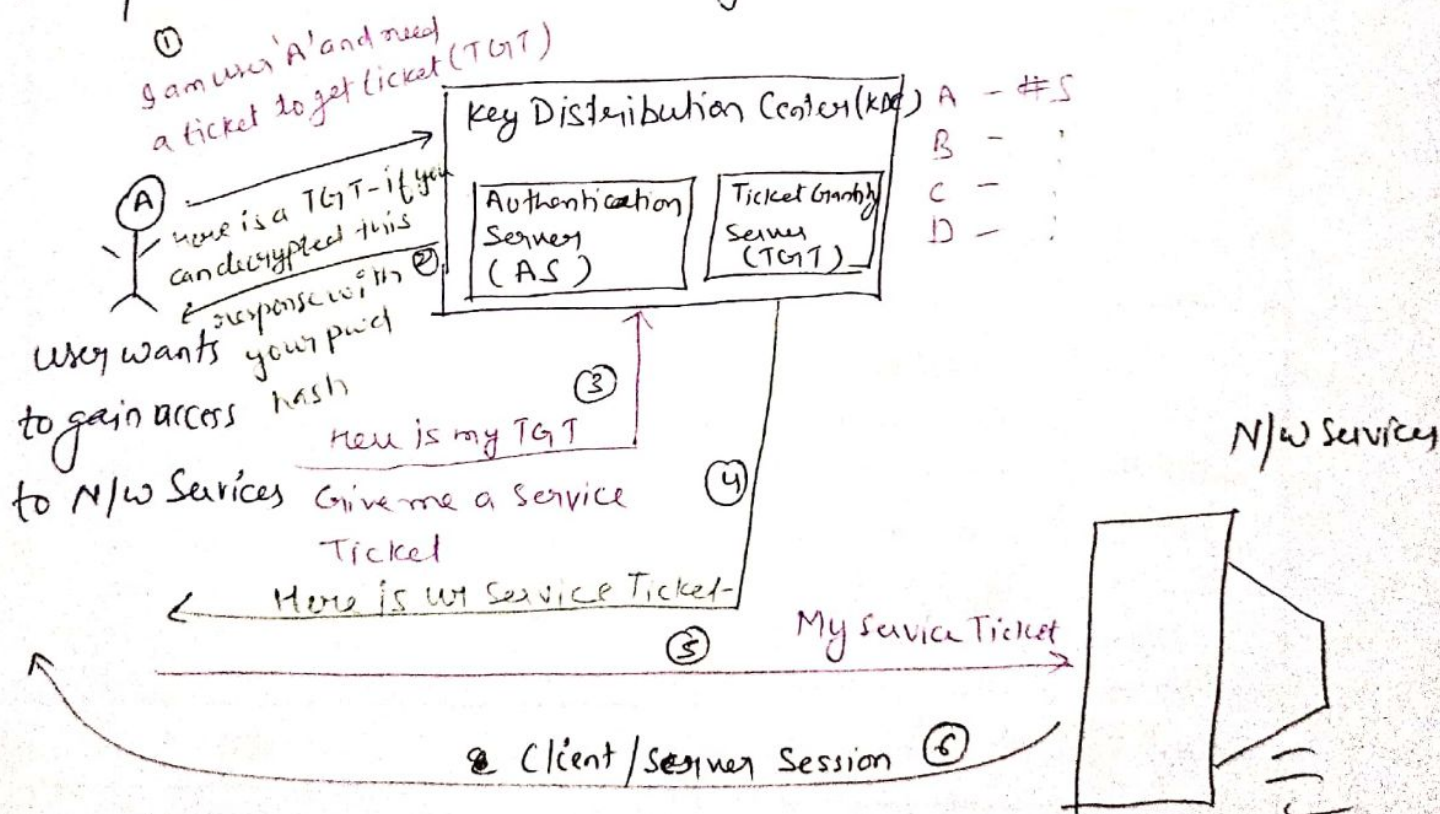
①

Kerberos:

It is a comp. N/w application authentication protocol

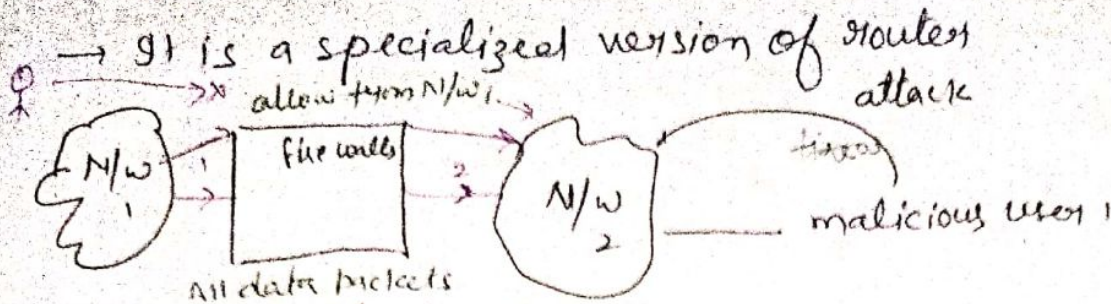
which works on the basis of "tickets" to allow nodes communicate over a non-secure n/w to prove their identity to one another in a secure manner.

- Client - Server Model
- Symmetric Key Model
- Requires a Trusted Third party



FIRE WALLS

②



Public
Internal

All data packets entering/leaving N/W pass through firewall and after examining firewall decide whether to allow or not.

Characteristics of good firewall

↳ All traffic must pass through firewall

(ii) Only authorized traffic should be allowed to pass

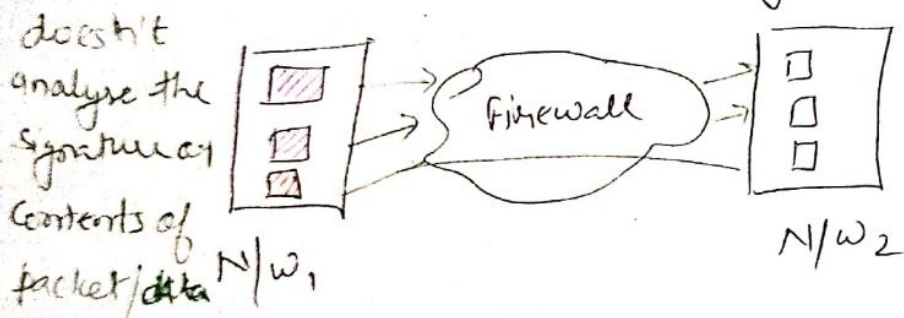
(iii) Firewall should be strong.

Limitation of firewall

① Insider's intrusion

② Direct internal traffic

③ Virus Attack



Types of firewall

ACL (Access control list) Firewall

Packet Filters

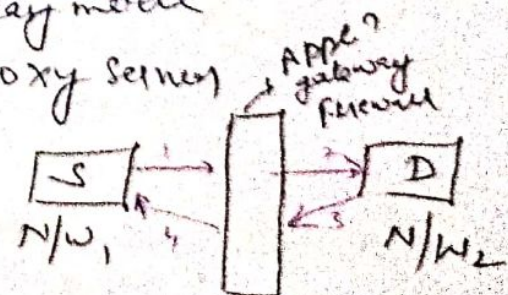
Use certain criteria to filter out the packet.

↳ IP addresses, Protocol, Port No
Various other Parameters

Application Gateways

↳ Acts as a relay mode

→ function as proxy server



Rule → Selection Criteria (condⁿ)
(if-else)

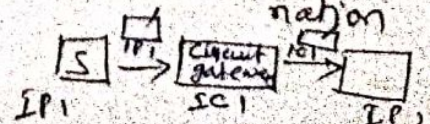
if ip-address = 127.0.0.1
then allow
else Block

Allow Packet

Block Packet

Circuit gateway

Creates a new conn
b/w itself and destination



Packet filter

Stateless

based on ACL

Stateful
used in all modern firewalls
monitor the ongoing traffic.

(3)

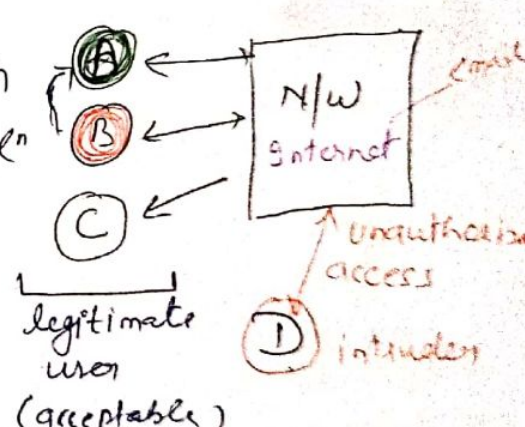
Intrusion → any unauthorized access.

Intruders are the one that try to intrude into the privacy of a network.

Type of intruders

① Masquerader : - user with no authority to use the system.
outsider ① → Penetrates the security system as a legitimate users.

② Misfeasor : - Legitimate user with no permission to access a app.
insider ② Legitimate user with but misuses the privileges



③ clandestine user : They try to steal and use the credentials of their supervisor

Audit Records

are used to record information about the activities of users.

Types of Audit Record

Native Record

Detection-specific Record

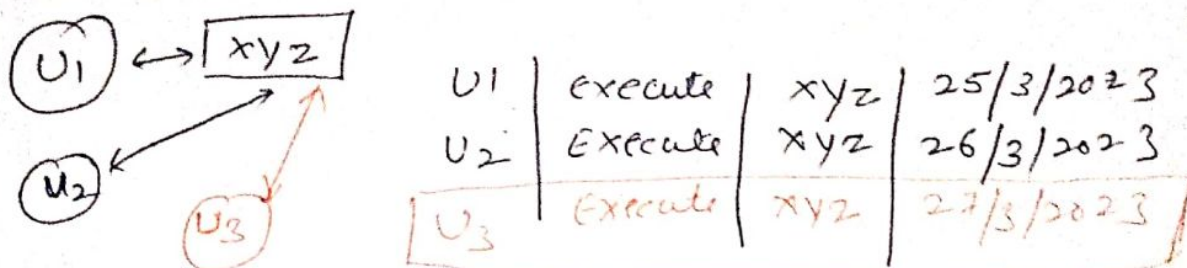
Native Records

↳ Stores all action of all users.

(4)

Detection - specific Records

↳ Collects info specific to intrusion detection



Intrusion Detection:

↳ Education, Engineering...
Ram - 2 hours of internet
Mohan - 4 hours. Movies, torrents...

Statistical Anomaly Detection

behaviour of user is analyzed over a period of time and rules are created to differentiate b/w legitimate and illegal users.

Rule Based Detection

Anomaly detⁿ shows
> shows

Penetration identification

↓
expert intelligent system

(packet transmission)

Threshold detection

2 hours. $\begin{cases} +0.5 \\ -0.5 \end{cases}$

Certain threshold are defined and if that threshold is crossed, it is considered as intrusion

Profile-Based detection

Profiles are created and they are matched for any illegal activity

Distributed Intrusion Detection

DIDS → [Win] [Linux]

Honey Pots

↳ it is trap that attracts

potential attackers.

