Experiment No 9

Aim: Design of personal firewall using iptables.

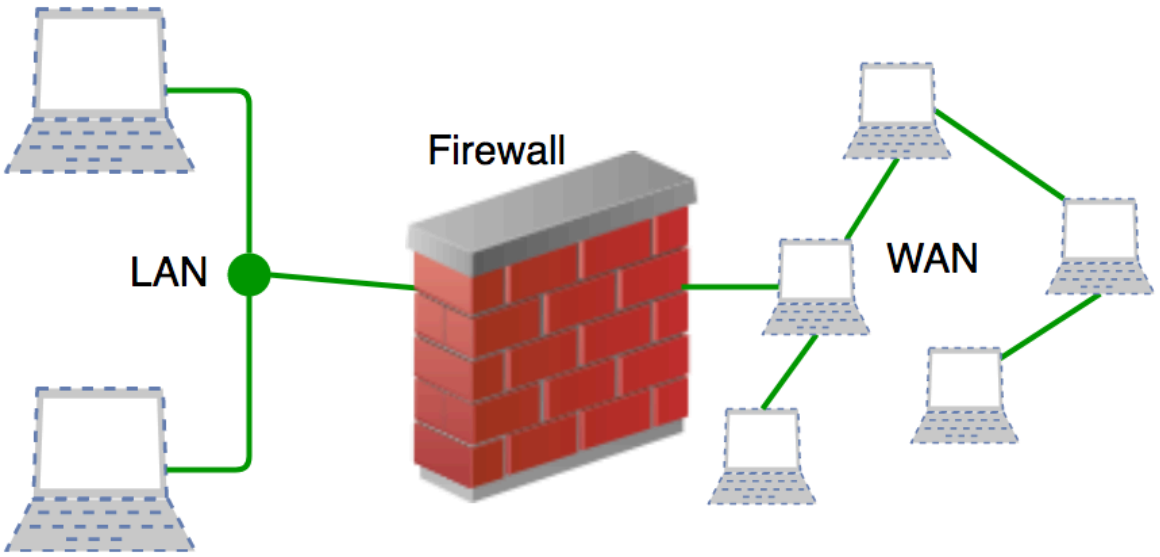
Theory:

A firewall is a network security device that prevents unauthorized access to a network. It monitors both incoming and outgoing traffic using a predefined set of security to detect and prevent threats.

What is Firewall?
A firewall is a network security device, either hardware or software-based, which monitors all incoming and outgoing traffic and based on a defined set of security rules accepts, rejects, or drops that specific traffic.

Accept: allow the traffic
Reject: block the traffic but reply with an “unreachable error”
Drop: block the traffic with no reply

A firewall is a type of network security device that filters incoming and outgoing network traffic with security policies that have previously been set up inside an organization. A firewall is essentially the wall that separates a private internal network from the open Internet at its very basic level.



Designing a personal firewall using iptables involves creating rules to control incoming and outgoing traffic on a Linux system. Below is a basic design outline for a personal firewall using iptables:

Define Default Policies: Set default policies for INPUT, OUTPUT, and FORWARD chains to DROP or REJECT to ensure that traffic is only allowed if explicitly permitted.

sudo iptables -P INPUT DROP
sudo iptables -P FORWARD DROP
sudo iptables -P OUTPUT ACCEPT

Allow Established Connections: Allow traffic related to established connections. This ensures that responses to outgoing connections are allowed back in.

sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

Allow Loopback Interface: Allow traffic on the loopback interface, which is essential for internal communication.

sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A OUTPUT -o lo -j ACCEPT

Allow Specific Incoming Connections: Allow incoming connections for specific services or ports you want to make accessible from outside.

sudo iptables -A INPUT -p tcp --dport <port_number> -j ACCEPT
sudo iptables -A INPUT -p udp --dport <port_number> -j ACCEPT

Allow Outgoing Connections: Allow outgoing connections from your system.

sudo iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

Logging: Optionally, you can log dropped packets to track potential security issues.

sudo iptables -A INPUT -j LOG --log-prefix "iptables: INPUT DROP: "
sudo iptables -A OUTPUT -j LOG --log-prefix "iptables: OUTPUT DROP: "

Save and Apply Rules: Once you have configured the rules, save them and ensure they are applied on system reboot.

sudo iptables-save > /etc/iptables/rules.v4
sudo systemctl enable netfilter-persistent
sudo systemctl start netfilter-persistent

Commands:

```
student@LAB301PC22:~$ sudo su root
[sudo] password for student:

root@LAB301PC22:/home/student# apt-get install iptables
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
libip4tc2 libip6tc2 libxtables12
Suggested packages:
firewalld
The following packages will be upgraded:
iptables libip4tc2 libip6tc2 libxtables12
4 upgraded, 0 newly installed, 0 to remove and 100 not upgraded.
Need to get 527 kB of archives.
After this operation, 0 B of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 iptables
amd64
1.8.7-1ubuntu5.2 [455 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libxtables12
amd64
1.8.7-1ubuntu5.2 [31.3 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libip6tc2
amd64
1.8.7-1ubuntu5.2 [20.3 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libip4tc2
amd64
1.8.7-1ubuntu5.2 [19.9 kB]
Fetched 527 kB in 2s (282 kB/s)
(Reading database ... 213473 files and directories currently installed.)
Preparing to unpack .../iptables_1.8.7-1ubuntu5.2_amd64.deb ...
Unpacking iptables (1.8.7-1ubuntu5.2) over (1.8.7-1ubuntu5.1) ...
Preparing to unpack .../libxtables12_1.8.7-1ubuntu5.2_amd64.deb …
Unpacking libxtables12:amd64 (1.8.7-1ubuntu5.2) over (1.8.7-1ubuntu5.1) ...
Preparing to unpack .../libip6tc2_1.8.7-1ubuntu5.2_amd64.deb ...
Unpacking libip6tc2:amd64 (1.8.7-1ubuntu5.2) over (1.8.7-1ubuntu5.1) ...
Preparing to unpack .../libip4tc2_1.8.7-1ubuntu5.2_amd64.deb ...
Unpacking libip4tc2:amd64 (1.8.7-1ubuntu5.2) over (1.8.7-1ubuntu5.1) ...
Setting up libip4tc2:amd64 (1.8.7-1ubuntu5.2) ...
Setting up libip6tc2:amd64 (1.8.7-1ubuntu5.2) ...
Setting up libxtables12:amd64 (1.8.7-1ubuntu5.2) ...
```

```
Setting up iptables (1.8.7-1ubuntu5.2) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.6) ...



root@LAB301PC22:/home/student# iptables -L
Chain INPUT (policy ACCEPT)
target   prot opt source       destination

Chain FORWARD (policy ACCEPT)
target   prot opt source       destination

Chain OUTPUT (policy ACCEPT)
target   prot opt source       destination

root@LAB301PC22:/home/student# iptables -I OUTPUT -s 192.168.208.18 -d
192.168.208.6 -p icmp -j DROP

root@LAB301PC22:/home/student# ping 192.168.208.6
PING 192.168.208.6 (192.168.208.6) 56(84) bytes of data.
--- 192.168.208.6 ping statistics ---
116 packets transmitted, 0 received, 100% packet loss, time 117754ms

root@LAB301PC22:/home/student# iptables -I OUTPUT -s 192.168.208.18 -d
192.168.208.6 -p icmp -j REJECT

root@LAB301PC22:/home/student# iptables -I INPUT -s 192.168.208.18 -p icmp -j
ACCEPT

student@LAB301PC22:~$ ping 192.168.208.6
PING 192.168.208.6 (192.168.208.6) 56(84) bytes of data.
--- 192.168.208.6 ping statistics --- 55 packets transmitted, 0 received, 100% packet
loss, time 55294ms

root@LAB301PC22:/home/student# iptables -F
root@LAB301PC22:/home/student# iptables -t filter -I OUTPUT -m string --string
facebook.com -j REJECT --algo kmp

root@LAB301PC22:/home/student# iptables -t filter -I OUTPUT -m string --string
facebook.com -j ACCEPT --algo kmp
```