Roll No: 2103163
Batch: C32
Name: Om Shete

Experiment No 9

Aim: Design of personal firewall using iptables.

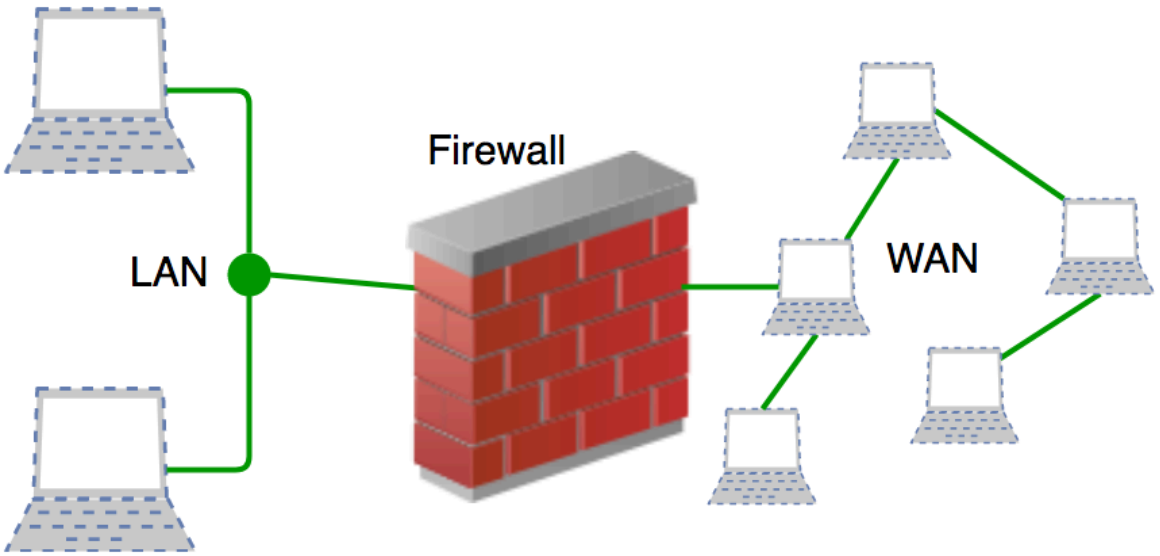
Description:

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:

Roll No: 2103163
Batch: C32
Name: Om Shete

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

Roll No: 2103163
Batch: C32
Name: Om Shete

Results:

```
  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 74 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
Get:2 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libxtables12 amd64 1.8.7-1ubu
Get:3 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libip6tc2 amd64 1.8.7-1ubuntu
Get:4 http://in.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libip4tc2 amd64 1.8.7-1ubuntu
Fetched 527 kB in 2s (276 kB/s)
(Reading database ... 310344 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@admini-OptiPlex-3050:/home/admini# ipconfig
Command 'ipconfig' not found, did you mean:
  command 'ifconfig' from deb net-tools (1.60+git20181103.0eebece-1ubuntu5)
  command 'iwconfig' from deb wireless-tools (30~pre9-13.1ubuntu4)
  command 'iconfig' from deb ipmiutil (3.1.8-1)
Try: apt install <deb name>
root@admini-OptiPlex-3050:/home/admini# ifconfig
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.161  netmask 255.255.252.0  broadcast 192.168.3.255
```

```
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.161  netmask 255.255.252.0  broadcast 192.168.3.255
        inet6 fe80::d60c:de4c:a36f:8c3b  prefixlen 64  scopeid 0x20<link>
        ether d8:9e:f3:2b:0d:92  txqueuelen 1000  (Ethernet)
        RX packets 4563  bytes 5598144 (5.5 MB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 2097  bytes 217870 (217.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 339  bytes 45851 (45.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 339  bytes 45851 (45.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:21:6b:fe:69:24  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@admini-OptiPlex-3050:/home/admini# ipaddress
Command 'ipaddress' not found, did you mean:
  command 'ip-address' from snap ip-address (1.0.0)
See 'snap info <snapname>' for additional versions.
root@admini-OptiPlex-3050:/home/admini# ip-address
Command 'ip-address' not found, but can be installed with:
snap install ip-address
root@admini-OptiPlex-3050:/home/admini# sudo-apt install ip-address
sudo-apt: command not found
root@admini-OptiPlex-3050:/home/admini# snap install ip-address
ip-address 1.0.0 from Daniel Dewberry (dwd-daniel) installed
root@admini-OptiPlex-3050:/home/admini# ip-address
ip         : 203.212.24.36
```

Roll No: 2103163
Batch: C32
Name: Om Shete

```
admini@admini-OptiPlex-3050:~$ sudo su root
[sudo] password for admini:
root@admini-OptiPlex-3050:/home/admini# apt-get update
Hit:1 https://packages.microsoft.com/repos/code stable InRelease
Ign:2 https://cloud.r-project.org/bin/linux/ubuntu jammy InRelease
Hit:3 http://security.ubuntu.com/ubuntu jammy-security InRelease
Hit:4 http://in.archive.ubuntu.com/ubuntu jammy InRelease
Hit:5 https://ppa.launchpadcontent.net/wireshark-dev/stable/ubuntu jammy InRelease
Hit:6 http://in.archive.ubuntu.com/ubuntu jammy-updates InRelease
Err:7 https://cloud.r-project.org/bin/linux/ubuntu jammy Release
  404  Not Found [IP: 108.158.61.26 443]
Hit:8 http://in.archive.ubuntu.com/ubuntu jammy-backports InRelease
Reading package lists... Done
E: The repository 'https://cloud.r-project.org/bin/linux/ubuntu jammy Release' does not have a R
N: Updating from such a repository can't be done securely, and is therefore disabled by default.
N: See apt-secure(8) manpage for repository creation and user configuration details.
root@admini-OptiPlex-3050:/home/admini# apt-get iptables
E: Invalid operation iptables
root@admini-OptiPlex-3050:/home/admini# apt-get install iptables
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  chromium-codecs-ffmpeg-extra gstreamer1.0-vaapi i965-va-driver
  intel-media-va-driver libaacs0 libaom3 libass9 libavcodec58 libavformat58
  libavutil56 libbdplus0 libbluray2 libbs2b0 libchromaprint1 libcodec2-1.0
  libdav1d5 libflashrom1 libflite1 libftdi1-2 libgme0 libgsm1
  libgstreamer-plugins-bad1.0-0 libigdgmm12 liblilv-0-0 libllvm13 libmfx1
  libmysofa1 libnorm1 libopenmpt0 libpgm-5.3-0 libpostproc55 librabbitmq4
  librubberband2 libserd-0-0 libshine3 libsord-0-0 libsratom-0-0
  libsrt1.4-gnutls libswresample3 libswscale5 libudfread0 libva-drm2
  libva-wayland2 libva-x11-2 libva2 libvdpau1 libvidstab1.1 libx265-199
  libxvidcore4 libzimg2 libzmq5 libzvbi-common libzvbi0 mesa-va-drivers
  mesa-vdpau-drivers pocketsphinx-en-us va-driver-all vdpau-driver-all
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libip4tc2 libip6tc2 libxtables12
Suggested packages:
```

Roll No: 2103163
Batch: C32
Name: Om Shete

```
root@admini-OptiPlex-3050:/home/admini# ip-address
ip          : 203.212.24.36
country     : India
country_iso: IN
country_eu : False
region_name: Maharashtra
zip_code    : 400070
city        : Mumbai
latitude    : 19.0748
longitude   : 72.8856
time_zone   : Asia/Kolkata
asn         : AS45243
asn_org     : FX Wireless Technology Solutions Pvt. Ltd.
root@admini-OptiPlex-3050:/home/admini# ^C
root@admini-OptiPlex-3050:/home/admini# 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@admini-OptiPlex-3050:/home/admini# iptables -I OUTPUT -s 203.212.24.36
root@admini-OptiPlex-3050:/home/admini# iptables -I OUTPUT -s 203.212.24.36 -d 203.212.24
root@admini-OptiPlex-3050:/home/admini# ifconfig
enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.161  netmask 255.255.252.0  broadcast 192.168.3.255
        inet6 fe80::d60c:de4c:a36f:8c3b  prefixlen 64  scopeid 0x20<link>
        ether d8:9e:f3:2b:0d:92  txqueuelen 1000  (Ethernet)
        RX packets 8657  bytes 11518308 (11.5 MB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 4196  bytes 406880 (406.8 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
```

```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 359  bytes 48217 (48.2 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlp3s0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:21:6b:fe:69:24  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@admini-OptiPlex-3050:/home/admini# ^C
root@admini-OptiPlex-3050:/home/admini# iptables -I OUTPUT -s 192.168.1.161 -d 192.168.1.193
root@admini-OptiPlex-3050:/home/admini# iptables -I OUTPUT -s 192.168.1.161 -d 192.168.1.193 -p icmp -j DROP
root@admini-OptiPlex-3050:/home/admini# ping 192.168.1.193
PING 192.168.1.193 (192.168.1.193) 56(84) bytes of data.
^C
--- 192.168.1.193 ping statistics ---
121 packets transmitted, 0 received, 100% packet loss, time 122887ms

root@admini-OptiPlex-3050:/home/admini# iptables -I OUTPUT -s 192.168.1.161 -d 192.168.1.193 -p icmp -j ACCEPT
root@admini-OptiPlex-3050:/home/admini# iptables -I OUTPUT -s 192.168.1.161 -d 192.168.1.193 -p icmp -j REJECT
root@admini-OptiPlex-3050:/home/admini# iptables -I OUTPUT -s 192.168.1.161 -d 192.168.1.193 -p icmp -j ACCEPT
root@admini-OptiPlex-3050:/home/admini# iptables -F
root@admini-OptiPlex-3050:/home/admini# iptables -t filter -I OUTPUT -m string --string whatsapp.com
iptables v1.8.7 (nf_tables): string: option "--algo" must be specified

Try `iptables -h' or 'iptables --help' for more information.
root@admini-OptiPlex-3050:/home/admini# iptables -t filter -I OUTPUT -m string --string whatsapp.com -j REJECT
iptables v1.8.7 (nf_tables): string: option "--algo" must be specified

Try `iptables -h' or 'iptables --help' for more information.
root@admini-OptiPlex-3050:/home/admini# iptables -t filter -I OUTPUT -m string --string google.com -j REJECT --algo kmp
root@admini-OptiPlex-3050:/home/admini# iptables -t filter -I OUTPUT -m string --string google.com -j ACCEPT --algo kmp
root@admini-OptiPlex-3050:/home/admini# iptables -I OUTPUT -s 192.168.1.161 -d 192.168.1.193 -p icmp -j ACCEPT
```