



UJAR TECH SOLUTION

NAME: Rithik varma

INTERN ID: UTS1103

TASK 10

Creating a Firewall with iptables or UFW:

Understand and practically identify to set up and manage a firewall using iptables or UFW (Uncomplicated Firewall) on a Linux system to control incoming and outgoing traffic, thereby strengthening system security.

PRACTICAL DESCRIPTION

Problem:- *Explore a Linux machine and build rules to block, allow, and monitor traffic based on IP, ports, and protocols — which is a core skill in system hardening, DevSecOps, and cybersecurity.*

Key Concepts of Firewall:-

A firewall is like a security guard for your system/network. It decides which traffic (network packets) are allowed or blocked based on rules you set.

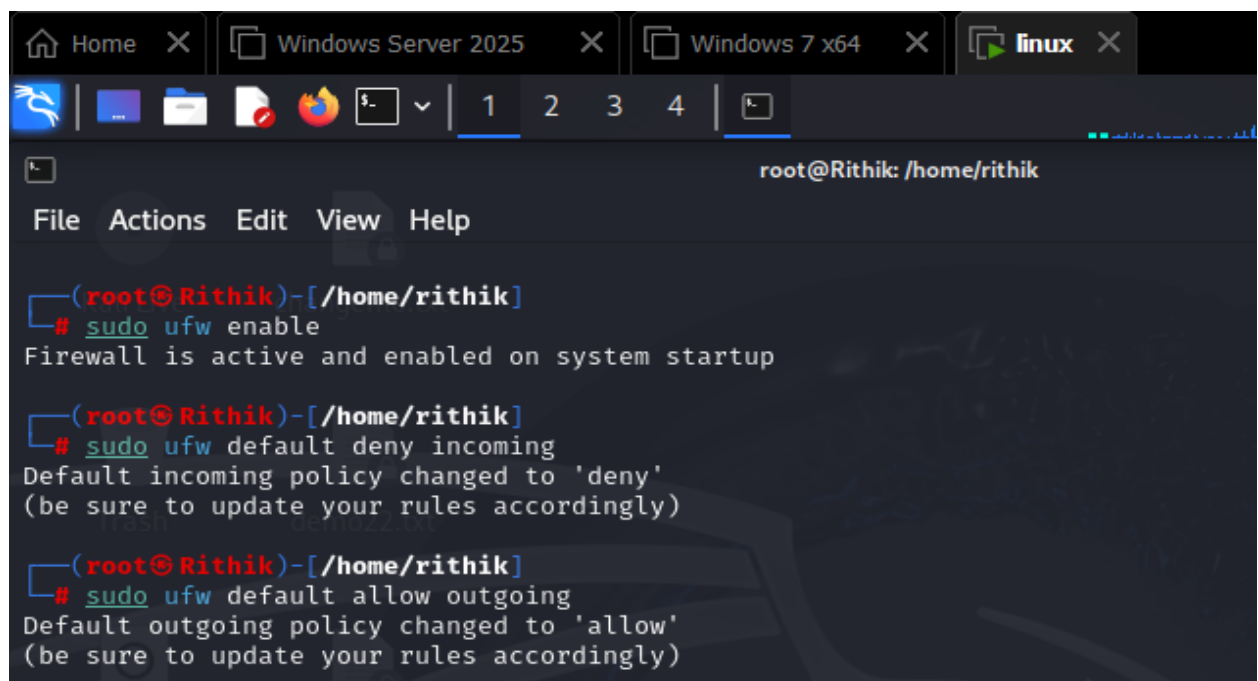
On Linux, two common tools are used:

- *iptables → A powerful but complex command-line tool for configuring firewall rules.*
- *UFW (Uncomplicated Firewall) → A simpler interface built on top of iptables, designed for beginners and easy management.*

Practical of Option A Using Kali Linux:-

UFW (Uncomplicated Firewall):-

- ***Enable UFW***

A screenshot of a terminal window titled 'root@Rithik: /home/rithik'. The window shows three commands being executed in a root shell. The first command is 'sudo ufw enable', which outputs 'Firewall is active and enabled on system startup'. The second command is 'sudo ufw default deny incoming', which outputs 'Default incoming policy changed to 'deny' (be sure to update your rules accordingly)'. The third command is 'sudo ufw default allow outgoing', which outputs 'Default outgoing policy changed to 'allow' (be sure to update your rules accordingly)'. The terminal has a dark background with light-colored text. The window title bar shows 'Home', 'Windows Server 2025', 'Windows 7 x64', and 'linux' tabs. The terminal window has a menu bar with 'File', 'Actions', 'Edit', 'View', and 'Help'.

```
(root@Rithik)-[/home/rithik]
# sudo ufw enable
Firewall is active and enabled on system startup

(root@Rithik)-[/home/rithik]
# sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

(root@Rithik)-[/home/rithik]
# sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
```

- ***Allow ssh,http,https Ports/Services***

```
(root@Rithik)-[/home/rithik]
# sudo ufw allow ssh
Skipping adding existing rule
Skipping adding existing rule (v6)

(root@Rithik)-[/home/rithik]
# sudo ufw allow 80/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)

(root@Rithik)-[/home/rithik]
# sudo ufw allow 443/tcp
Rule added
Rule added (v6)
```

- ***Deny or Block Ports and check status***

```
(root@Rithik)-[/home/rithik]
# sudo ufw deny from 192.168.1.50
Rule added

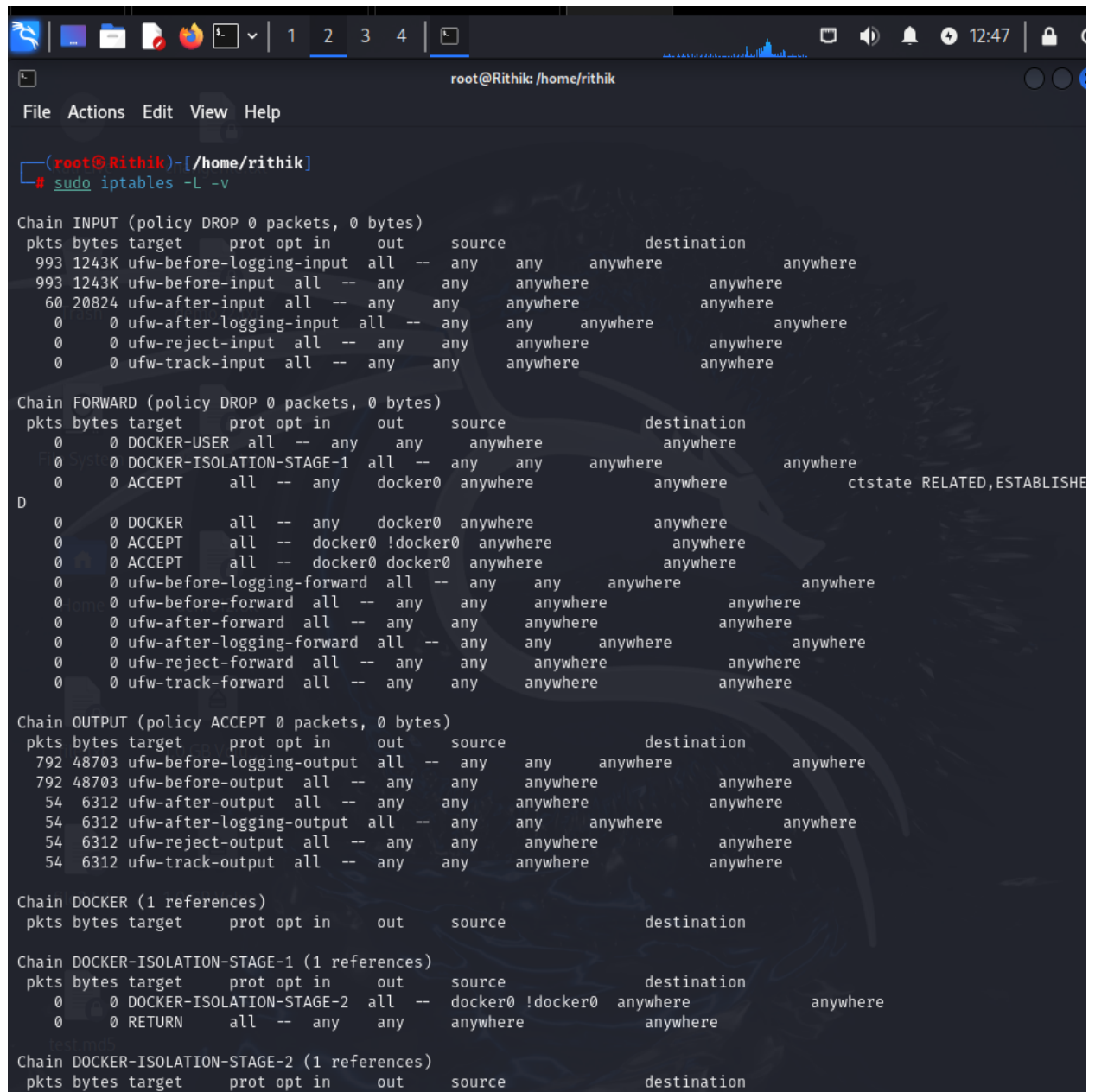
(root@Rithik)-[/home/rithik]
# sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip

To Action From
--
22/tcp ALLOW IN Anywhere
80/tcp ALLOW IN Anywhere
443/tcp ALLOW IN Anywhere
Anywhere DENY IN 192.168.1.50
22/tcp (v6) ALLOW IN Anywhere (v6)
80/tcp (v6) ALLOW IN Anywhere (v6)
443/tcp (v6) ALLOW IN Anywhere (v6)
```

Practical of Option B Using Kali Linux:-

Using iptables (Advanced)

- ***View Existing Rules***



```
root@Rithik: /home/rithik
File Actions Edit View Help

(root@Rithik)-[/home/rithik]
# sudo iptables -L -v

Chain INPUT (policy DROP 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
993 1243K ufw-before-logging-input all  -- any    any     anywhere          anywhere
993 1243K ufw-before-input  all  -- any    any     anywhere          anywhere
60 20824 ufw-after-input   all  -- any    any     anywhere          anywhere
0      0 ufw-after-logging-input all  -- any    any     anywhere          anywhere
0      0 ufw-reject-input  all  -- any    any     anywhere          anywhere
0      0 ufw-track-input   all  -- any    any     anywhere          anywhere

Chain FORWARD (policy DROP 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
0      0 DOCKER-USER      all  -- any    any     anywhere          anywhere
0      0 DOCKER-ISOLATION-STAGE-1 all  -- any    any     anywhere          anywhere
0      0 ACCEPT           all  -- any    docker0 anywhere          anywhere ctstate RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
792 48703 ufw-before-logging-output all  -- any    any     anywhere          anywhere
792 48703 ufw-before-output  all  -- any    any     anywhere          anywhere
54 6312 ufw-after-output   all  -- any    any     anywhere          anywhere
54 6312 ufw-after-logging-output all  -- any    any     anywhere          anywhere
54 6312 ufw-reject-output  all  -- any    any     anywhere          anywhere
54 6312 ufw-track-output   all  -- any    any     anywhere          anywhere

Chain DOCKER (1 references)
pkts bytes target      prot opt in     out     source            destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
pkts bytes target      prot opt in     out     source            destination
0      0 DOCKER-ISOLATION-STAGE-2 all  -- docker0 !docker0 anywhere          anywhere
0      0 RETURN           all  -- any    any     anywhere          anywhere

Chain DOCKER-ISOLATION-STAGE-2 (1 references)
pkts bytes target      prot opt in     out     source            destination
```

- ***Set Default Policies***

```
(root@Rithik)-[/home/rithik]
# sudo iptables -P INPUT DROP

(root@Rithik)-[/home/rithik]
# sudo iptables -P FORWARD DROP

(root@Rithik)-[/home/rithik]
# sudo iptables -P OUTPUT ACCEPT~
zsh: bad pattern: ^[[200~sudo

(root@Rithik)-[/home/rithik]
# sudo iptables -P OUTPUT ACCEPT

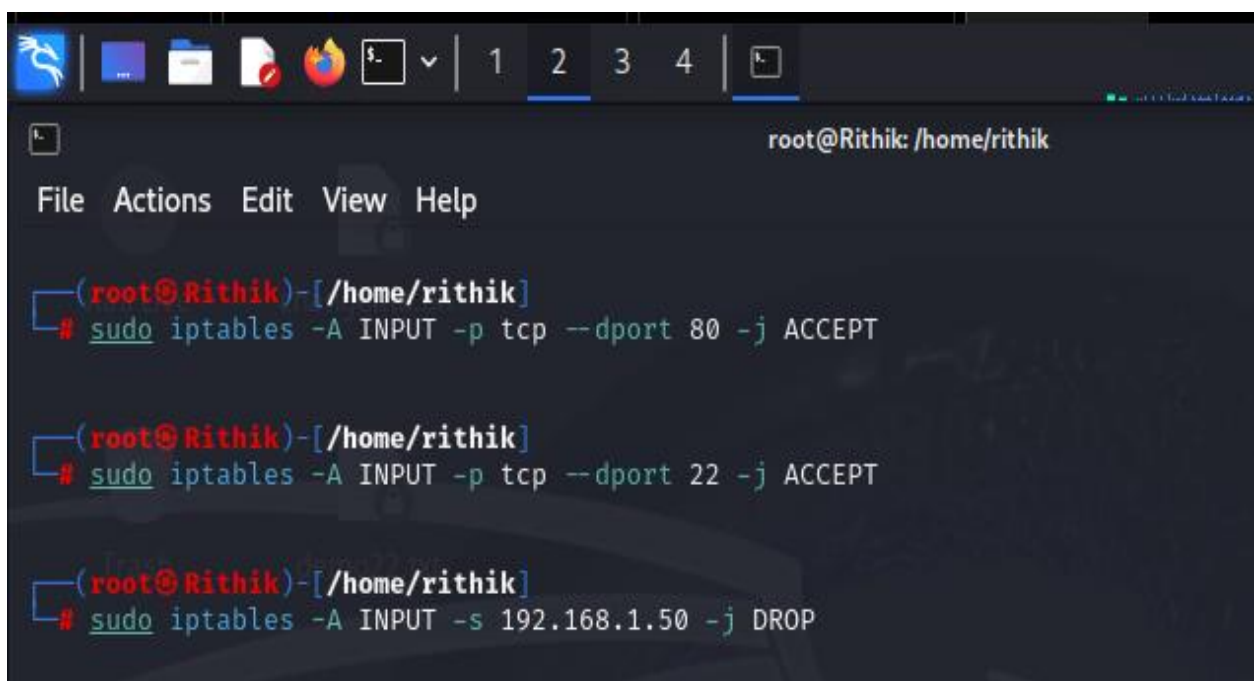
(root@Rithik)-[/home/rithik]
# sudo iptables -A INPUT -i lo -j ACCEPT
sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

(root@Rithik)-[/home/rithik]
# sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

(root@Rithik)-[/home/rithik]
# sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

(root@Rithik)-[/home/rithik]
# sudo iptables -A INPUT -s 192.168.1.50 -j DROP
```

- ***Allow Ports(80,22) and Block a Malicious IP***



The screenshot shows a terminal window with a dark background and a light blue dragon logo in the top left corner. The terminal title bar indicates the user is root@Rithik in the /home/rithik directory. The terminal content shows the following commands and their outputs:

```
(root@Rithik)-[/home/rithik]
# sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

(root@Rithik)-[/home/rithik]
# sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

(root@Rithik)-[/home/rithik]
# sudo iptables -A INPUT -s 192.168.1.50 -j DROP
```


- **Save Rules Permanently**

```
root@Rithik: /home/rithik
File Actions Edit View Help

(root@Rithik)-[/home/rithik]
# sudo apt install iptables-persistent -y
The following packages were automatically installed and are no longer required:
 libpython3.12-dev python3-wheel-whl python3.12 python3.12-dev python3.12-minimal python3.12-venv
Use 'sudo apt autoremove' to remove them.

Installing:
 iptables-persistent

Installing dependencies:
 netfilter-persistent

REMOVING:
 ufw

Summary:
Upgrading: 0, Installing: 2, Removing: 1, Not Upgrading: 1820
Download size: 18.5 kB
Freed space: 783 kB

Get:1 http://kali.download/kali kali-rolling/main amd64 netfilter-persistent all 1.0.23 [7948 B]
Get:2 http://mirror.kku.ac.th/kali kali-rolling/main amd64 iptables-persistent all 1.0.23 [10.5 kB]
Fetched 18.5 kB in 38s (482 B/s)
Preconfiguring packages ...
(Reading database ... 427716 files and directories currently installed.)
Removing ufw (0.36.2-9) ...
Selecting previously unselected package netfilter-persistent.
(Reading database ... 427619 files and directories currently installed.)
Preparing to unpack .../netfilter-persistent_1.0.23_all.deb ...
Unpacking netfilter-persistent (1.0.23) ...
Selecting previously unselected package iptables-persistent.
Preparing to unpack .../iptables-persistent_1.0.23_all.deb ...
Unpacking iptables-persistent (1.0.23) ...
Setting up netfilter-persistent (1.0.23) ...
update-rc.d: We have no instructions for the netfilter-persistent init script.
update-rc.d: It looks like a non-network service, we enable it.
netfilter-persistent.service is a disabled or a static unit, not starting it.
Setting up iptables-persistent (1.0.23) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.4.0) ...
Scanning processes ...
Scanning linux images ...

Running kernel seems to be up-to-date.
```

```
(root@Rithik)-[/home/rithik]
# sudo netfilter-persistent save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/15-ip4tables save
run-parts: executing /usr/share/netfilter-persistent/plugins.d/25-ip6tables save
```

- **View Existing Rules**

```

root@Rithik: /home/rithik
File Actions Edit View Help
(root@Rithik)-[/home/rithik]
# sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
1045 1268K ufw-before-logging-input all -- any    any      anywhere          anywhere
1045 1268K ufw-before-input    all -- any    any      anywhere          anywhere
62 21282 ufw-after-input     all -- any    any      anywhere          anywhere
0 0 ufw-after-logging-input all -- any    any      anywhere          anywhere
0 0 ufw-reject-input    all -- any    any      anywhere          anywhere
0 0 ufw-track-input     all -- any    any      anywhere          anywhere
0 0 ACCEPT            all -- lo     any      anywhere          anywhere
0 0 ACCEPT            tcp -- any    any      anywhere          anywhere          ctstate RELATED,ESTABLISHED
0 0 ACCEPT            tcp -- any    any      anywhere          anywhere          tcp dpt:http
0 0 ACCEPT            tcp -- any    any      anywhere          anywhere          tcp dpt:ssh
0 0 DROP              all -- any    any      192.168.1.50      anywhere

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
0 0 DOCKER-USER       all -- any    any      anywhere          anywhere
0 0 DOCKER-ISOLATION-STAGE-1 all -- any    any      anywhere          anywhere
0 0 ACCEPT            all -- any    docker0        anywhere          anywhere          ctstate RELATED,ESTABLISHED

D
0 0 DOCKER            all -- any    docker0        anywhere          anywhere
0 0 ACCEPT            all -- docker0 !docker0        anywhere          anywhere
0 0 ACCEPT            all -- docker0 docker0         anywhere          anywhere
0 0 ufw-before-logging-forward all -- any    any      anywhere          anywhere
0 0 ufw-before-forward  all -- any    any      anywhere          anywhere
0 0 ufw-after-forward   all -- any    any      anywhere          anywhere
0 0 ufw-after-logging-forward all -- any    any      anywhere          anywhere
0 0 ufw-reject-forward  all -- any    any      anywhere          anywhere
0 0 ufw-track-forward   all -- any    any      anywhere          anywhere

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
pkts bytes target      prot opt in     out     source            destination
857 53370 ufw-before-logging-output all -- any    any      anywhere          anywhere
857 53370 ufw-before-output    all -- any    any      anywhere          anywhere
78 8107 ufw-after-output     all -- any    any      anywhere          anywhere
78 8107 ufw-after-logging-output all -- any    any      anywhere          anywhere
78 8107 ufw-reject-output    all -- any    any      anywhere          anywhere
78 8107 ufw-track-output     all -- any    any      anywhere          anywhere

Chain DOCKER (1 references)
pkts bytes target      prot opt in     out     source            destination

Chain DOCKER-ISOLATION-STAGE-1 (1 references)
pkts bytes target      prot opt in     out     source            destination
0 0 DOCKER-ISOLATION-STAGE-2 all -- docker0 !docker0        anywhere          anywhere
0 0 RETURN            all -- any    any      anywhere          anywhere

```

Key Differences

- **iptables** = powerful, granular, but harder to configure.
- **UFW** = beginner-friendly, recommended for most admins.