

Firewall Configuration & Testing Report

Task 10 – Cyber Security Internship

1. Aim of the Task

The aim of this task is to understand firewall concepts and to configure, test, and analyze firewall rules using **UFW (Uncomplicated Firewall)**. The task focuses on allowing and denying network traffic, testing connectivity, blocking malicious IP addresses, observing logs, and documenting the impact of firewall rules.

2. Tools Used

- **Operating System:** Kali Linux
- **Firewall Tool:** UFW (Uncomplicated Firewall)
- **Alternative (Not Used):** iptables

3. Firewall Overview

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules. It acts as a barrier between a trusted internal network and untrusted external networks.

Firewalls help in:

- Preventing unauthorized access
- Reducing attack surface
- Controlling network communication
- Monitoring suspicious activities

4. Firewall Configuration Steps

4.1 Checking Firewall Status

Initially, the firewall status was checked to verify whether UFW was active or inactive.

- Command used:
sudo ufw status

The firewall was found to be inactive.

4.2 Enabling the Firewall

The UFW firewall was enabled to start filtering network traffic.

- Command used:
sudo ufw enable

After enabling, the firewall status was verified.

- Command used:

```
sudo ufw status verbose
```

The firewall was successfully activated with default policies set to deny incoming traffic and allow outgoing traffic.

4.3 Allowing Required Ports

To ensure normal system functionality, essential ports were allowed.

- SSH (Port 22) – Remote access
- HTTP (Port 80) – Web traffic
- HTTPS (Port 443) – Secure web traffic

These rules allow only trusted services while keeping other ports blocked.

4.4 Blocking Unused / Risky Ports

An unused and insecure port (Telnet – Port 23) was blocked to prevent potential attacks.

Blocking unused ports helps reduce vulnerabilities and prevents unauthorized access.

4.5 Testing Connectivity

Connectivity tests were performed to verify firewall behavior:

- Blocked ports failed to establish a connection
- Allowed ports successfully established a connection

This confirmed that the firewall rules were working as expected.

4.6 Enabling and Observing Firewall Logs

Firewall logging was enabled to monitor blocked and allowed traffic.

- Logs were checked to observe blocked connection attempts
- Suspicious activities were recorded in firewall logs

Firewall logs help in identifying attack attempts and monitoring network behavior.

4.7 Blocking a Malicious IP Address

A suspicious IP address was manually blocked using firewall rules.

Blocking malicious IP addresses helps prevent attacks such as brute force attempts, scanning, and unauthorized access.

5. Firewall Rules Summary

| Rule Type | Description |
|----------------|----------------------------------|
| Allowed Ports | 22 (SSH), 80 (HTTP), 443 (HTTPS) |
| Blocked Ports | 23 (Telnet) |
| Blocked IP | 192.168.1.100 |
| Logging | Enabled |
| Default Policy | Deny incoming, Allow outgoing |

```
Session Actions Edit View Help
[kali㉿kali] ~
$ sudo ufw status
[sudo] password for kali:
Status: inactive

[kali㉿kali] ~
$ sudo ufw enable
Firewall is active and enabled on system startup

[kali㉿kali] ~
$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), deny (routed)
New profiles: skip
```

```
[kali㉿kali] ~
$ sudo ufw allow 80
Rule added
Rule added (v6)

[kali㉿kali] ~
$ sudo ufw status numbered
Status: active
      To          Action    From
      --          ____     ____
[ 1] 22/tcp      ALLOW IN  Anywhere
[ 2] 80          ALLOW IN  Anywhere
[ 3] 22/tcp (v6) ALLOW IN  Anywhere (v6)
[ 4] 80 (v6)    ALLOW IN  Anywhere (v6)
```

```
[kali㉿kali] ~
$ sudo ufw deny 23
Rule added
Rule added (v6)

[kali㉿kali] ~
$ sudo ufw status numbered
Status: active
      To          Action    From
      --          ____     ____
[ 1] 22/tcp      ALLOW IN  Anywhere
[ 2] 80          ALLOW IN  Anywhere
[ 3] 23          DENY IN   Anywhere
[ 4] 22/tcp (v6) ALLOW IN  Anywhere (v6)
[ 5] 80 (v6)    ALLOW IN  Anywhere (v6)
[ 6] 23 (v6)    DENY IN   Anywhere (v6)
```

```
Session Actions Edit View Help
[kali㉿kali)-[~]
$ telnet localhost 23
Trying ::1...
Connection failed: Connection refused
Trying 127.0.0.1 ...
telnet: Unable to connect to remote host: Connection refused

[kali㉿kali)-[~]
$ curl http://localhost

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Apache2 Debian Default Page: It works</title>
<style type="text/css" media="screen">
* {
margin: 0px 0px 0px 0px;
padding: 0px 0px 0px 0px;
}

body, html {
padding: 3px 3px 3px 3px;
background-color: #D8DBE2;
font-family: Verdana, sans-serif;
font-size: 1pt;
text-align: center;
}

div.main_page {
```

```
Session Actions Edit View Help
[kali㉿kali)-[~]
$ sudo ufw logging on
Logging enabled
[kali㉿kali)-[~]
$ sudo tail -f /var/log/ufw.log
tail: cannot open '/var/log/ufw.log' for reading: No such file or directory
tail: no files remaining
[kali㉿kali)-[~]
$ sudo ufw deny from 192.168.1.100
Rule added
[kali㉿kali)-[~]
$ sudo ufw status numbered
Status: active

 To           Action      From
 --          _____
 [ 1] 22/tcp    ALLOW IN   Anywhere
 [ 2] 80        ALLOW IN   Anywhere
 [ 3] 23        DENY IN    Anywhere
 [ 4] Anywhere  DENY IN    192.168.1.100
 [ 5] 22/tcp (v6) ALLOW IN   Anywhere (v6)
 [ 6] 80 (v6)   ALLOW IN   Anywhere (v6)
 [ 7] 23 (v6)   DENY IN    Anywhere (v6)
```

6. Impact of Firewall Configuration

- Unauthorized network access was blocked
- Only essential services were allowed
- Attack surface was reduced
- Malicious traffic was denied
- Network activity could be monitored through logs
- Overall system security was improved

7. Conclusion

This task provided hands-on experience in configuring and managing firewall rules using UFW. It improved understanding of network security, traffic filtering, logging, and real-world firewall management practices.