🔒 Firewall Configuration and Testing Report

System: Terminal for UFW
Firewall Tool: 192.168.245.131
Prepared by: [Suryadev kumar]
Date: [30/05/2025]

📋 Objective

The objective of this task is to configure basic firewall rules to:

- Allow essential traffic (SSH, HTTP/HTTPS, local loopback)
- Block unauthorized access (specific 192.168.245.131,used ports 80,8080)
- Test and verify the effectiveness of these rules

Configuration file showing firewall .

Terminal showing GUI.

```
┌──(kali㊀kali)-[~]
└─$ sudo apt install gufw
Solving dependencies ... Error!
Some packages could not be installed. This may mean that you have
requested an impossible situation or if you are using the unstable
distribution that some required packages have not yet been created
or been moved out of Incoming.
The following information may help to resolve the situation:

Unsatisfied dependencies:
 gir1.2-soup-3.0 : Depends: libsoup-3.0-0 (= 3.6.4-2) but 3.6.5-1 is to be installed
Error: Unable to correct problems, you have held broken packages.
Error: The following information from --solver 3.0 may provide additional context:
   Unable to satisfy dependencies. Reached two conflicting decisions:
   1. gir1.2-webkit2-4.1:amd64 Depends gir1.2-soup-3.0
      but none of the choices are installable:
      - gir1.2-soup-3.0:amd64 Depends libsoup-3.0-0 (= 3.6.4-2)
        but none of the choices are installable:
        - libsoup-3.0-0:amd64=3.6.4-2 is not selected for install
   2. gir1.2-webkit2-4.1:amd64 is selected for install because:
      1. gufw:amd64=24.04.0-2 is selected for install
      2. gufw:amd64 Depends gir1.2-webkit2-4.1

┌──(kali㊀kali)-[~]
└─$
```

Port Locally Connect .

```
  ┌──(kali⊛kali)-[~]
  └─$ sudo ufw allow ssh

Skipping adding existing rule
Skipping adding existing rule (v6)

  ┌──(kali⊛kali)-[~]
  └─$ sudo ufw allow 22/tcp

Skipping adding existing rule
Skipping adding existing rule (v6)

  ┌──(kali⊛kali)-[~]
  └─$ sudo ufw allow ssh

Skipping adding existing rule
Skipping adding existing rule (v6)

  ┌──(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), disabled (routed)
New profiles: skip

To                         Action        From
--                         ──────        ────
22/tcp                     ALLOW IN      Anywhere
80/tcp                     DENY IN       Anywhere
443/tcp                    ALLOW IN      Anywhere
8080/tcp                   ALLOW IN      Anywhere
8080                       DENY IN       Anywhere
22/tcp (v6)                ALLOW IN      Anywhere (v6)
80/tcp (v6)                DENY IN       Anywhere (v6)
443/tcp (v6)               ALLOW IN      Anywhere (v6)
Anywhere (v6)              ALLOW IN      fe80::7930:83ec:e478:ea78
8080/tcp (v6)              ALLOW IN      Anywhere (v6)
8080 (v6)                  DENY IN       Anywhere (v6)
```

Remove the test block rule to restore original state.

Local connection.

SSH Access	TCP 22	ACCEPT	Remote management
HTTP/HTTPS Access	TCP 80/443	ACCEPT	Web access
Block Specific IP	All	All	DROP	Prevents access from attacker

✅ Conclusion

The firewall rules were successfully configured and tested. The system now blocks all unsolicited inbound traffic except for essential services, and malicious IP addresses can be blacklisted effectively.