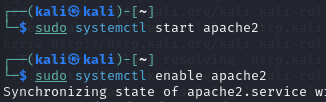
Task 3 :

Firewall & Network Security

Setting up apache web server :



1. We begin by starting and enabling the Apache2 server to ensure it is active and available for use.

1. We begin by starting and enabling the Apache2 server to ensure it is active and available for use.

3. We initiate the Apache2 server by starting and enabling it to ensure continuous operation and availability.

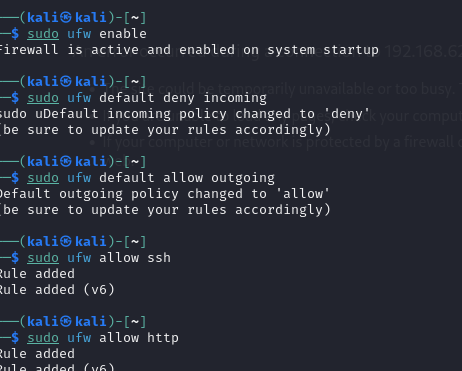
Exploit : port scanning with Nmap and Netcat:

1.First we perform a basic Nmap scan to check for open ports.

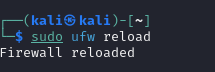
Mitigation: Firewall & Network Hardening



1. First we enable firewall for active defense

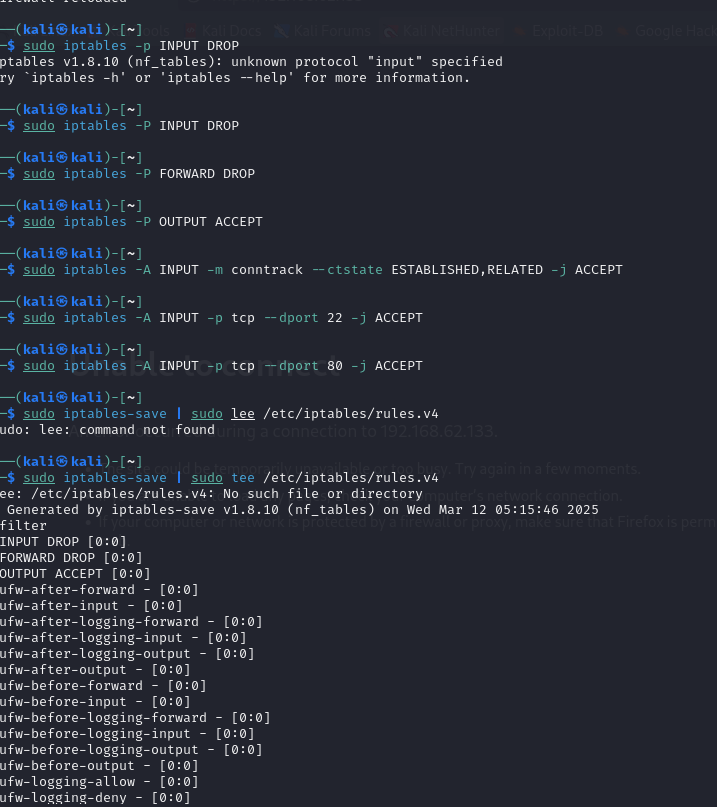


2. Then we set rules for allowing necessary ports.



3. Finally we reload the firewall to save changes.

Additional Protection with Iptables.



SUMMARY:

| 1. Installed Apache with UFW disabled (vulnerable state) |
| --- |
| 2. Simulated an attack using nmap and netcat |
| 3. Hardened the server by restricting access via UFW and Iptables |