TASK 3:

Firewall & Network Security

1. **Overview:**

This Proof of Concept highlights the dangers of misconfigured firewalls and exposed network services. The process includes deploying a simple web server, identifying open ports through scanning, and securing the system by implementing ufw and iptables to limit access and block unwanted traffic.

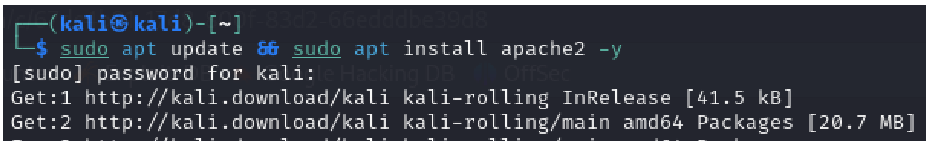
2.Objectives:

- **Deployment:** Install and set up a basic web server (Apache2) and deactivate the firewall (ufw disable).
- **Assessment:** Utilize nmap and netcat to identify open ports and running services, illustrating how attackers can detect exposed services.
- **Protection:** Limit access using ufw (allowing only SSH and HTTP) and enforce iptables rules to block unnecessary traffic.

3. Setup

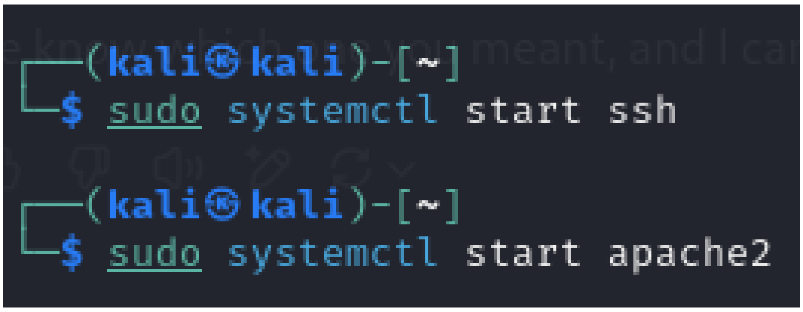
3.1. Install and Configure Apache Web Server

1. Update and Install Apache:



```
┌──(kali㉿kali)-[~]
└─$ sudo apt update && sudo apt install apache2 -y
[sudo] password for kali:
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [20.7 MB]
```

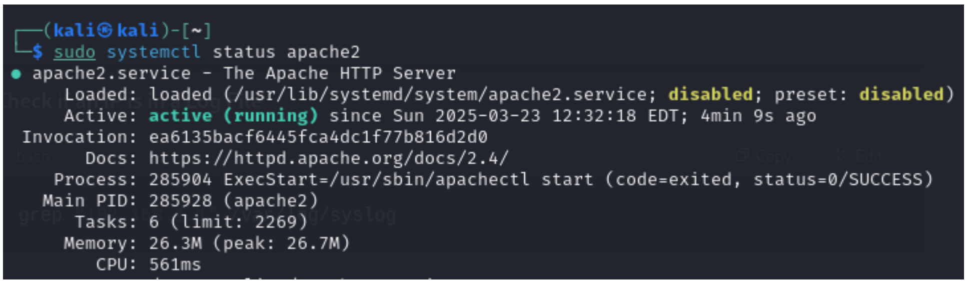
2. Start SSH and Apache:



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start ssh

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start apache2
```

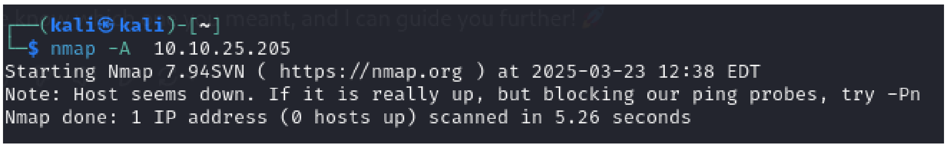
3. Enable and verify Apache Status:



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; preset: disabled)
     Active: active (running) since Sun 2025-03-23 12:32:18 EDT; 4min 9s ago
 Invocation: ea6135bacf6445fca4dc1f77b816d2d0
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 285904 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 285928 (apache2)
      Tasks: 6 (limit: 2269)
     Memory: 26.3M (peak: 26.7M)
        CPU: 561ms
```

4. Exploitation

4.1. Scan for Open Ports Using Nmap Scan the Local Machine:

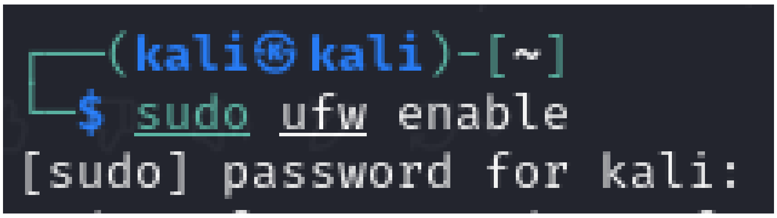


```
┌──(kali㉿kali)-[~]
└─$ nmap -A  10.10.25.205
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-23 12:38 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 5.26 seconds
```

5. Mitigation

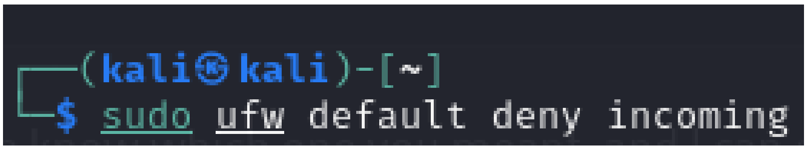
5.1. Enable and Configure UFW

1. Enable UFW:

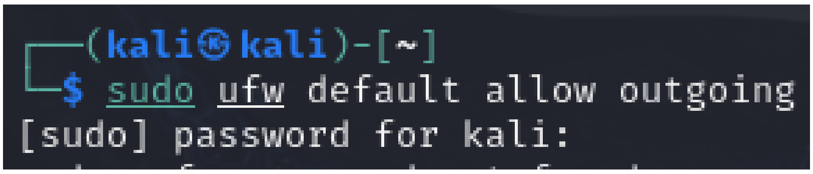


```
┌──(kali㉿kali)-[~]
└─$ sudo ufw enable
[sudo] password for kali:
```

2. Set Default Policies:

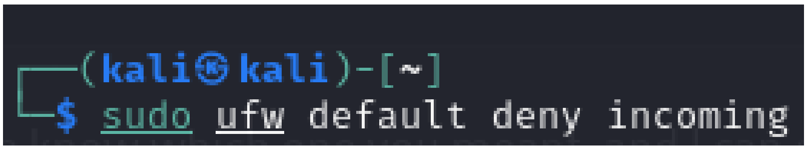


```
┌──(kali㉿kali)-[~]
└─$ sudo ufw default deny incoming
```

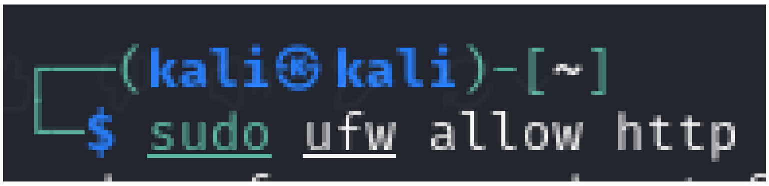


```
┌──(kali㉿kali)-[~]
└─$ sudo ufw default allow outgoing
[sudo] password for kali:
```

3. Allow SSH and HTTP:

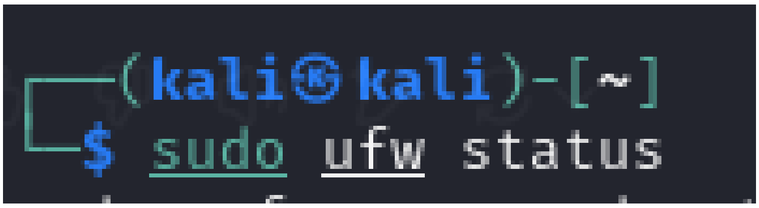


```
┌──(kali㉿kali)-[~]
└─$ sudo ufw default deny incoming
```



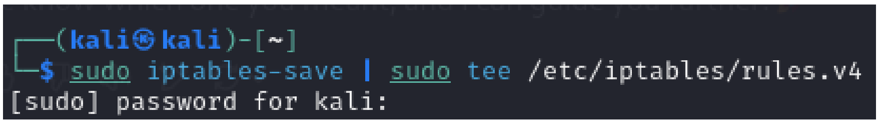
```
┌──(kali㉿kali)-[~]
└─$ sudo ufw allow http
```

4. Verify UFW Status:

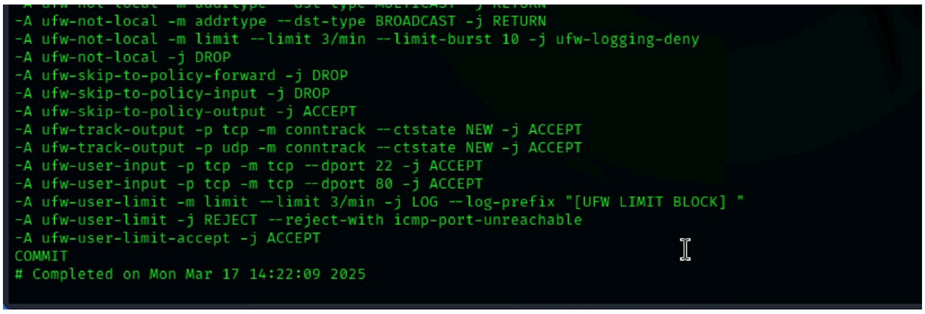


```
┌──(kali㉿kali)-[~]
└─$ sudo ufw status
```

5.Save IPTables Rules:



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables-save | sudo tee /etc/iptables/rules.v4
[sudo] password for kali:
```



```
-A ufw-not-local -m addrtype --dst-type MULTICAST -j RETURN
-A ufw-not-local -m addrtype --dst-type BROADCAST -j RETURN
-A ufw-not-local -m limit --limit 3/min --limit-burst 10 -j ufw-logging-deny
-A ufw-not-local -j DROP
-A ufw-skip-to-policy-forward -j DROP
-A ufw-skip-to-policy-input -j DROP
-A ufw-skip-to-policy-output -j ACCEPT
-A ufw-track-output -p tcp -m conntrack --ctstate NEW -j ACCEPT
-A ufw-track-output -p udp -m conntrack --ctstate NEW -j ACCEPT
-A ufw-user-input -p tcp -m tcp --dport 22 -j ACCEPT
-A ufw-user-input -p tcp -m tcp --dport 80 -j ACCEPT
-A ufw-user-limit -m limit --limit 3/min -j LOG --log-prefix "[UFW LIMIT BLOCK] "
-A ufw-user-limit -j REJECT --reject-with icmp-port-unreachable
-A ufw-user-limit-accept -j ACCEPT
COMMIT
# Completed on Mon Mar 17 14:22:09 2025
```

Conclusion:

This proof of concept highlights the critical role of firewall configuration and network security. By limiting access to essential services and preventing unnecessary traffic, administrators can effectively minimize potential attack vectors and enhance overall system protection.