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).

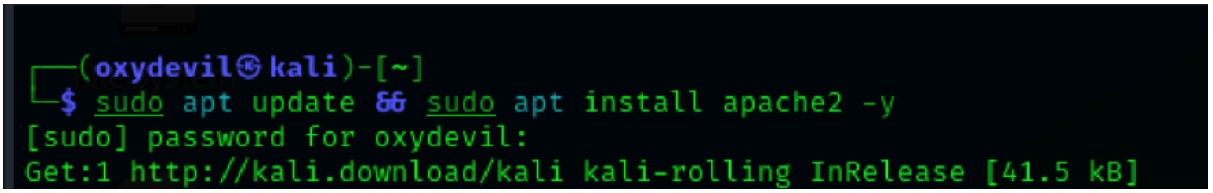
• **Assessment:** Utilize nmap and netcat to identify open ports and running services, illustrating how attackers can detect exposed services.

• **Protection:** Limit access using ufw (allowing only SSH and HTTP) and enforce iptables rules to block unnecessary traffic.

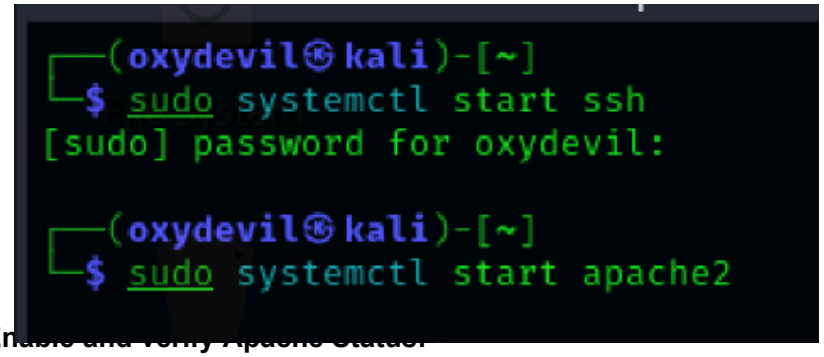
3. Setup

3.1. Install and Configure Apache Web Server

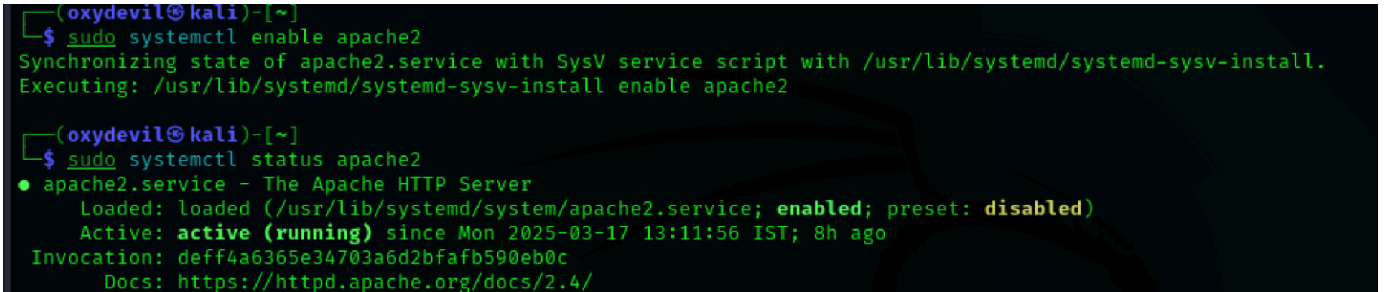
1. Update and Install Apache:



2. Start SSH and Apache:

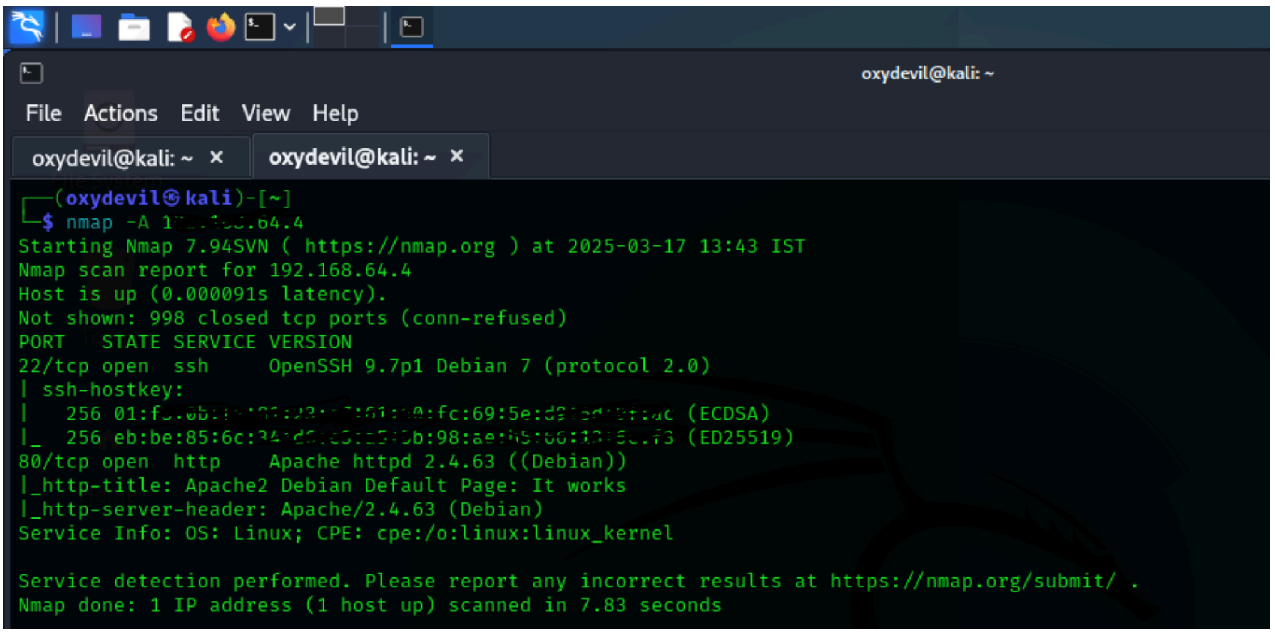


3. Enable and Verify Apache Status:

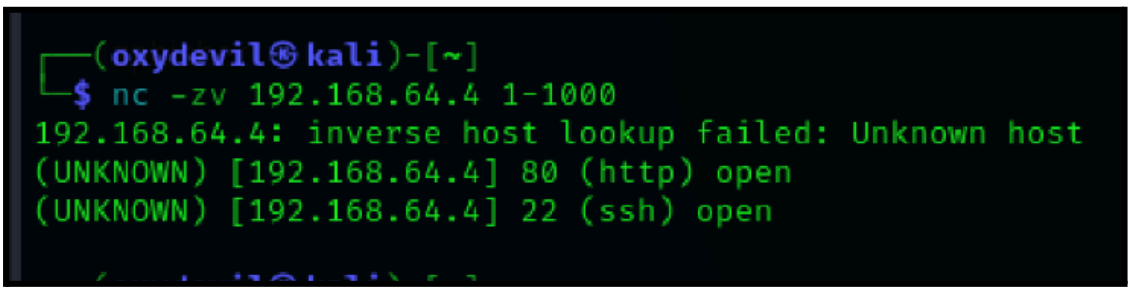


4. Exploitation

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



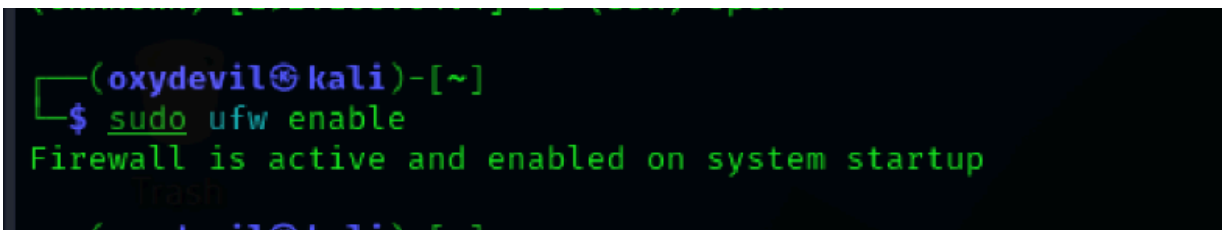
4.2. Use Netcat to Test Open Ports



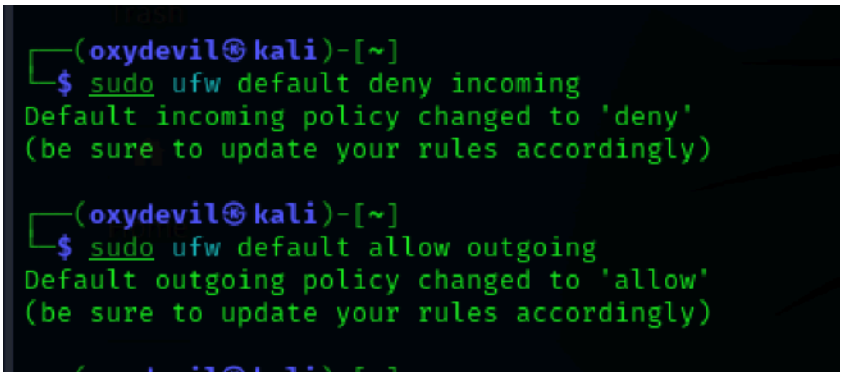
5. Mitigation

5.1. Enable and Configure UFW

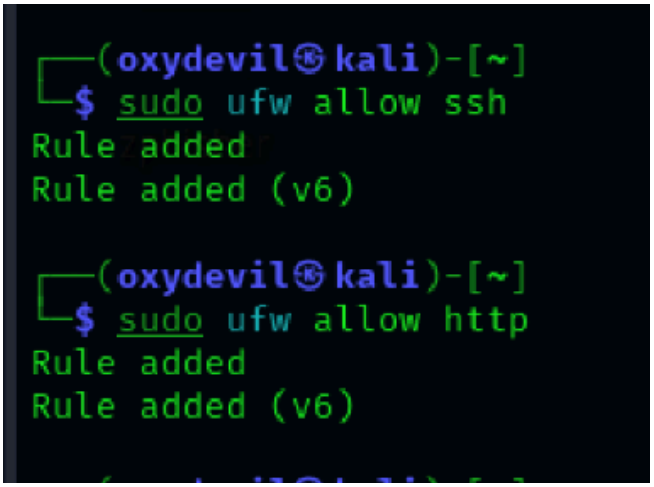
1. Enable UFW:



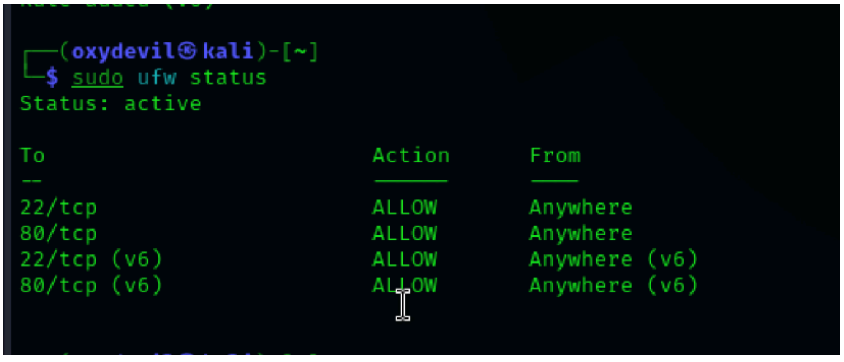
2. Set Default Policies:



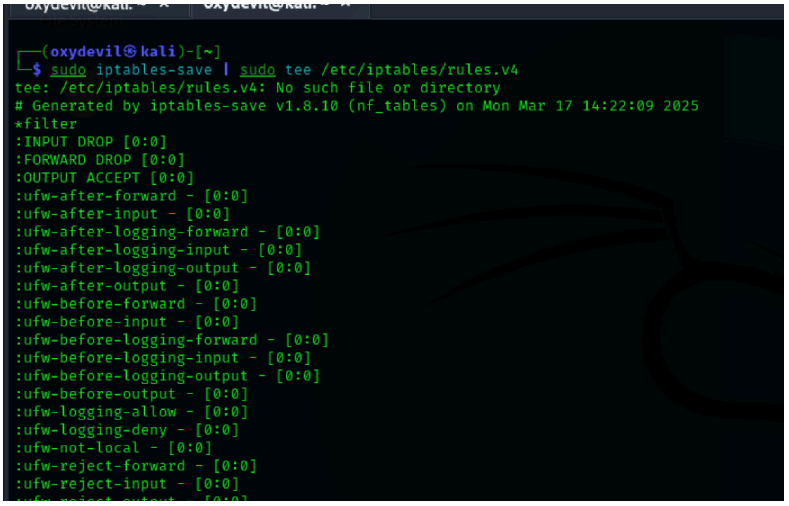
3. Allow SSH and HTTP:

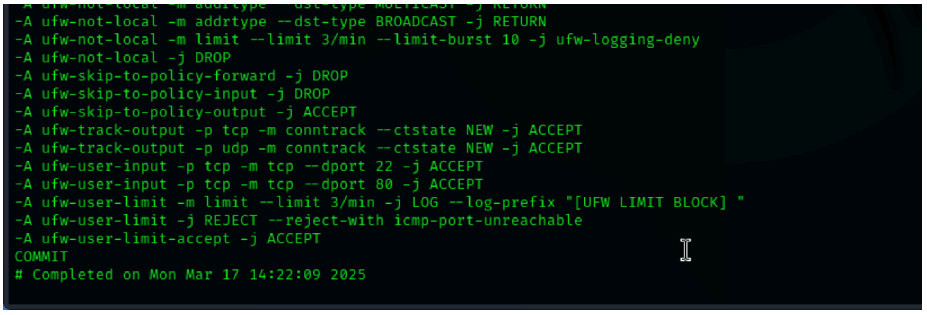


4. Verify UFW Status:



5.Save IPTables Rules:





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.