**Task 3: Firewall & Network Security**

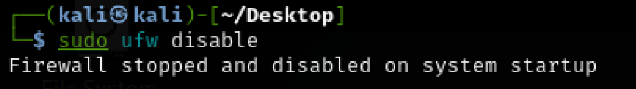
**Step 1: Setup – Install & Configure a Web Server**

We will set up **Apache2** as a web server and disable the firewall to simulate an insecure environment.

**1. Install Apache Web Server**



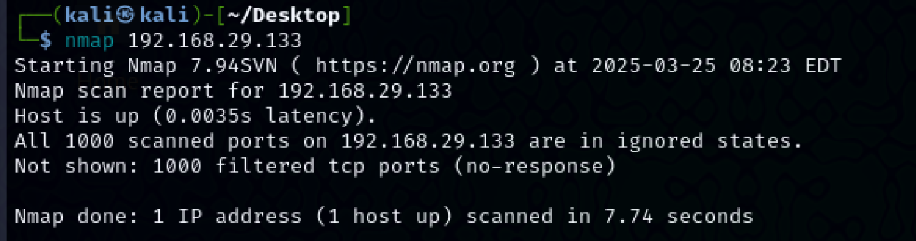
2. Disable Firewall to Allow All Traffic



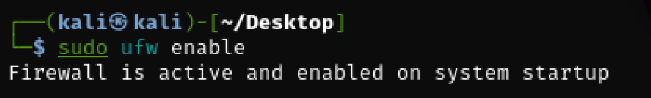
3. Verify Open Ports



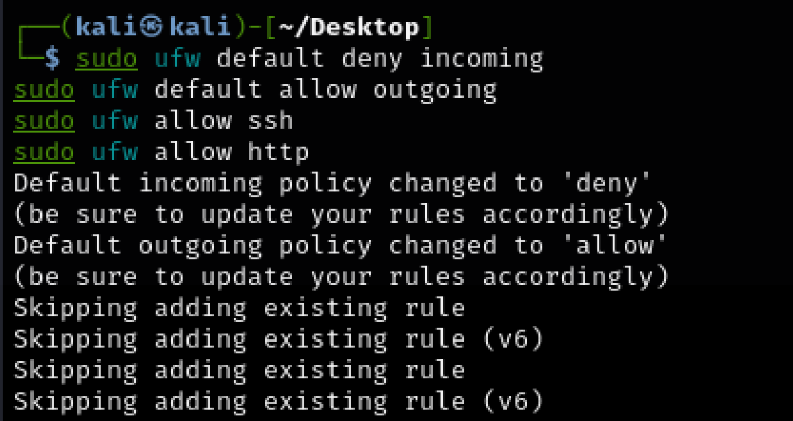
Step 2: Exploit – Scan for Open Ports & Services



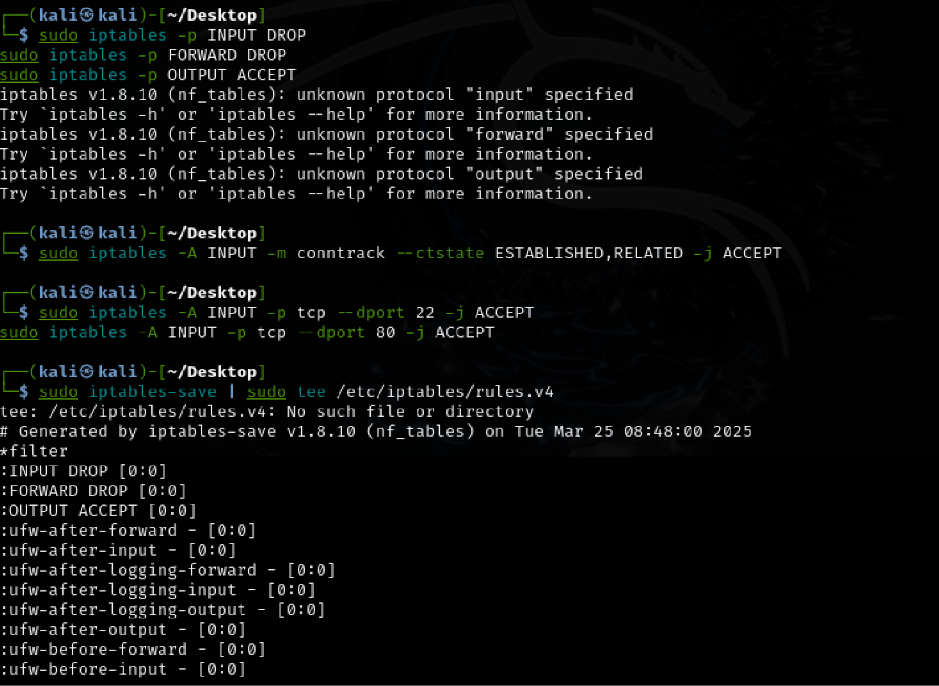
Step 3: Mitigation – Secure the Firewall & Network



1. Enable & Configure UFW (Uncomplicated Firewall)



2.Reload all firewall and iptables protection:



**Summary**

**Setup:** Installed **Apache** and disabled the firewall.  
 **Exploit:** Used **Nmap & Netcat** to scan for open ports.  
 **Mitigation:** Configured **UFW & iptables** to restrict access.

**Task 4: SUID & Privilege Escalation**

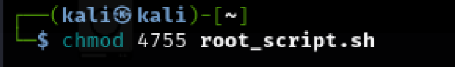
**Step 1: Setup – Create a Vulnerable SUID Binary & Script**

1. **Enable SUID on /bin/bash**

****

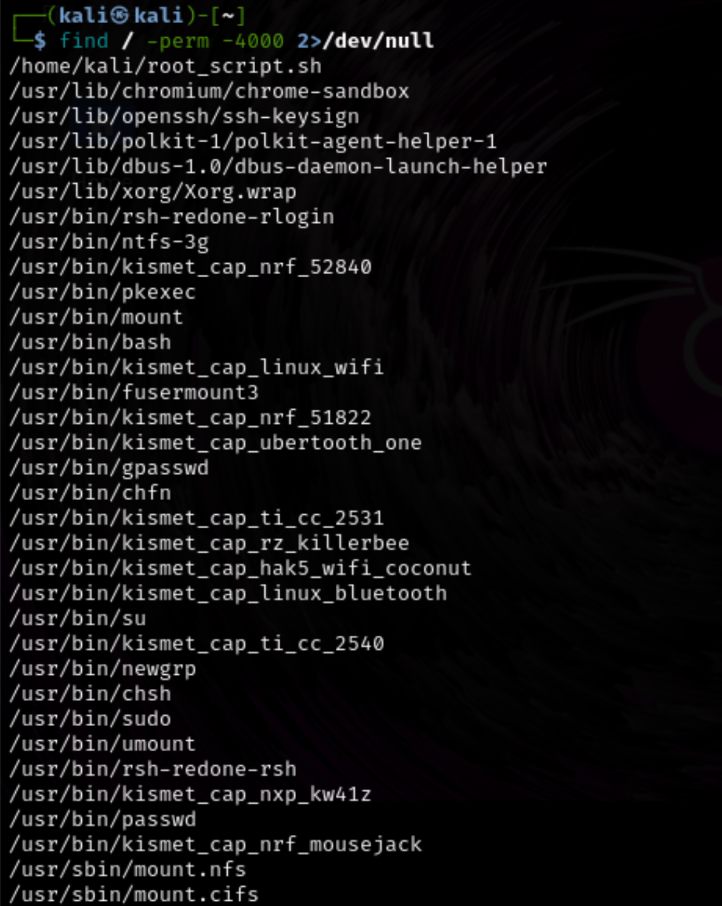
1. Create a Root-Privileged Script with SUID
2. gives **SUID privileges** (allowing execution as root)

Any user can now **run this script as root**.



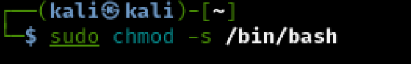
**Step 2: Exploit – Find & Abuse SUID Misconfigurations**

**1. Identify SUID Binaries**

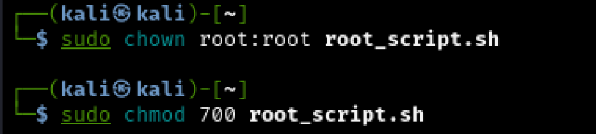


**Step 3: Mitigation – Secure the System**

1. **Remove SUID from /bin/bash**



1. Restrict the Root Script



**Summary**

**Setup:** Added SUID to /bin/bash & created a **root-executable script**.  
 **Exploit:** Used find to locate SUID misconfigurations and **escalated privileges**.  
 **Mitigation:** **Removed SUID**, restricted script execution, and enforced **regular audits**.