# PROOF OF CONCEPT

## LINUX SECURITY - EXPLOITATION & HARDENING

**Task 2: Remote Access & SSH Hardening**

## 1.EXECUTIVE SUMMARY

This PoC demonstrates the risks associated with insecure SSH configurations, such as allowing root login and password-based authentication. It includes enabling SSH, performing a brute-force attack, and then hardening the SSH configuration to prevent unauthorized access.

## 2.OBJECTIVES

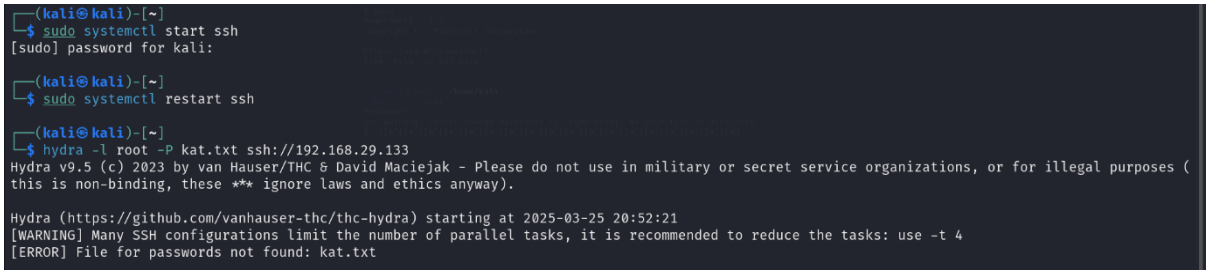
- Setup: Enable SSH on a Linux machine, allow root login, and enable password authentication.
- Exploit: Perform a brute-force attack on SSH using tools like hydra or medusa.
- Mitigation: Disable root login, enable key-based authentication, and configure fail2ban to prevent brute-force attacks.

## 3. SETUP

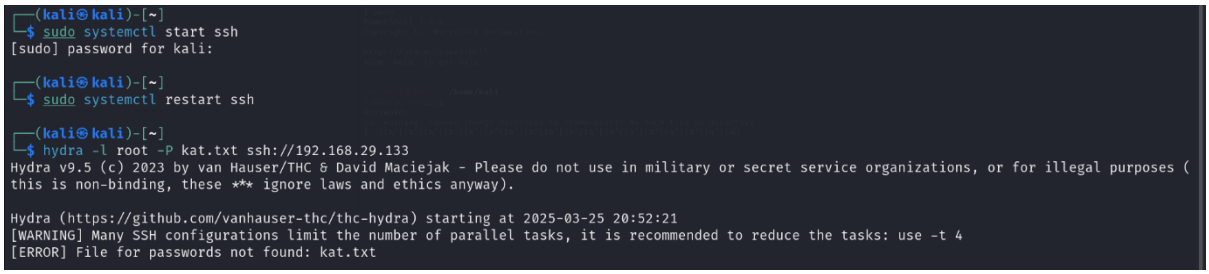
### 3.1. Enable SSH and Configure Insecure Settings

1. Start and Enable SSH Service:


2. Edit SSH Configuration to allow root login and password authentication:

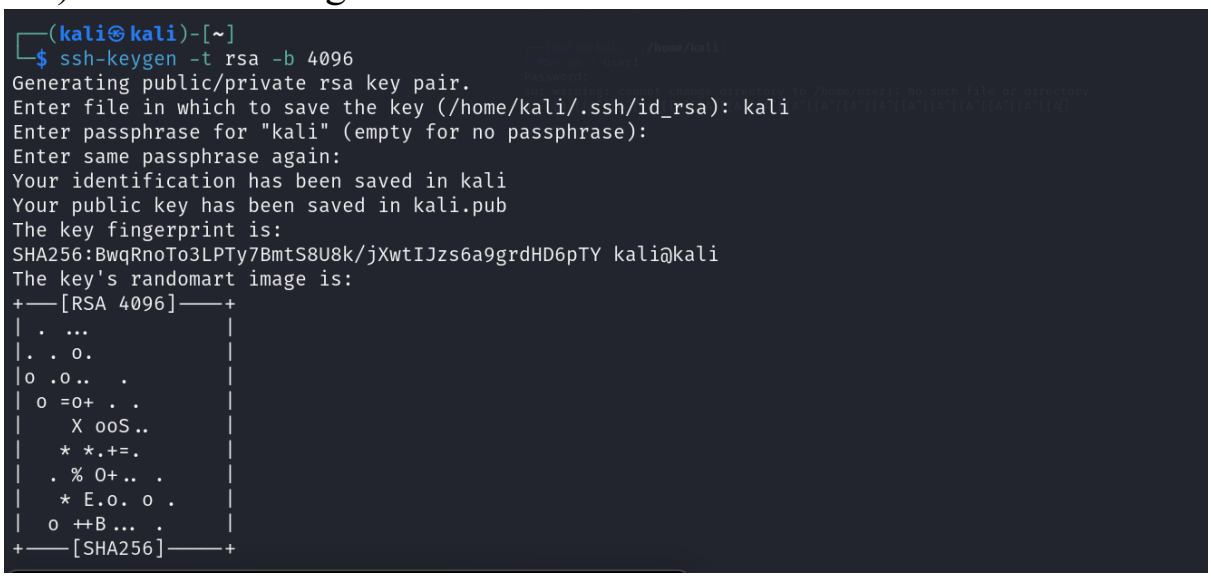



3.Restart SSH to apply changes:

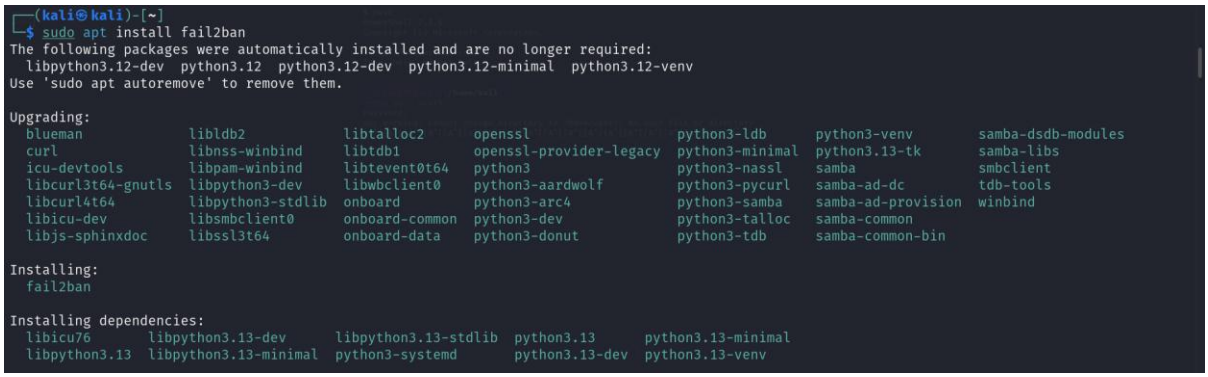



## 4) EXPLOIT:

## 4.1)Disable root login:




## 4.2) Configure fail2ban:




## 4.3) sudo systemctl enable fail2b: