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.

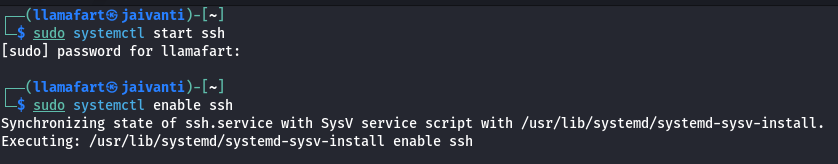
**2. Objectives**

* **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**:

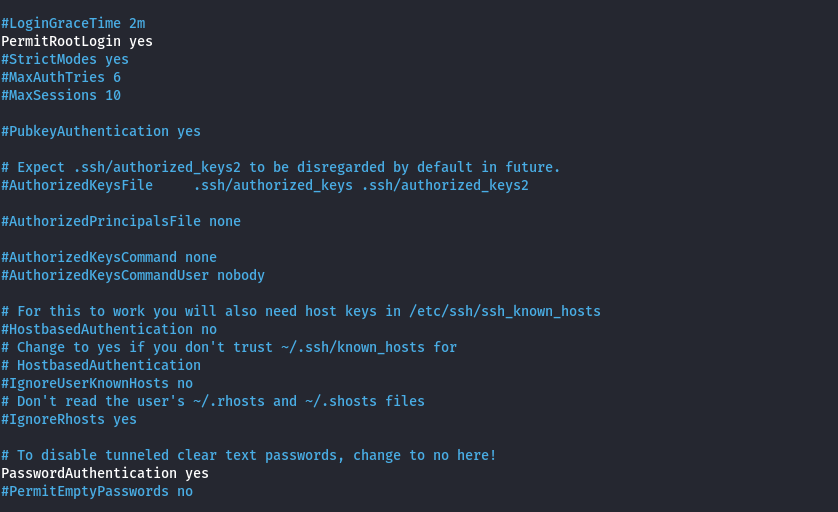


1. **Edit SSH Configuration to allow root login and password authentication:**

Open the SSH configuration file:



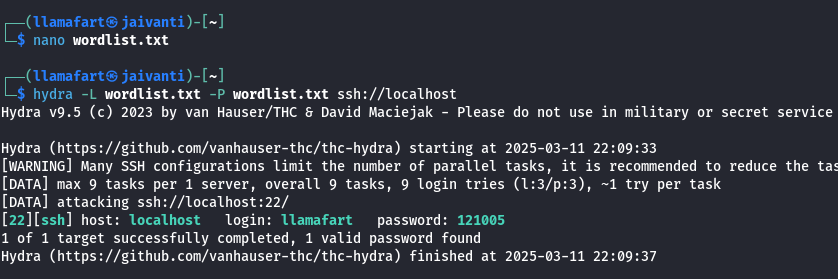
Modify the following lines:



**4. Exploitation**

**4.1. Perform a Brute-Force Attack Using Hydra**

* 1. **Create a Wordlist & Run Hydra to Brute-Force SSH**:

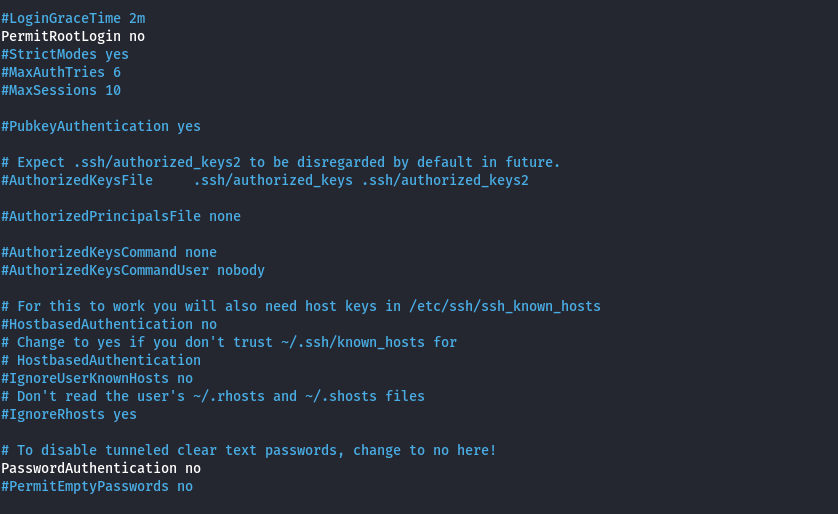


**5. Mitigation**

**5.1. Disable Root Login and Password Authentication**

**1. Edit SSH Configuration:**

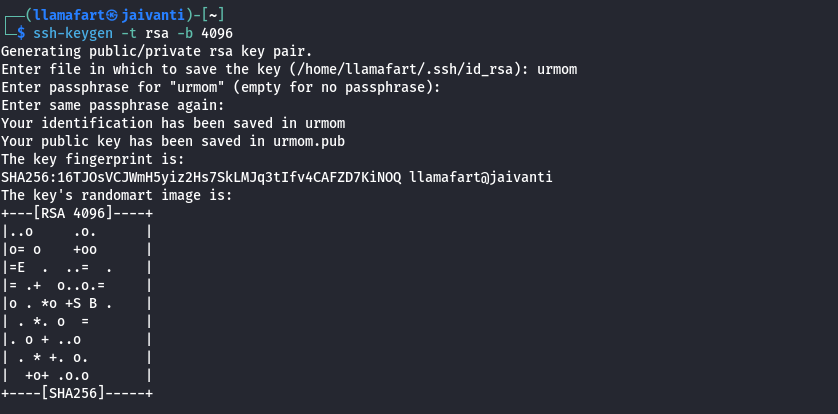
**Open the SSH configuration file and modify the following lines:**



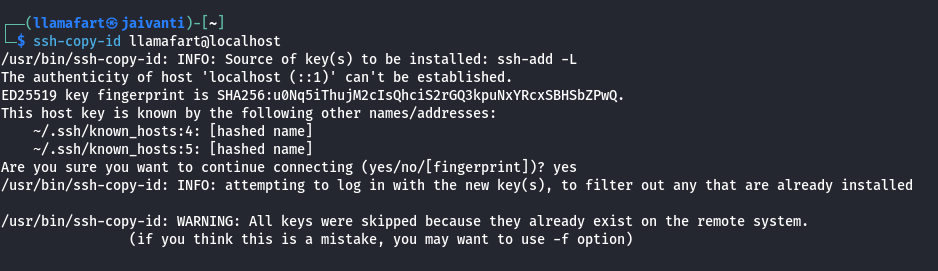
**Save and exit the file, then restart the SSH service:**

**5.2. Enable Key-Based Authentication**

1. **Generate SSH Keys (on the client machine):**



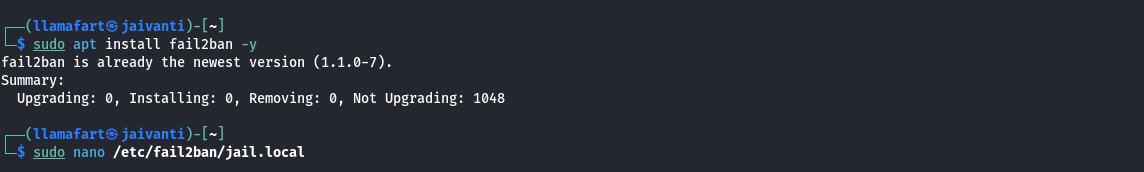
1. **Copy the Public Key to the Server:**



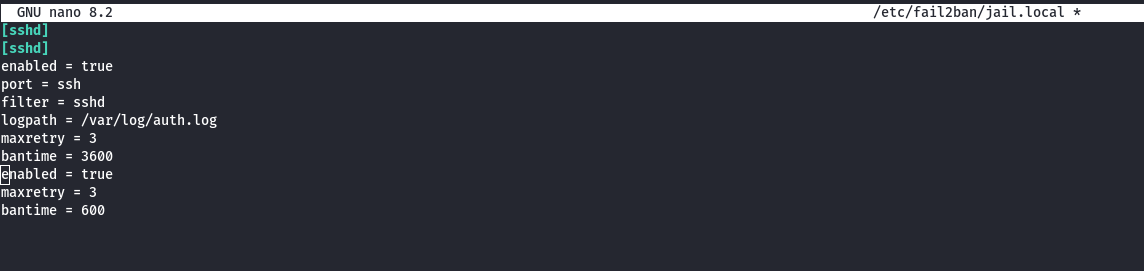
**5.3. Configure Fail2Ban to Prevent Brute-Force Attacks**

1. **Install Fail2Ban & Configure Fail2Ban for SSH:**

Create a local configuration file:



Add the following lines:



Save and exit the file, then restart Fail2Ban:



1. **Verify Fail2Ban Status**:



**6. Conclusion**:

This PoC successfully demonstrated the risks of insecure SSH configurations and the effectiveness of hardening measures. By disabling root login, enforcing key-based authentication, and preventing brute-force attacks, the SSH service was secured