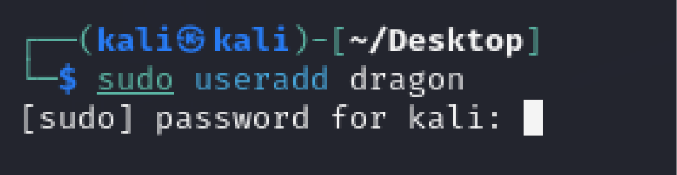
**Task 1: User & Permission Misconfigurations**

Step 1: Setup – Create Users & Assign Incorrect Permissions

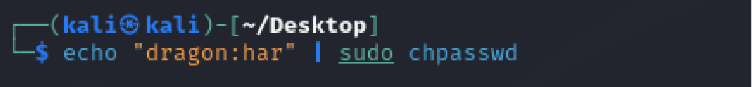
We will create multiple users and deliberately misconfigure file permissions.

1. Create Users

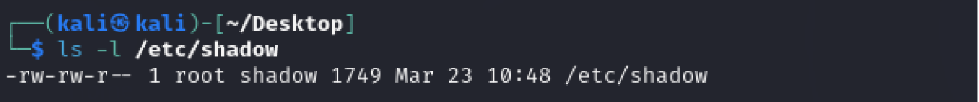
Run the following commands as root or using sudo :



* useradd creates users.
* chpasswd sets passwords for users.

****

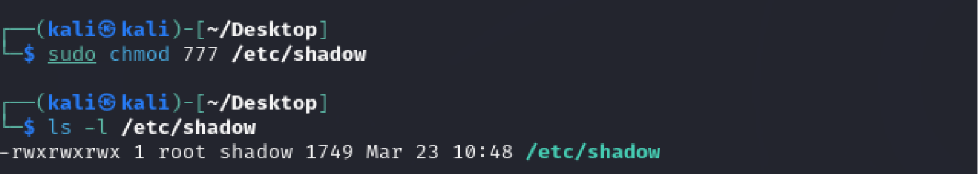
Step 2: Exploit and detecting – Access Sensitive Files as a Low-Privilege User Modify User Information as a Low-Privilege User to check



Step 3: Change the permissions of /etc/shadow (which stores hashed passwords) to be world-readable and writable

sudo chmod 777 /etc/shadow

sudo chmod 777 /etc/passwd

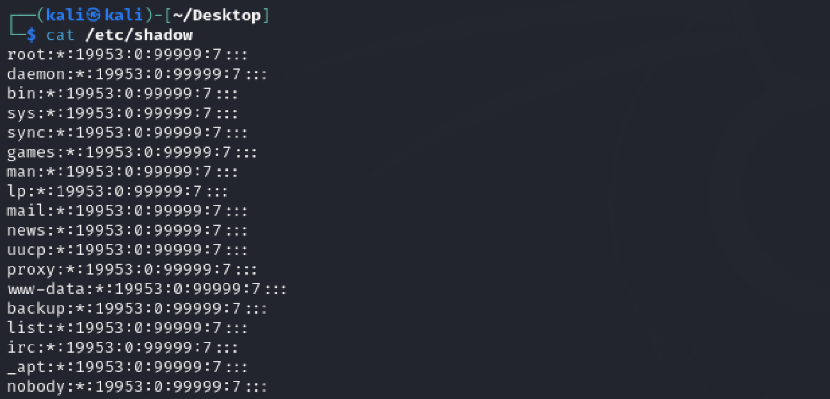
* 777 gives **read, write, and execute permissions to everyone**, including normal users.
* This is a **critical security risk** because now any user can read **password hashes** or even modify user information.
* 

**Step 4: Mitigation – Fix the Permission Issues and Verify File Permissions**

To **correct the misconfiguration**, switch back to root and secure file permissions.

**1. Restore Correct File Permissions**

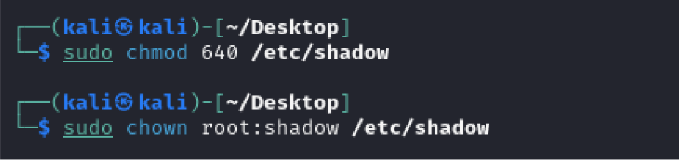
* /etc/shadow should be **readable only by root (640)**.
* /etc/passwd should be **readable by all but writable only by root (644)**.



Step 5: Check whether the verifications and restrictions are assigned:

Remove unnecessary users from sudo access.

Restrict useradd from running dangerous commands.

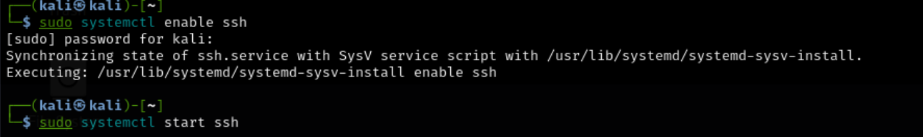


**Summary**

**Setup:** Created users and changed permissions to 777.  
**Exploit:** Accessed /etc/shadow and modified /etc/passwd as a low-privilege user.  
**Mitigation:** Restored secure file permissions and restricted sudo access. This task helps **understand privilege escalation** and **how misconfigured permissions can lead to security breaches**.

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

Step 1: Setup – Enable SSH with Weak Security Settings



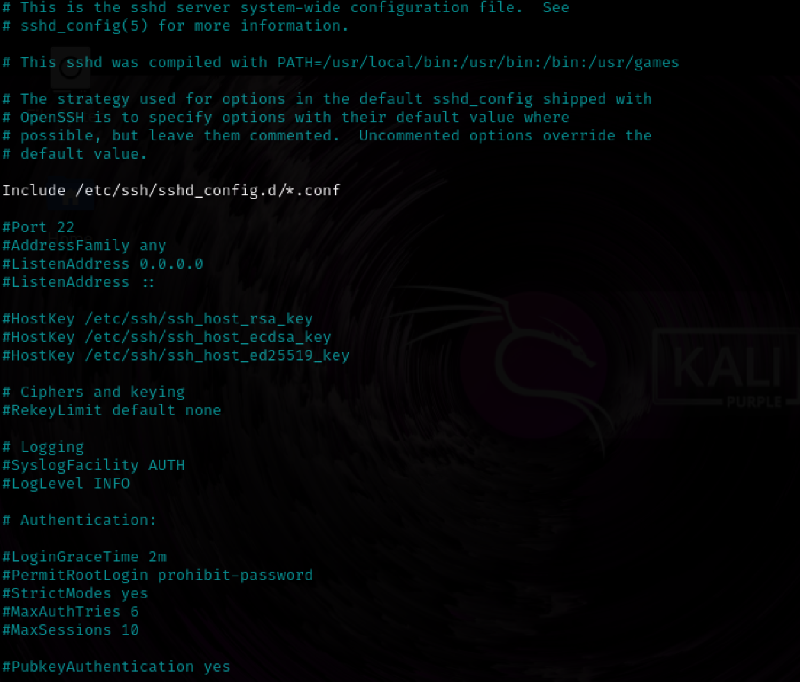
Step 2: Allow Root Login & Password Authentication

Edit the SSH configuration file:

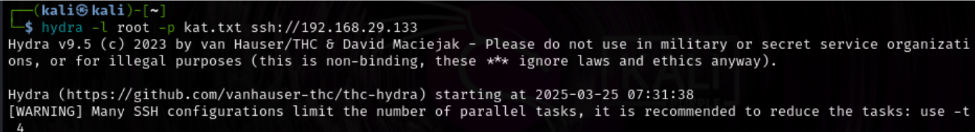


-PermitRootLogin yes **allows root login** (security risk).

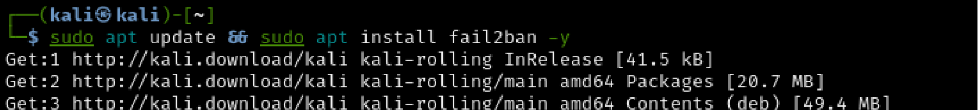
-PasswordAuthentication yes **enables password-based login**, making it vulnerable to brute-force attacks then after this make sure you restart the terminal.



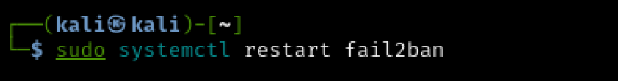
Step 3: Exploit – Perform a Brute-Force Attack on SSH



Step 4 : **Configure Fail2Ban to Block Brute-Force Attempts**

****

Step 5 : And atlast check and restart fail2ban:



**Summary**

**Setup:** Enabled SSH with root login & password authentication.  
**Exploit:** Performed a brute-force attack using **Hydra/Medusa**.  
**Mitigation:** Disabled root login, enforced **key-based authentication**, and configured **Fail2Ban**.