TASK 2

TASK 2:

Remote Access & SSH Hardening

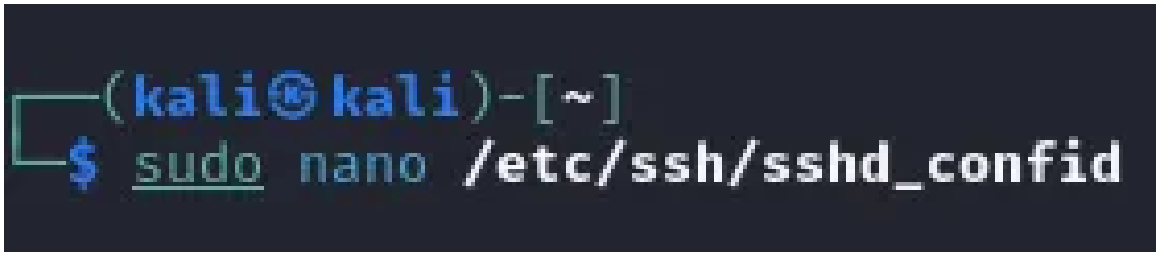
Setup: Enabling SSH & Weak Configuration :

1.To start the SSH service, we enable it with **sudo systemctl enable ssh** and start it using **sudo systemctl start ssh** for remote access.

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable ssh
[sudo] password for kali:
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh

┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable ssh && sudo systemctl start ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
```

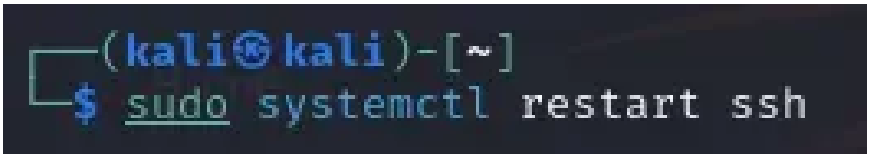
2.
Next, we modify the SSH configuration to allow root login and enable password authentication by editing the
/etc/ssh/sshd_config file. We open the file using a text editor such as **nano** or **vim** with elevated privileges Inside the file, we locate and modify the following lines After saving the changes, we restart the SSH service to apply the new configuration:



3.Update the **PermitRootLogin** and **PasswordAuthentication** parameters to yes.

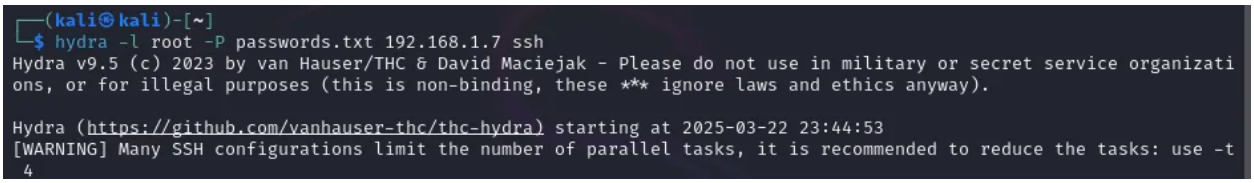
4. Then we restart the ssh service.

TASK 2 .1



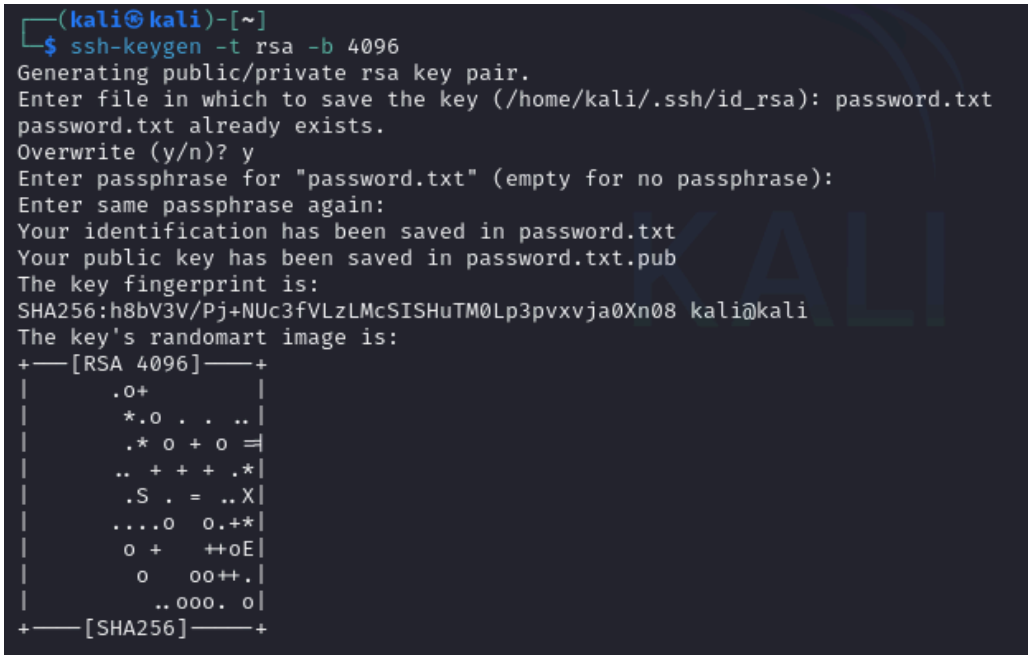
Exploitation: Brute-Forcing SSH🛠️:

1.We use **Hydra** with a custom wordlist to brute-force SSH root login on our machine, testing authentication security and password strength.



2.To secure SSH, we disable root login and password authentication by setting **PermitRootLogin no** and **PasswordAuthentication no**, then restart the service..

3 .To secure authentication, generate an SSH key pair with **ssh-keygen -t rsa -b 4096**, copy the public key using **ssh-copy-id user@<server_ip>**, and restart SSH.



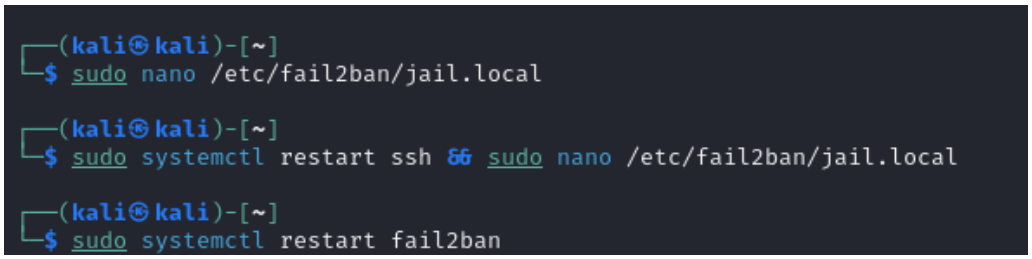
TASK 2 .2

Configure Fail2Ban to Prevent Brute-Force Attacks:

- Install **Fail2Ban** with **sudo apt install fail2ban -y** to block brute-force attacks.
- Configure it by editing **/etc/fail2ban/jail.local** with **sudo nano**, then set:
- ini
  CopyEdit

TASK 2 .3

3.Finally restart fail2ban to avoid ssh attacks.


┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/fail2ban/jail.local
┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart ssh && sudo nano /etc/fail2ban/jail.local
┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart fail2ban