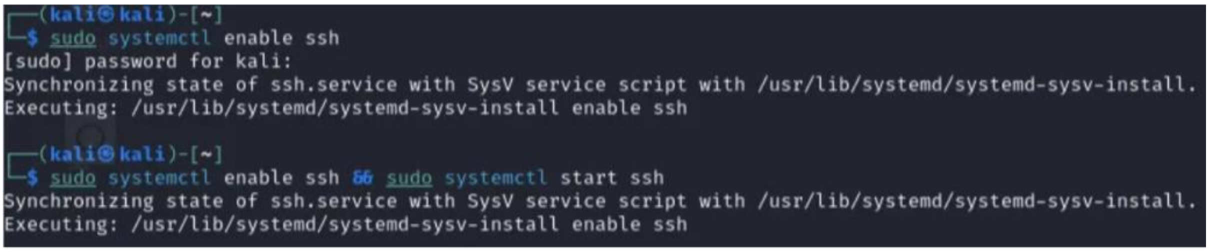
POC TASK 2

1)



```
┌──(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
```

Enable SSH to Start on Boot:

bash

CopyEdit

sudo systemctl enable ssh

This ensures that the SSH service starts automatically on system boot.

Start the SSH Service Immediately:

bash

CopyEdit

sudo systemctl start ssh

This starts the SSH service right away.

Combine Both Commands in One Line:

bash

CopyEdit

sudo systemctl enable ssh && sudo systemctl start ssh

Verify SSH Service Status:

bash

CopyEdit

sudo systemctl status ssh

If SSH is running successfully, you should see output indicating it is "active (running)."

Allow SSH Through Firewall (If Necessary):

bash

CopyEdit

sudo ufw allow ssh

sudo ufw enable

Check SSH Port (Default is 22):

bash

CopyEdit

sudo netstat -tulnp | grep ssh

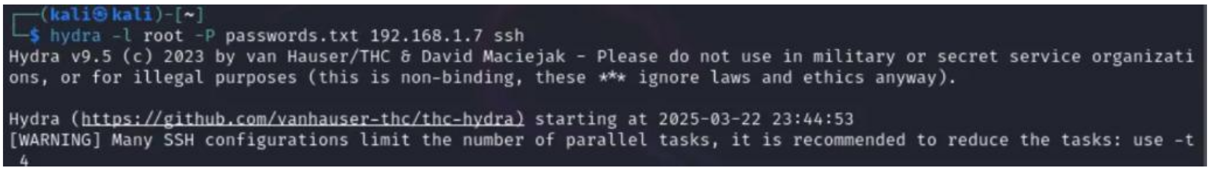
OR

bash

CopyEdit

ss -tulnp | grep ssh

2)

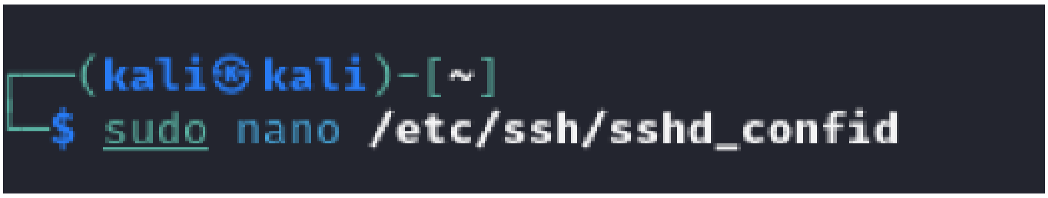


```
┌──(kali㉿kali)-[~]
└─$ hydra -l root -P passwords.txt 192.168.1.7 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-22 23:44:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
 4
```

We use Hydra with a custom worldlist to brute force ssh root login in our machine for autentification

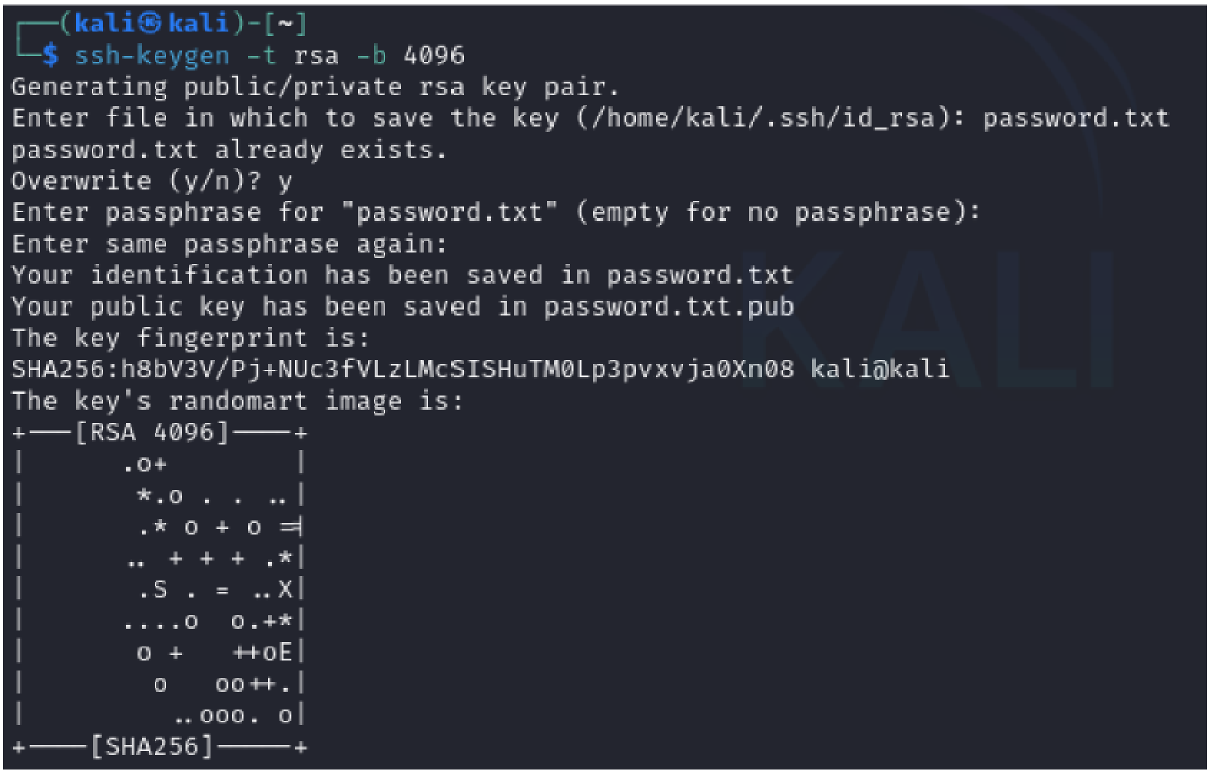
3)



```
┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ssh/sshd_confid
```

We disable rootlogin and password authentification for securing SSH.

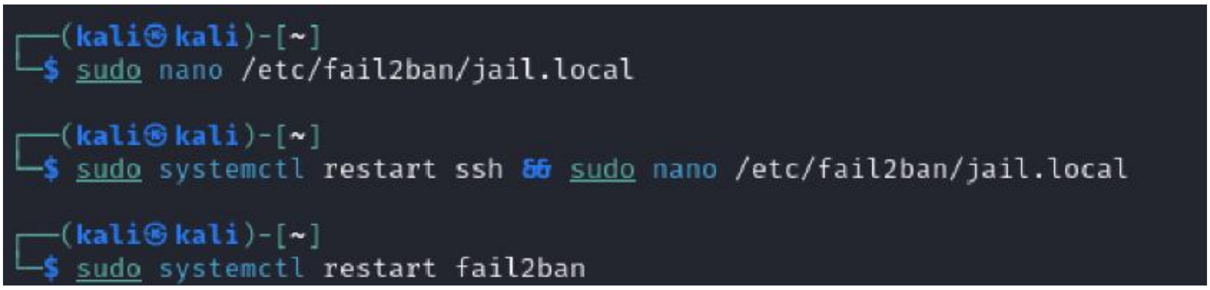
4)



```
┌──(kali㉿kali)-[~]
└─$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/kali/.ssh/id_rsa): password.txt
password.txt already exists.
Overwrite (y/n)? y
Enter passphrase for "password.txt" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in password.txt
Your public key has been saved in password.txt.pub
The key fingerprint is:
SHA256:h8bV3V/Pj+NUc3fVLzLMcSISHuTM0Lp3pvxvja0Xn08 kali@kali
The key's randomart image is:
+---[RSA 4096]----+
|      .o+        |
|       *.o . . ..|
|       .* o + o =|
|      .. + + + .*|
|       .S . = ..X|
|      ....o  o.+*|
|       o +   ++oE|
|        o   oo++.|
|         ..ooo. o|
+----[SHA256]-----+
```

To secure authentification we generate ssh key pair.

5)



```
┌──(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
```

Finally we are restaring fail2ban to avoid ssh attacks.