POC Task 2

1. Setup: Enabling SSH & Weak Security Settings

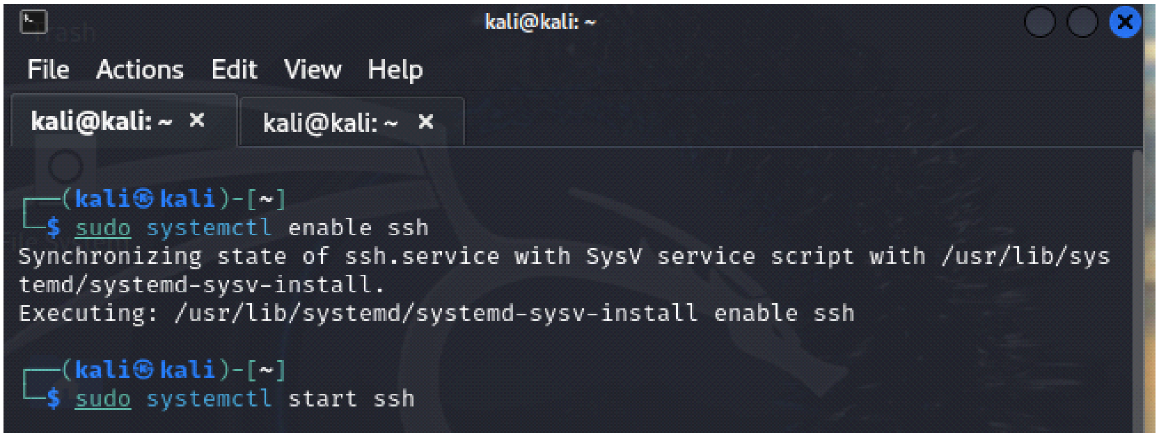
1.1 Install & Enable SSH

Ensure SSH is installed and running:

sudo apt update && sudo apt install -y openssh-server

sudo systemctl enable ssh

sudo systemctl start ssh

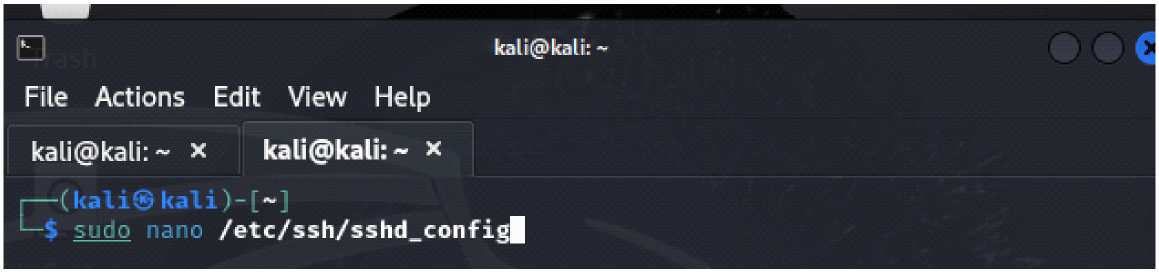


```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start ssh
```

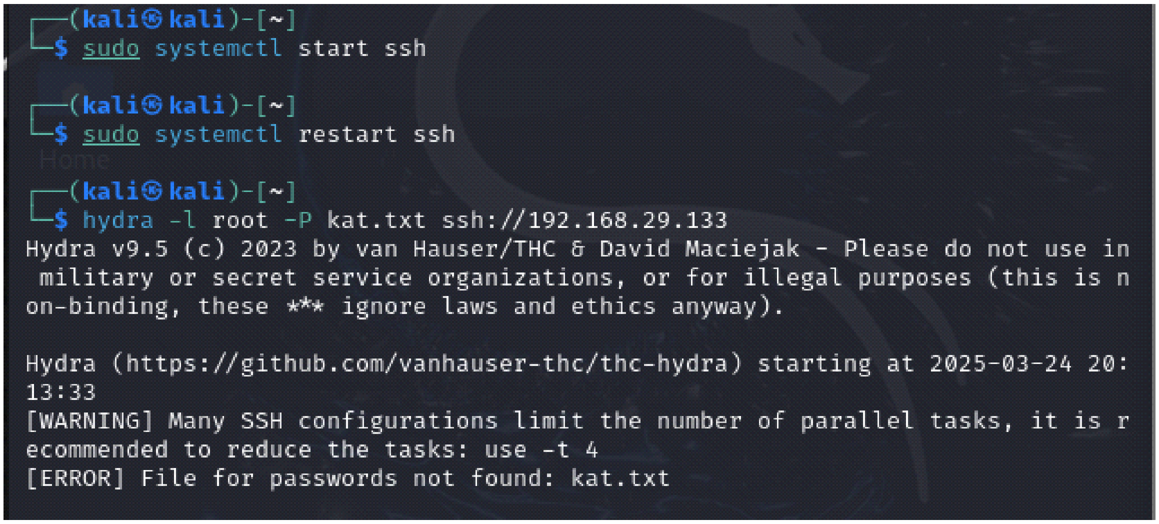
1.2 Allow Root Login & Password Authentication

Edit the SSH configuration file:



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

Restart SSH to apply changes:



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start ssh

┌──(kali㉿kali)-[~]
└─$ sudo systemctl restart ssh

┌──(kali㉿kali)-[~]
└─$ hydra -l root -P kat.txt ssh://192.168.29.133
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-24 20:
13:33
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[ERROR] File for passwords not found: kat.txt
```

2) Exploit:

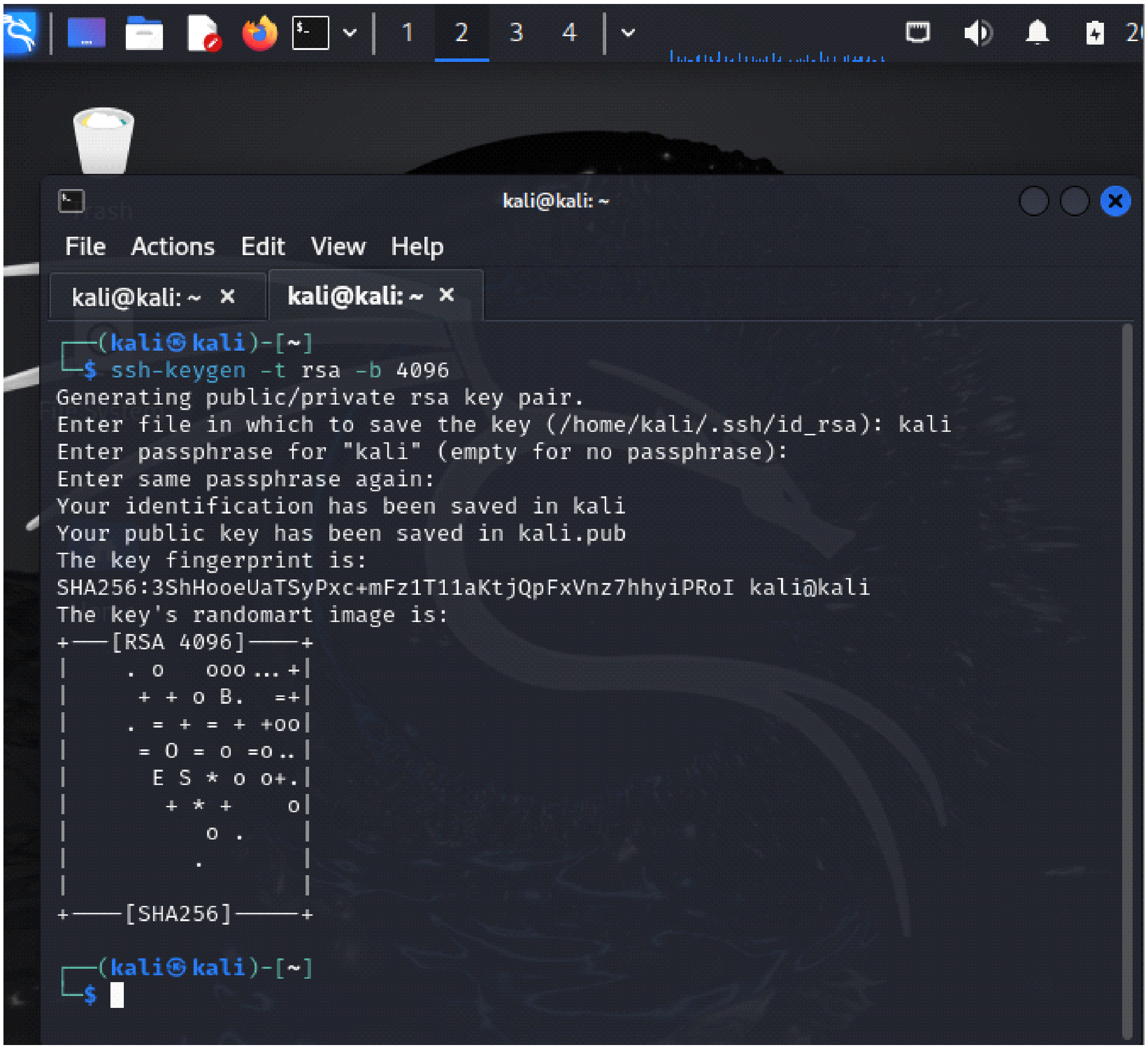
2.1)Disable root login:

sudo nano /etc/ssh/sshd_config

# Set PermitRootLogin no

3.2 Enable Key-Based Authentication

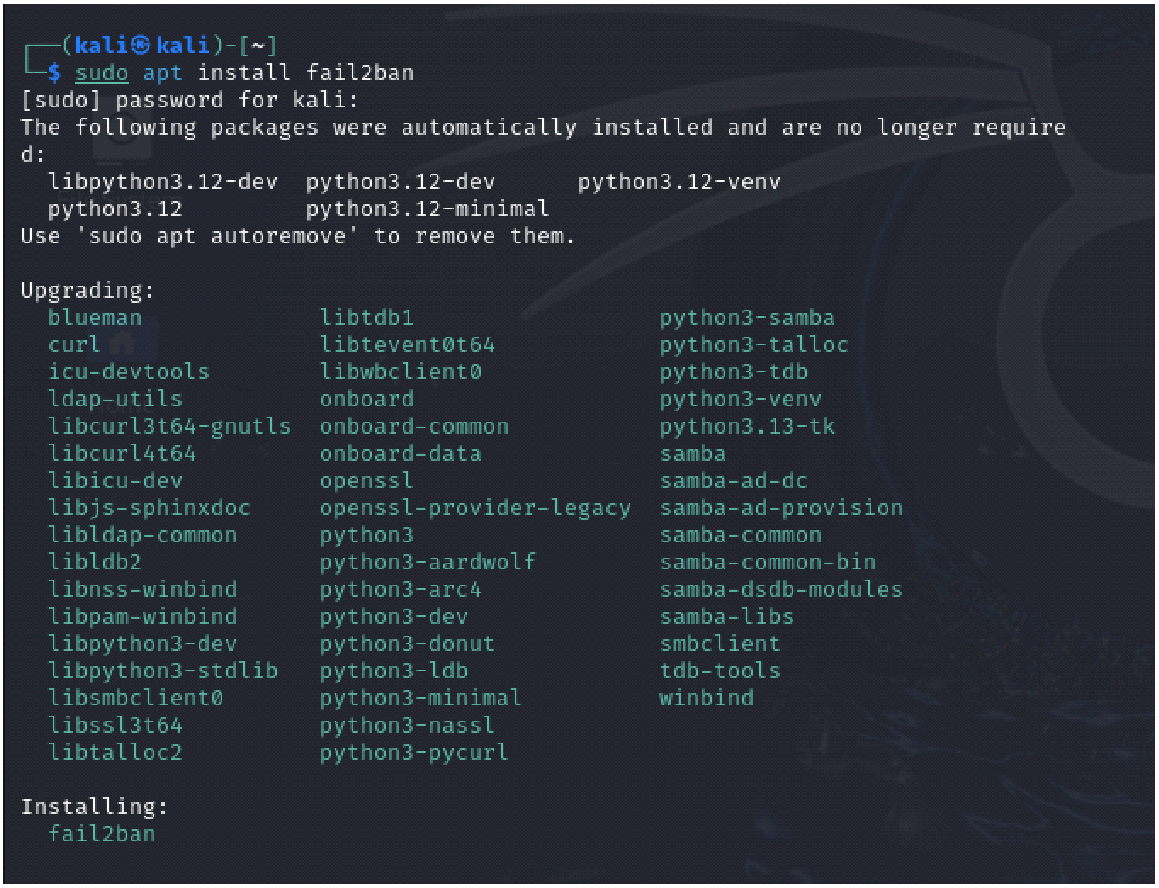
On your local machine, generate SSH keys:



```
┌──(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): kali
Enter passphrase for "kali" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in kali
Your public key has been saved in kali.pub
The key fingerprint is:
SHA256:3ShHooeUaTSyPxc+mFz1T11aKtjQpFxVnz7hhyiPRoI kali@kali
The key's randomart image is:
+───[RSA 4096]────+
|    . o   ooo...+|
|     + + o B.  =+|
|    . = + = + +oo|
|     = O = o =o..|
|      E S * o o+.|
|       + * +    o|
|          o .    |
|         .       |
|                 |
+────[SHA256]─────+

┌──(kali㉿kali)-[~]
└─$
```

4) Configure fail2ban:

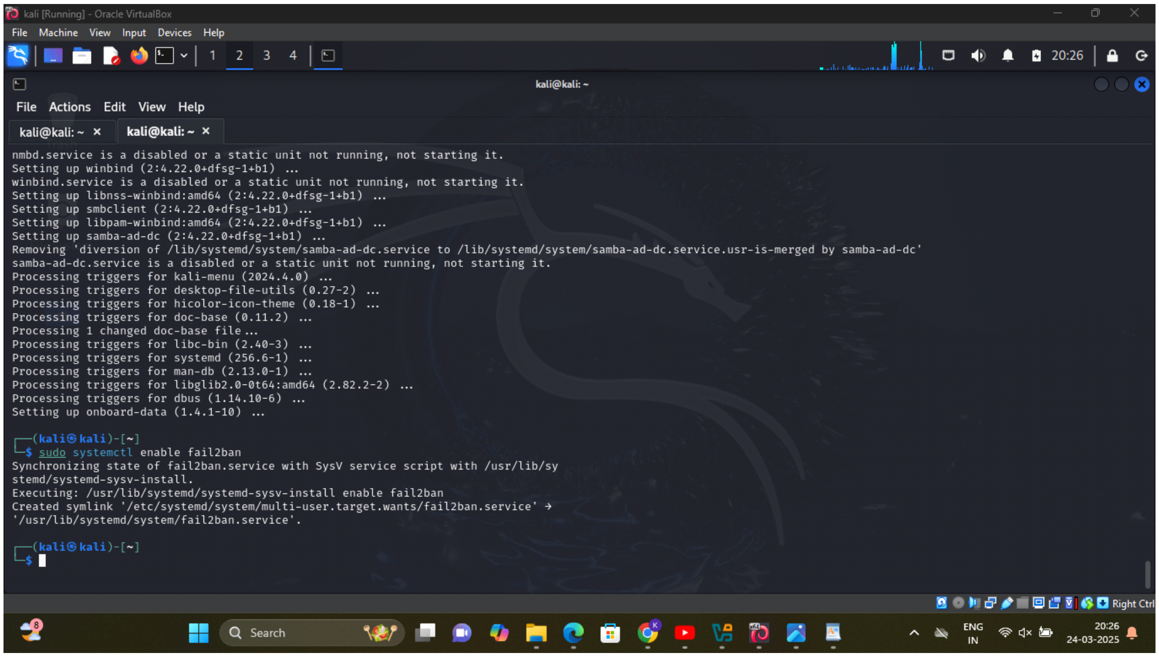


```
┌──(kali㉿kali)-[~]
└─$ sudo apt install fail2ban
[sudo] password for kali:
The following packages were automatically installed and are no longer require
d:
  libpython3.12-dev  python3.12-dev      python3.12-venv
  python3.12         python3.12-minimal
Use 'sudo apt autoremove' to remove them.

Upgrading:
  blueman              libtdb1                  python3-samba
  curl                 libtevent0t64            python3-talloc
  icu-devtools         libwbclient0             python3-tdb
  ldap-utils           onboard                  python3-venv
  libcurl3t64-gnutls   onboard-common           python3.13-tk
  libcurl4t64          onboard-data             samba
  libicu-dev           openssl                  samba-ad-dc
  libjs-sphinxdoc      openssl-provider-legacy  samba-ad-provision
  libldap-common       python3                  samba-common
  libldb2              python3-aardwolf         samba-common-bin
  libnss-winbind       python3-arc4             samba-dsdb-modules
  libpam-winbind       python3-dev              samba-libs
  libpython3-dev       python3-donut            smbclient
  libpython3-stdlib    python3-ldb              tdb-tools
  libsmbclient0        python3-minimal          winbind
  libssl3t64           python3-nassl
  libtalloc2           python3-pycurl

Installing:
  fail2ban
```

4.2) sudo systemctl enable fail2b



```
nmbd.service is a disabled or a static unit not running, not starting it.
Setting up winbind (2:4.22.0+dfsg-1+b1) ...
winbind.service is a disabled or a static unit not running, not starting it.
Setting up libnss-winbind:amd64 (2:4.22.0+dfsg-1+b1) ...
Setting up smbclient (2:4.22.0+dfsg-1+b1) ...
Setting up libpam-winbind:amd64 (2:4.22.0+dfsg-1+b1) ...
Setting up samba-ad-dc (2:4.22.0+dfsg-1+b1) ...
Removing 'diversion of /lib/systemd/system/samba-ad-dc.service to /lib/systemd/system/samba-ad-dc.service.usr-is-merged by samba-ad-dc'
samba-ad-dc.service is a disabled or a static unit not running, not starting it.
Processing triggers for kali-menu (2024.4.0) ...
Processing triggers for desktop-file-utils (0.27-2) ...
Processing triggers for hicolor-icon-theme (0.18-1) ...
Processing triggers for doc-base (0.11.2) ...
Processing 1 changed doc-base file...
Processing triggers for libc-bin (2.40-3) ...
Processing triggers for systemd (256.6-1) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for libglib2.0-0t64:amd64 (2.82.2-2) ...
Processing triggers for dbus (1.14.10-6) ...
Setting up onboard-data (1.4.1-10) ...

┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /usr/lib/sy
stemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable fail2ban
Created symlink '/etc/systemd/system/multi-user.target.wants/fail2ban.service' →
'/usr/lib/systemd/system/fail2ban.service'.

┌──(kali㉿kali)-[~]
└─$ 
```