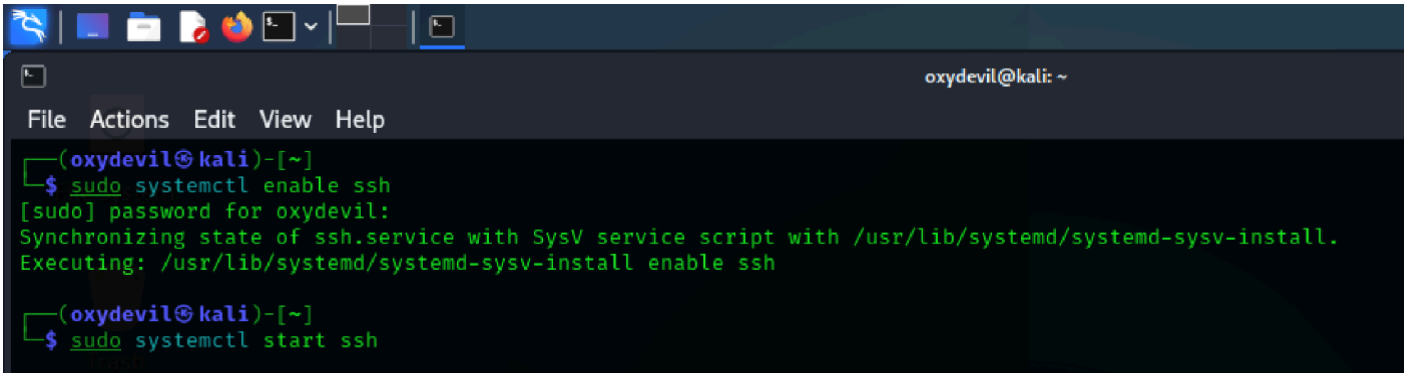
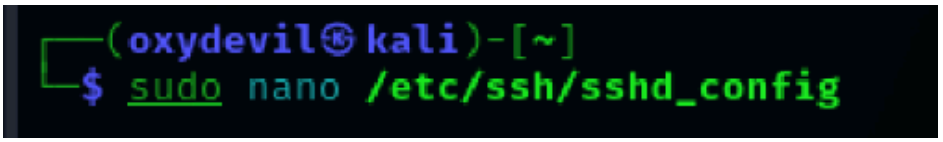
TASK 2:

Setup: Enabling SSH & Weak Configuration

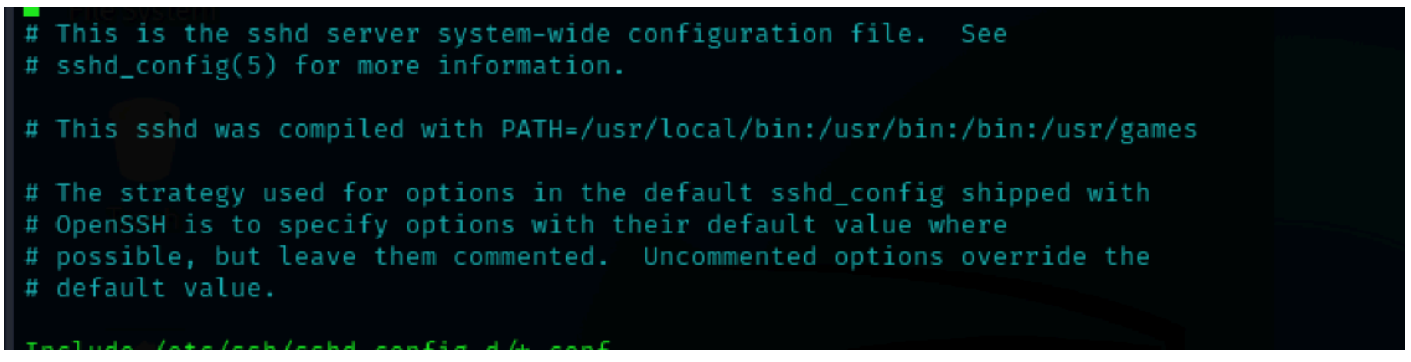
1.To initiate the SSH service, we first **activate** it using sudo systemctl enable ssh, followed by sudo systemctl start ssh.

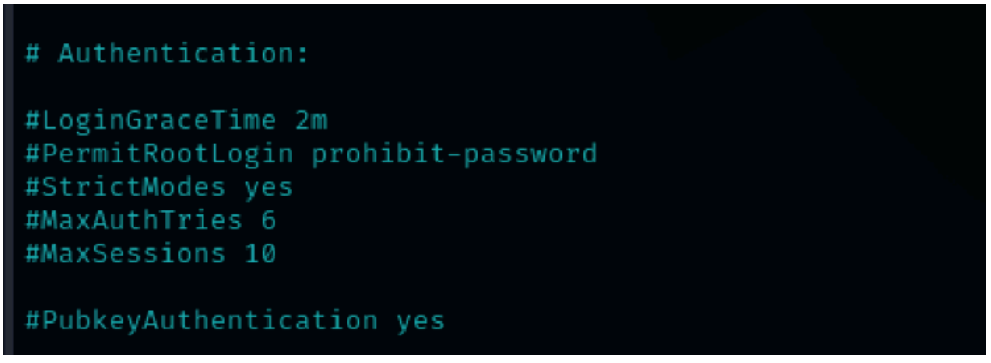


2.Next, we update the SSH configuration to allow root login and enable password authentication by modifying the /etc/ssh/sshd_config file.

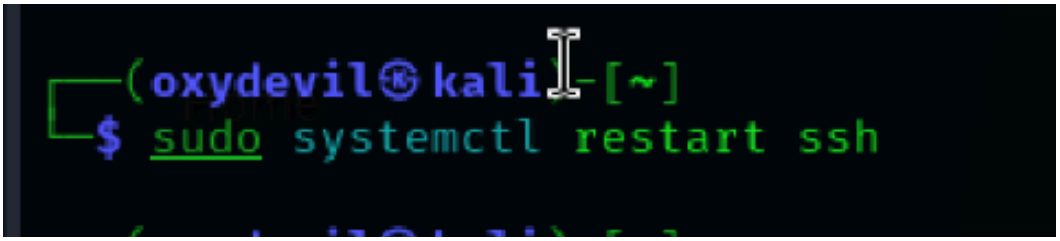


3. Update the PermitRootLogin and PasswordAuthentication parameters to yes.



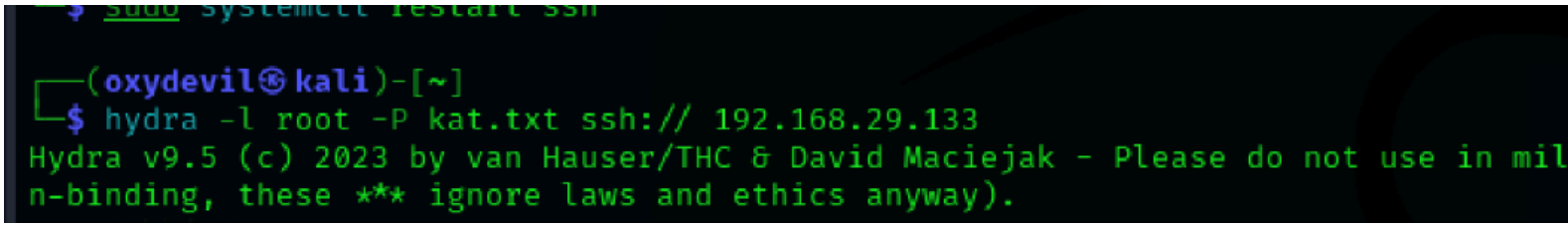


4.Then we restart the ssh service.

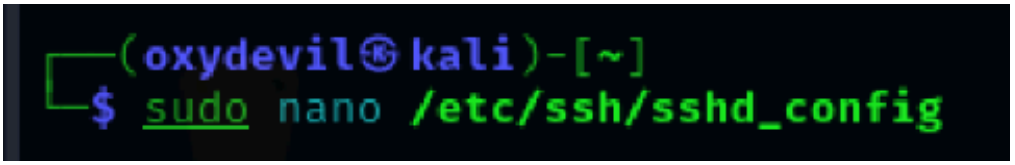


EXPOILATION: BRUTE FORCING SSH

1. We use Hydra to perform a brute-force SSH root login.



2.Root login and password authentication are disabled by setting PermitRootLogin no and PasswordAuthentication no to enhance security.



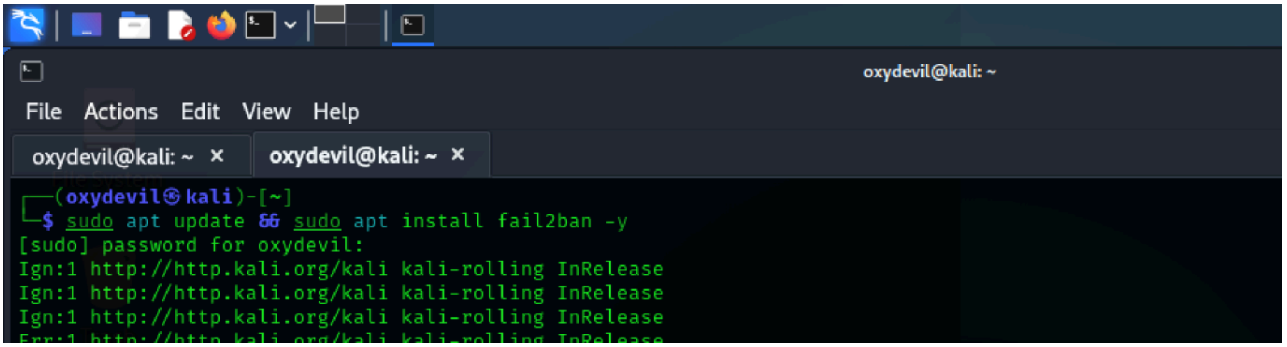
3.To enhance authentication security, generate an SSH key pair on the client machine using ssh-keygen -t rsa -b 4096 . Next, copy the public key to the server with ssh-copy-id user@ , and finally, restart the SSH service using sudo systemctl restart ssh.

```
┌──(oxydevil㉿kali)-[~]
└─$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/oxydevil/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Passphrases do not match.  Try again.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/oxydevil/.ssh/id_rsa
Your public key has been saved in /home/oxydevil/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:3llZ9jASZ30GKUMBhqJ3MPdxhv6DEXfBSz7+co5A6tA oxydevil@kali
The key's randomart image is:
+---[RSA 4096]----+
|          .o++o== |
|       + o.+ *+= +|
|      . = o *.*=o.|
|     . . . +  =++ |
|      . .S  ++. ..|
|        . o.=o .  |
|         o E .. . |
|          o    ...o|
|           .   .+.|
+----[SHA256]-----+
```

```
┌──(oxydevil㉿kali)-[~]
└─$ ssh-copy-id user@192.168.62.133
/usr/bin/ssh-copy-id: INFO: Source of key(s) to
```

Configure Fail2Ban to Prevent Brute-Force Attacks

1.To improve system security, install Fail2Ban using sudo apt install fail2ban -y. It helps defend against brute-force attacks by detecting and blocking suspicious login attempts.



2. Finally restart fail2ban to avoid ssh attacks.

```
┌──(oxydevil㉿kali)-[~]
└─$ sudo systemctl restart fail2ban
```