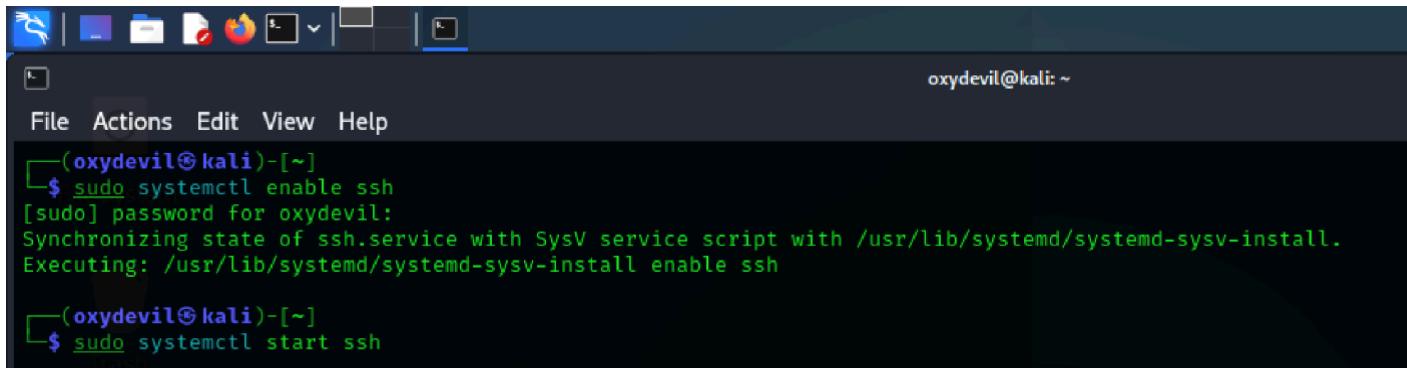


TASK 2:

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.



The screenshot shows a terminal window with a dark theme. The title bar says "oxydevil@kali: ~". The menu bar includes "File", "Actions", "Edit", "View", and "Help". The terminal prompt is "(oxydevil㉿kali)-[~] \$". The user runs the command "sudo systemctl enable ssh", which prompts for a password. The output shows the service being synchronized and executed. Then, the user runs "sudo systemctl start ssh".

```
(oxydevil㉿kali)-[~]
$ sudo systemctl enable ssh
[sudo] password for oxydevil:
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

(oxydevil㉿kali)-[~]
$ sudo systemctl start ssh
```

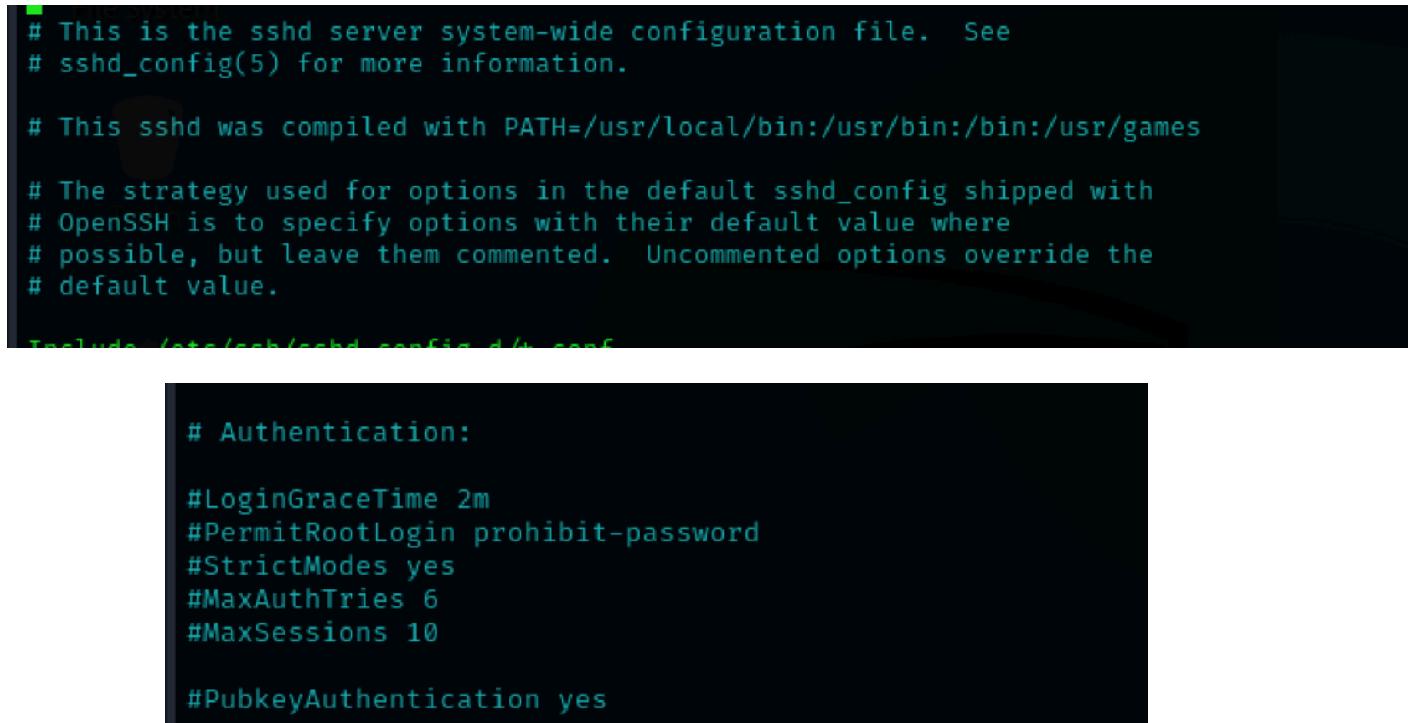
2. Next, we update the SSH configuration to allow root login and enable password authentication by modifying the /etc/ssh/sshd_config file.



The screenshot shows a terminal window with a dark theme. The prompt is "(oxydevil㉿kali)-[~] \$". The user runs the command "sudo nano /etc/ssh/sshd_config".

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

3. Update the PermitRootLogin and PasswordAuthentication parameters to yes.



The screenshot shows the contents of the /etc/ssh/sshd_config file. It includes comments about the file's purpose and compilation, and a section for authentication parameters. The "Authentication:" section is highlighted.

```
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes
```

4.Then we restart the ssh service.

```
(oxydevil㉿kali)-[~]
$ sudo systemctl restart ssh
```

EXPOILATION: BRUTE FORCING SSH

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

```
* sudo systemctl restart ssh

(oxydevil㉿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 mil
n-binding, these ** ignore laws and ethics anyway).
```

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

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

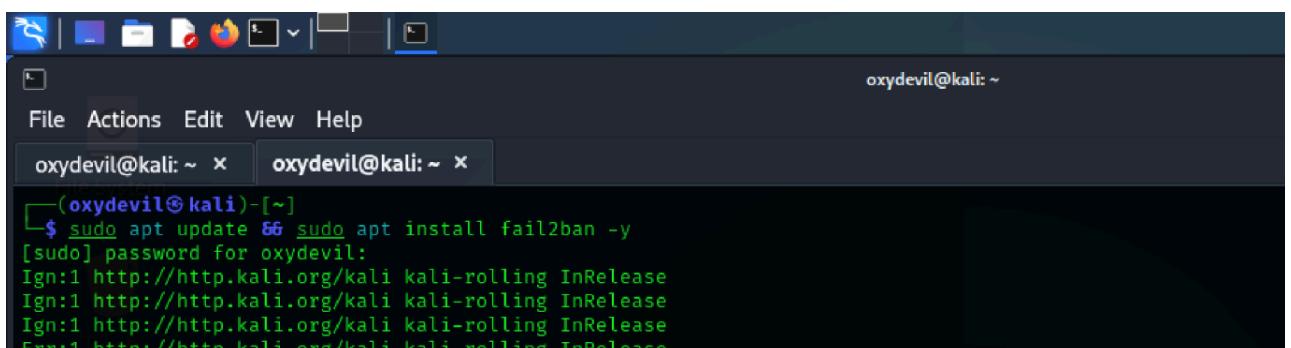
3.To enhance authentication security, generate an SSH key pair on the client machine using ssh-keygen -t rsa -b 4096 . Next, copy the public key to the server with ssh-copy-id user@ , and finally, restart the SSH service using sudo systemctl restart ssh.

```
└─(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: TNEO: Source of key(s) to
```

Configure Fail2Ban to Prevent Brute-Force Attacks

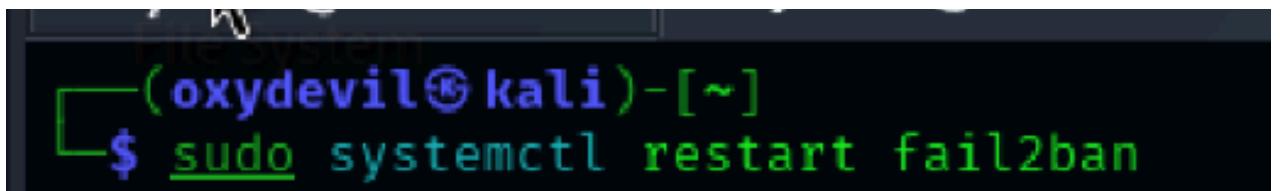
1. To improve system security, install Fail2Ban using sudo apt install fail2ban -y. It helps defend against brute-force attacks by detecting and blocking suspicious login attempts.



The screenshot shows a terminal window with two tabs open. The current tab is titled 'oxydevil@kali: ~'. The command entered is '\$ sudo apt update && sudo apt install fail2ban -y'. The output shows the update process and the successful installation of fail2ban. The status bar at the bottom right indicates 'oxydevil@kali: ~'.

```
oxydevil@kali: ~
$ sudo apt update && sudo apt install fail2ban -y
[sudo] password for oxydevil:
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Ign:1 http://http.kali.org/kali kali-rolling InRelease
Err:1 http://http.kali.org/kali kali-rolling InRelease
```

2. Finally restart fail2ban to avoid ssh attacks.



The screenshot shows a terminal window with two tabs open. The current tab is titled 'oxydevil@kali: ~'. The command entered is '\$ sudo systemctl restart fail2ban'. The status bar at the bottom right indicates 'oxydevil@kali: ~'.

```
oxydevil@kali: ~
$ sudo systemctl restart fail2ban
```