

# 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:

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

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

4. Then we restart the ssh service.

## TASK 2.1

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

### 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.

```
(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 organizations, 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
```

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

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

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.

```

(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]--+

```

```

(kali@kali)-[~]
$ sudo systemctl 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
```