Task 2 : Remote Access & SSH Hardening

Step 1: Enabling SSH & Weak Configuration :

```
File  Actions  Edit  View  Help
┌──(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 start ssh
```

1.To start the SSH service, first enable it using **sudo systemctl enable ssh**, then start it with **sudo systemctl start ssh** to ensure it is running and ready for remote access

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

[sudo] password for kali:
```

2.we modify the SSH configuration to permit root login and enable password authentication by editing **/etc/ssh/sshd_config** file.

```
# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication no
#PermitEmptyPasswords no
```

```
#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
```

Update the **PermitRotLogin** and **PasswordAuthentication** parameters to **yes**.

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

1. Now ,restart the ssh service.

Exploitation:

Brute-Forcing SSH :

```
┌──(kali㉿vbox)-[~]
└─$ hydra -l root -P kat.txt  ssh://192.168.29.133
```

1.We use Hydra to brute-force SSH root login with a custom wordlist to test authentication security.

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

[sudo] password for kali:
```

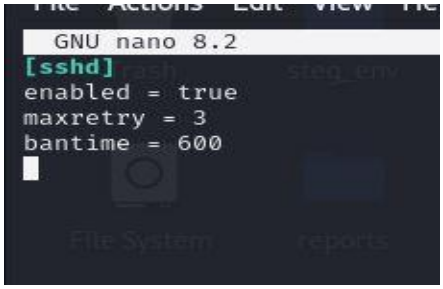
2.To improve security, disable root login and password authentication in the SSH config file, then restart SSH to apply the changes.

```
┌──(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): file.txt
Enter passphrase for "file.txt" (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in file.txt
Your public key has been saved in file.txt.pub
The key fingerprint is:
SHA256:NKcjknYrEhQjx+a44XNbj1XwlLHAuP/T3gLePunzL/0 kali@kali
The key's randomart image is:
+---[RSA 4096]----+
|..+   o. .o      |
| ooo . o.o.      |
| +.   . *..      |
|o..  o . *       |
|.o. + + S        |
|.o + + = o       |
|  + + = o + . .  |
|   o o . + B.. . |
|          =+=oo.E|
+----[SHA256]-----+
```

4.Generate an SSH key pair on the client using ssh-keygen, copy the public key to the server with ssh-copy-id **user@server**, and restart SSH using **sudo systemctl restart ssh** to apply the changes.

Configure Fail2Ban to Prevent Brute-Force Attacks

Install Fail2Ban using **sudo apt install fail2ban** to protect against brute-force attacks by blocking suspicious login.



2.Edit the Fail2Ban config file with **sudo nano /etc/fail2ban/jail.local**, then add settings under [sshd] to limit login attempts.

3. Finally restart fail2ban to avoid ssh attacks.