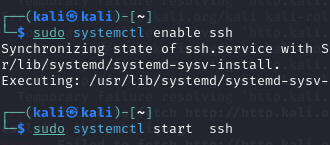
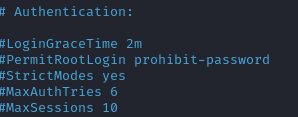
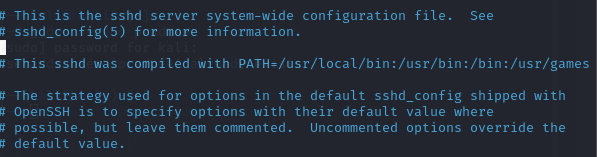
Task 2 : Remote Access & SSH Hardening

Setup: Enabling SSH & Weak Configuration



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



2.Next, we modify the SSH configuration to permit root login and enable password authentication by editing the /etc/ssh/sshd\_config file. 

3. Update the PermitRootLogin and PasswordAuthentication parameters to yes.



4.Then we restart the ssh service.

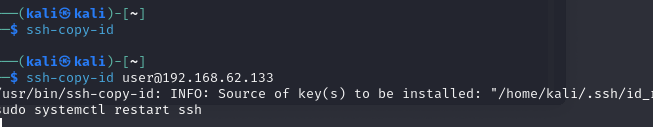
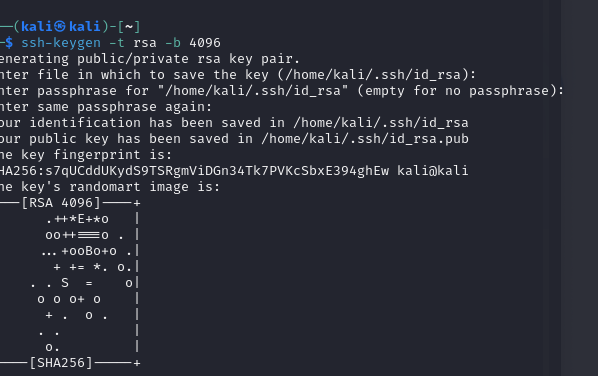
EXPOILATION: BRUTE\_FORCING SSH



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



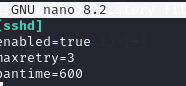
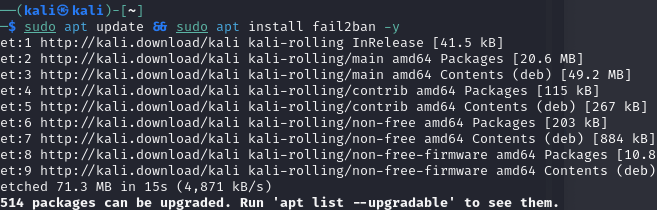
2. To enhance security, root login and password authentication are disabled by setting PermitRootLogin no and PasswordAuthentication no.



4 . 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.

Configure Fail2Ban to Prevent Brute-Force Attacks

1. To enhance system security, install Fail2Ban by running sudo apt install fail2ban -y , which helps protect against brute-force attacks by monitoring and blocking suspicious login attempts.

(here we installed the Fail2ban and performed the required tasks).

3. To configure Fail2Ban, edit the jail configuration file using sudo nano /etc/fail2ban/jail.local , then add the following settings under [sshd] : enabled = true , maxretry = 3 , and bantime = 600.



4. Finally restart fail2ban to avoid ssh attacks.