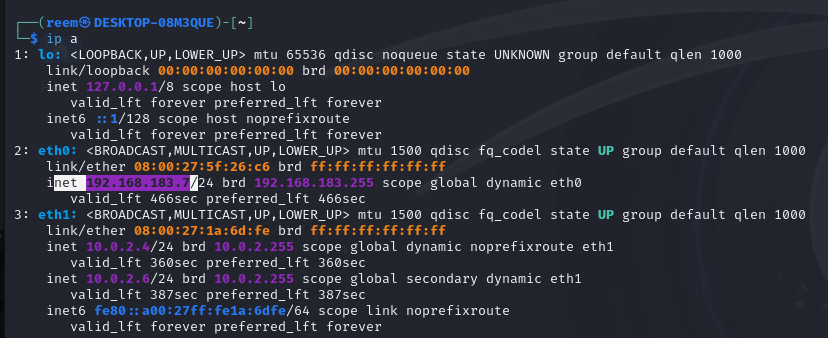
**Phase-3**

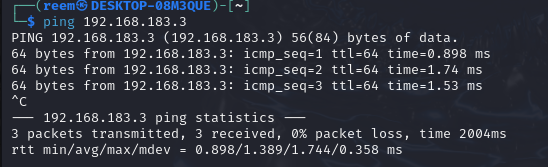
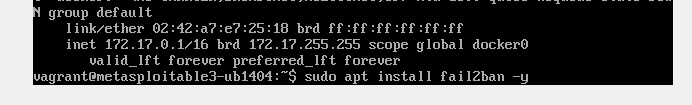
**Defense Mechanism**:  
We implemented Fail2Ban on the Metasploitable3 to protect against SSH brute-force attacks.   
Also validate an effective defense mechanism against SSH brute-force attacks on the Metasploitable3 victim machine. Fail2Ban was chosen for its ability to monitor failed login attempts and automatically block attacker IPs after a defined number of failures. The defense was tested using Hydra from the attacker machine to simulate a real brute-force scenario.

**Testing & Validation**:  
we performed a brute-force SSH attack with hydra on the attacker machine, using incorrect credentials from a password list. As intended, the attack triggered Fail2Ban failed login attempts. The attacker's IP address 192.168.183.7 was automatically blocked  
Fail2Ban successfully mitigated SSH brute-force attacks by detecting failed login patterns and banning the attacker. This demonstrates an effective defense mechanism against automated intrusion attempts.

**Attacker IP:**  


**Victim IP:**  
A screenshot of a computer

AI-generated content may be incorrect.

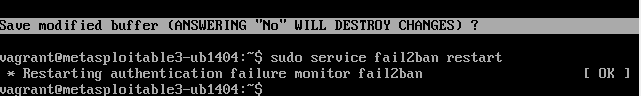
**Pinging the victim’s machine:**  
  
  
**Before the attack:**  
  
  
  
  
  
**Install Fail2Ban on Metasploitable3**  
(sudo apt-get update)  
(sudo apt-get install fail2ban)

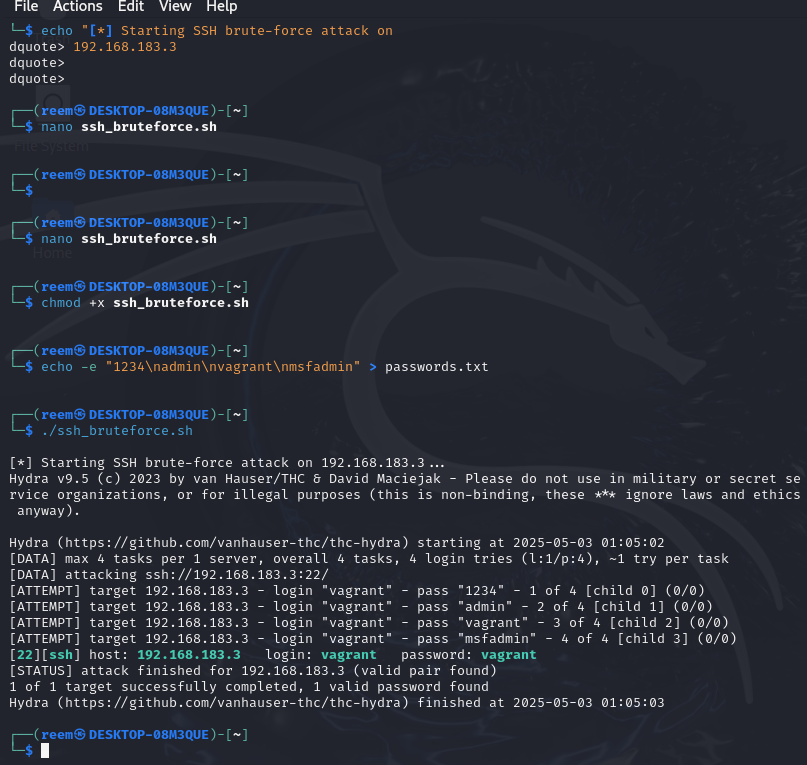
**Configure Fail2Ban for SSH**  
(sudo nano /etc/fail2ban/jail.d/ssh.con)



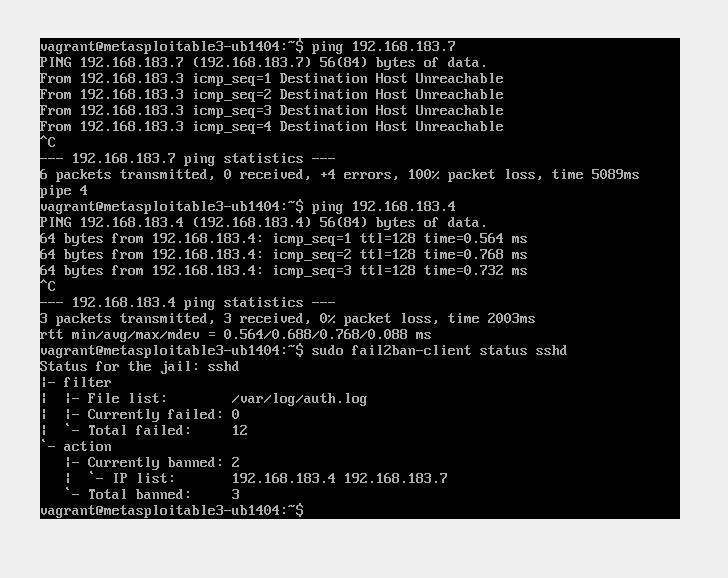
Then putting this and put the maxretry as 3that means block after 3 failed login attempts

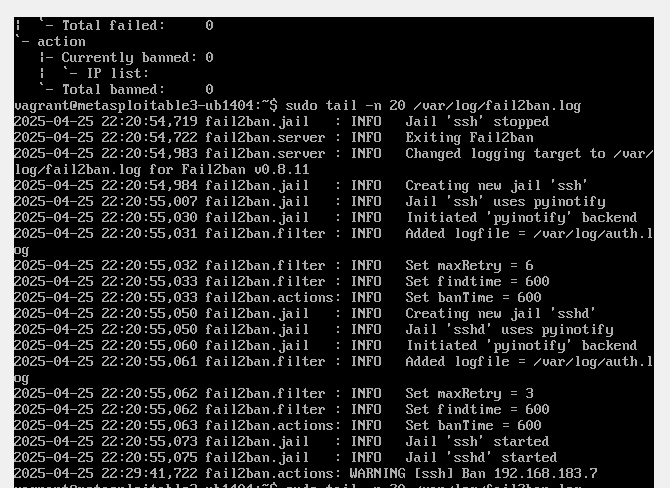


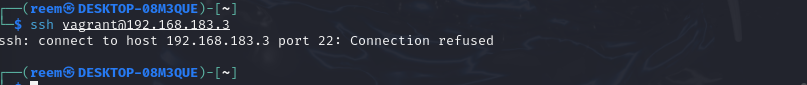
**Restart Fail2Ban Service**  
(sudo service fail2ban restart)  


**Rerun Hydra Attack from Kali:**

hydra -l root -P pass.txt ssh://192.168.183.3 -t 4

**Check if IP Got Banned on Metasploitable3**  
(sudo fail2ban-client status sshd)  
to make sure it is banned:( sudo tail /var/log/fail2ban.log)  
and IP (Ban 192.168.183.7) was stated in the result, so it is verified  




After applying the Defense successfully, we tested the defense by simulating a brute-force attack on the attacker machine, by running:   
(ssh vagrant@192.168.183.3)  
  
**After the defense:**  


**Fail2Ban service was successfully started and configured to monitor SSH login attempts**  
(fail2ban-client, tail -f /var/log/fail2ban.log)  
to confirm that the defense mechanism is actively running and logging as intended

