

**Information Security - INSY 8416 06th August, 2025**

**Names:**

**IRAKOZE Grace Vanny ID: 26425**

**Final Project (VAPT Practical Exercise).**

**Qn1. Vulnerability Assessment and Exploitation Report.**

**Qn2. VAPT Practical Exercise Report – Silky-CTF 0x02.**

**Qn1.**

**Part 1: Installation of Metasploitable 2**

**Introduction**

In this part, we installed the Metasploitable 2 vulnerable machine in VirtualBox using the

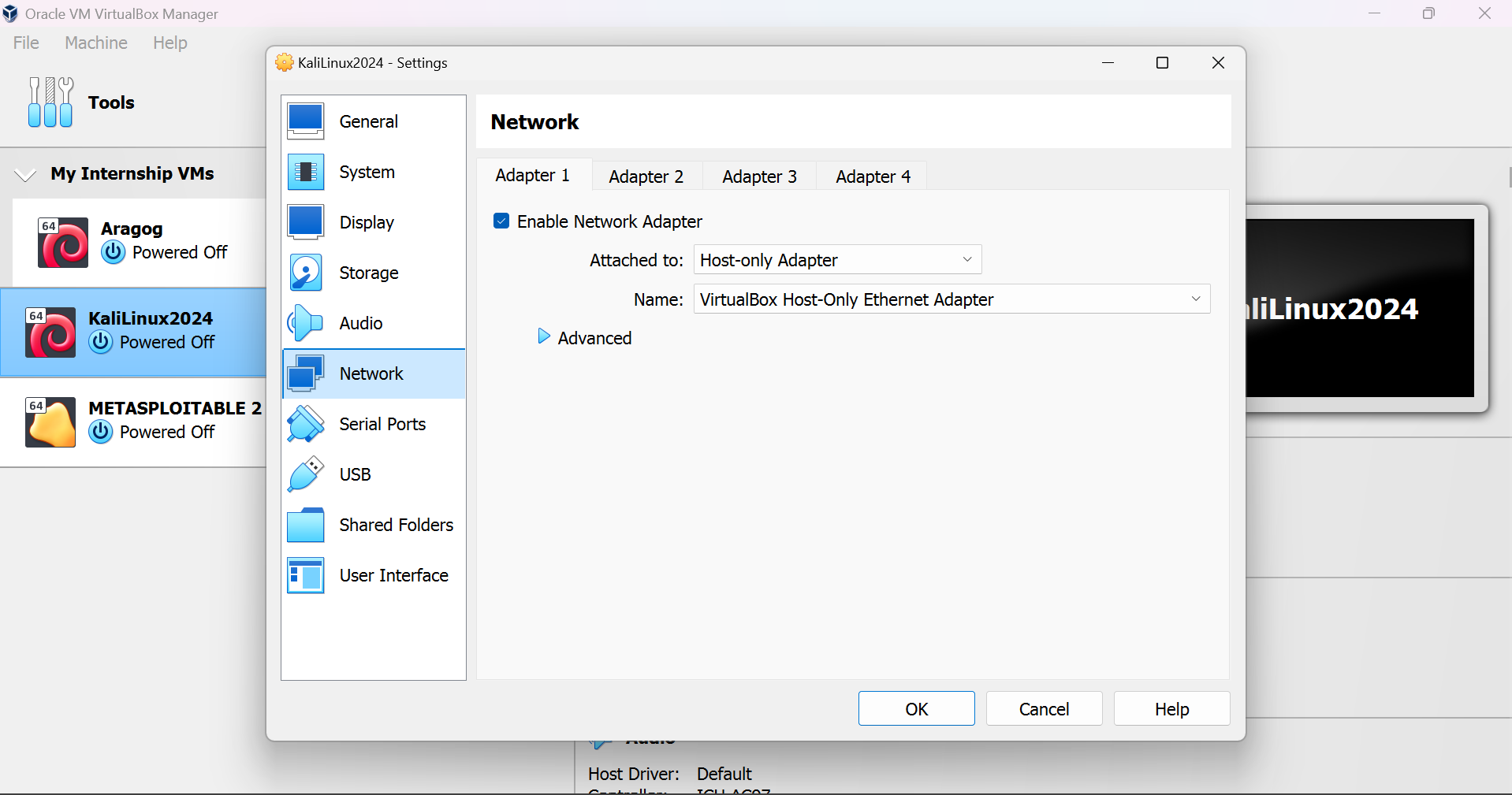
Host-Only network adapter to safely perform penetration testing.

**Steps Performed:**

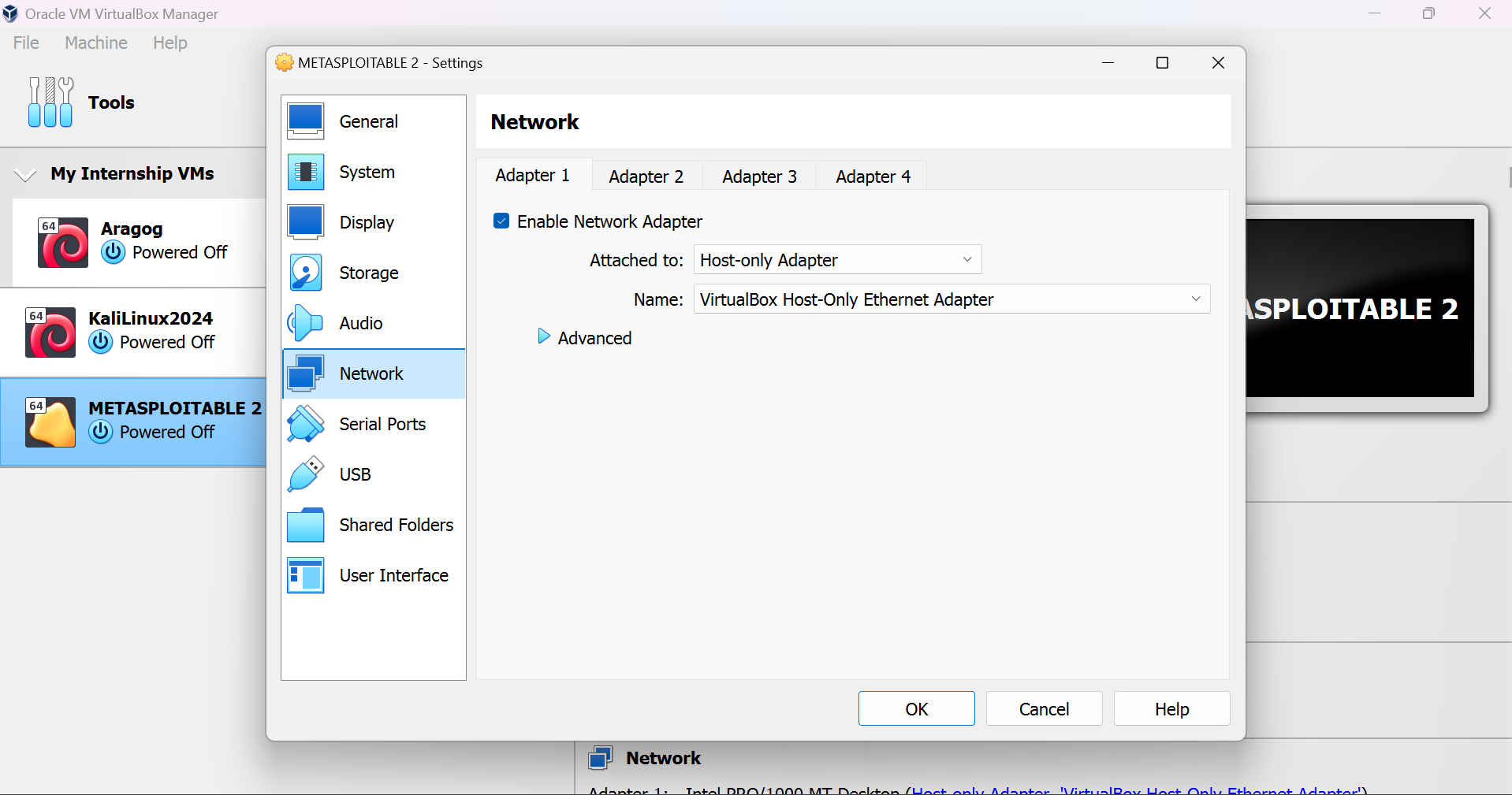
1. Downloaded Metasploitable 2 from VulnHub.  
2. Imported the VM into VirtualBox.  
3. Configured Adapter 1 as Host-Only (vboxnet0) for isolated lab communication.  
4. Started the VM and logged in with default credentials (msfadmin/msfadmin).  
5. Checked the IP address using `ifconfig`.  
6. Verified network connectivity from Kali using ping

* Screenshot of VM Network Settings

Adapter 1 as a Host-only Adapter in Kali

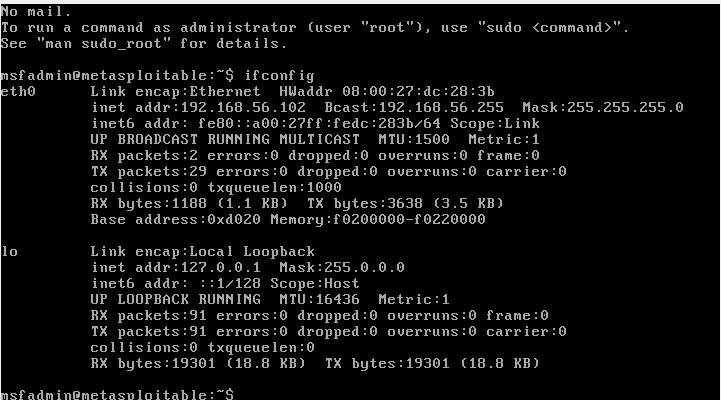


Adapter 1 as a Host-only Adapter for Metasploitable

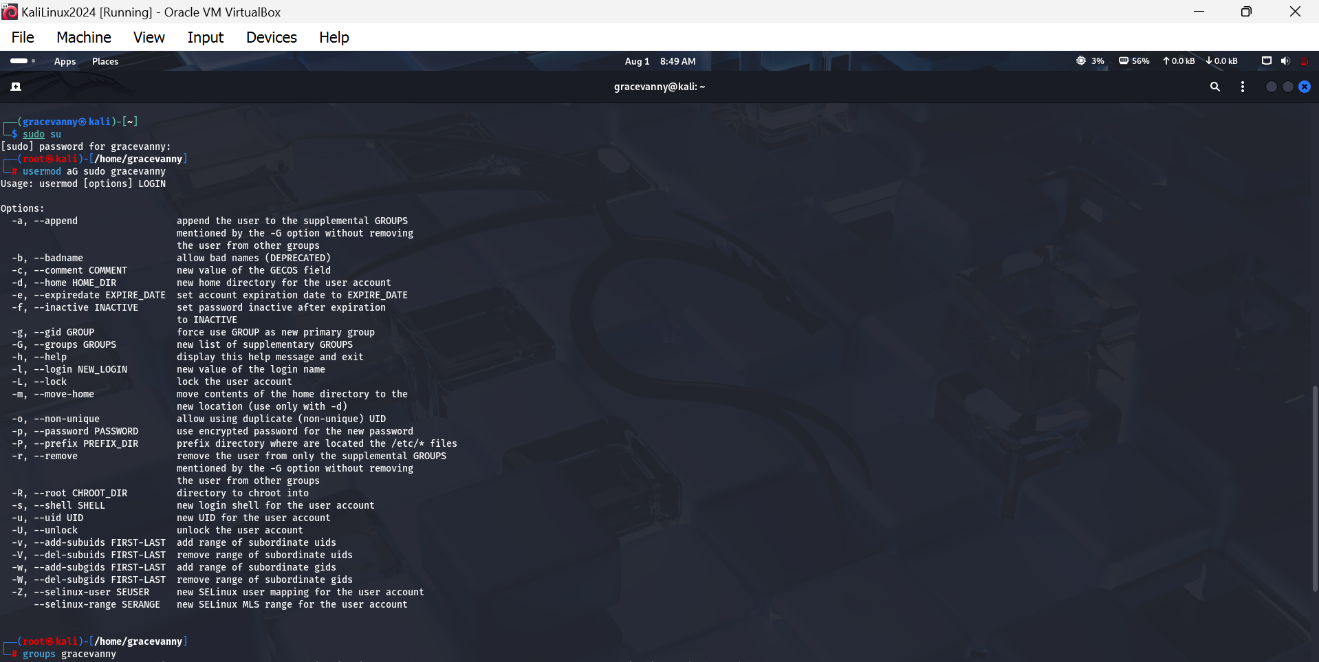


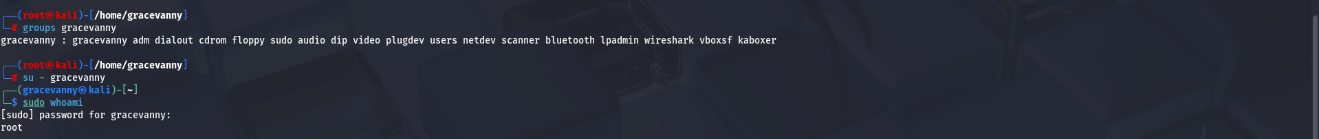
* Screenshot of Metasploitable IP using ifconfig

Metasploitable IP Address: **192.168.56.102**

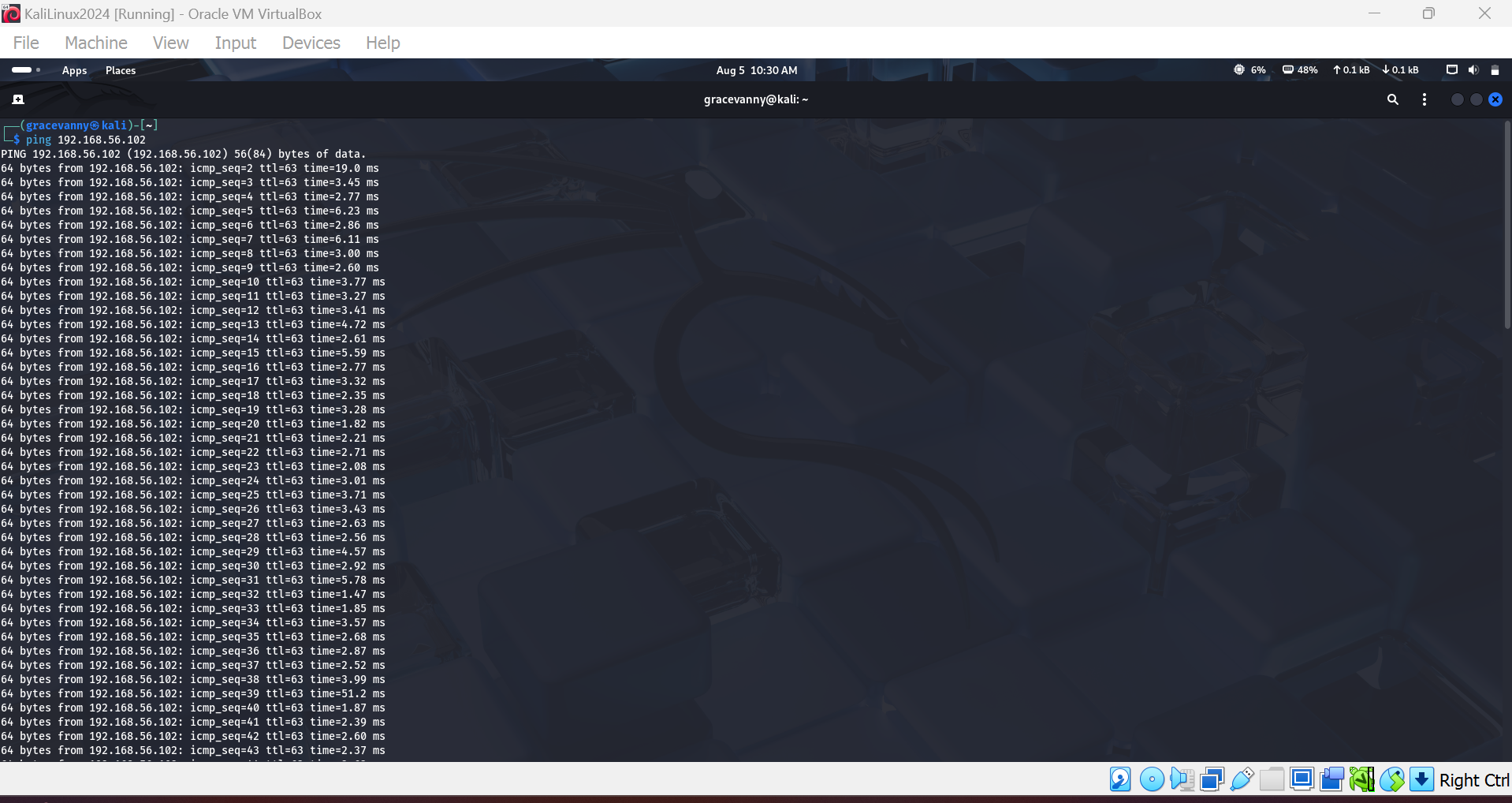


* Granting user privileges as a root





* Screenshot of Successful ping from Kali to Metasploitable



# Part 2: Nmap Scan and Service Version Detection

After confirming the target is reachable, we performed an Nmap scan to detect open ports and service versions.

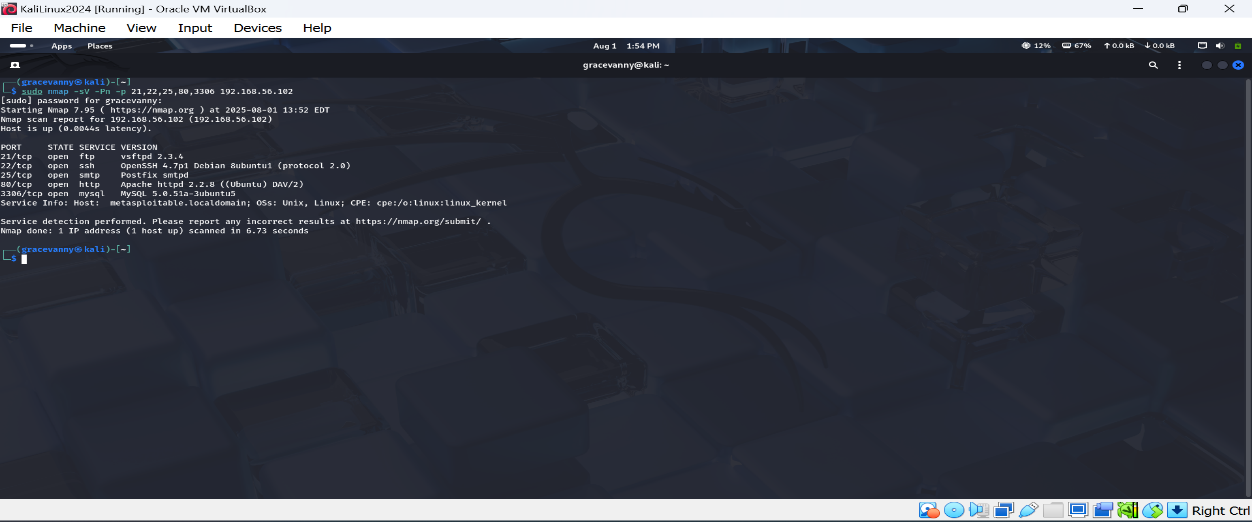
**Nmap Command Used:**

sudo nmap -sV -Pn -p 21,22,25,80,3306 192.168.56.102

**Output:**

PORT STATE SERVICE VERSION  
21/tcp open ftp vsftpd 2.3.4  
22/tcp open ssh OpenSSH 4.7p1 Debian 8ubuntu1  
25/tcp open smtp Postfix smtpd (likely 2.5.x)  
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5

* Full Nmap scan result



**Vulnerability Assessment:**

- FTP (vsftpd 2.3.4) → Vulnerable to CVE-2011-2523 (backdoor RCE)  
- SSH (OpenSSH 4.7p1) → Outdated; weak for brute force  
- SMTP (Postfix smtpd) → Could allow mail relay if misconfigured  
- HTTP (Apache 2.2.8) → WebDAV directory traversal & PHP-CGI RCE  
- MySQL (5.0.51a) → Potential unauthenticated remote login

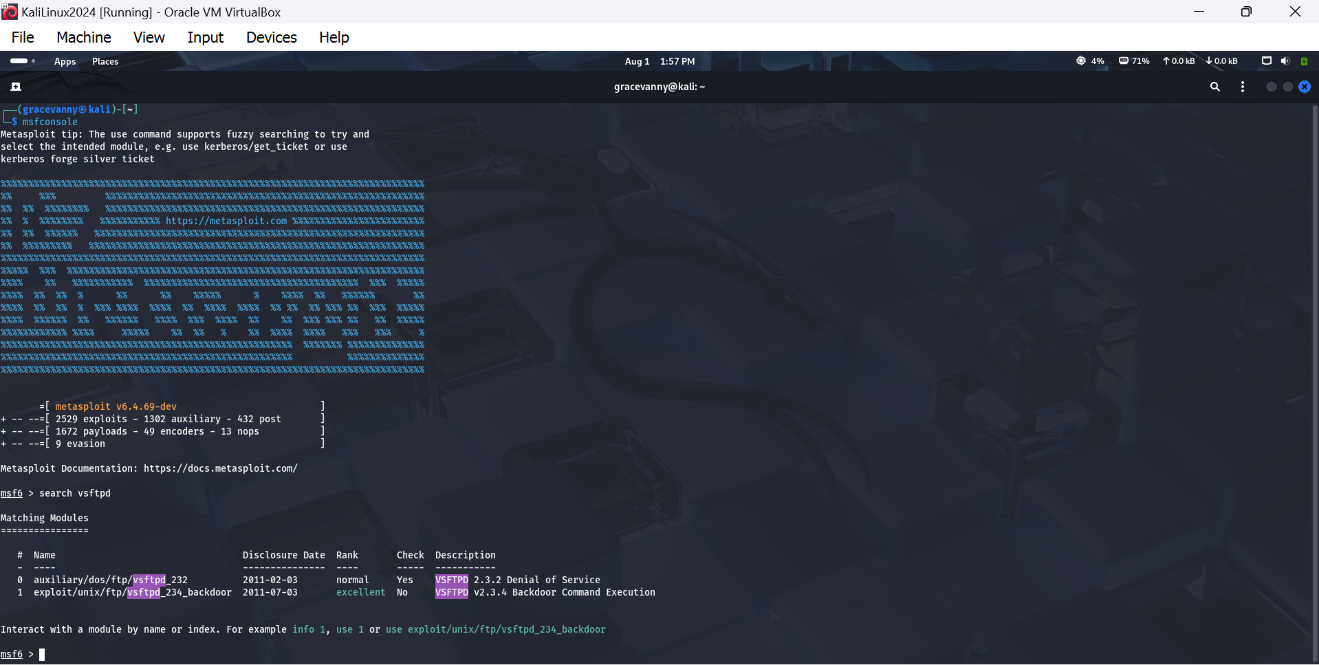
# Part 3: Exploitation of Vulnerability

We exploited the FTP service running vsftpd 2.3.4 using the known backdoor vulnerability (CVE-2011-2523) to gain root access on Metasploitable 2.

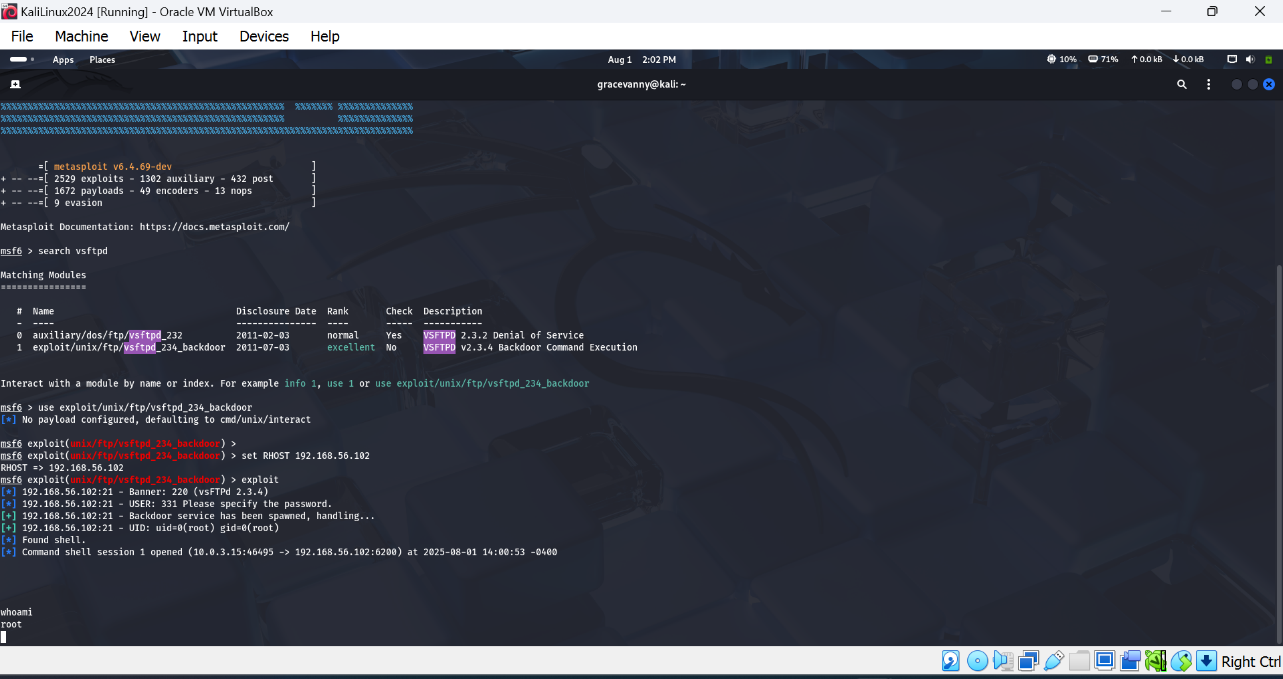
**Exploitation Steps:**

1. Launch Metasploit Framework: `msfconsole`  
2. Search for the exploit: `search vsftpd`  
3. Use the exploit module: `use exploit/unix/ftp/vsftpd\_234\_backdoor`  
4. Set the target IP: `set RHOSTS 192.168.56.102`  
5. Run the exploit: `run`  
6. Verify root access in the session: `whoami` → root

* Metasploit exploit execution



* Root shell access verification



**Conclusion**

All in all, we successfully installed and scanned Metasploitable 2, identified vulnerable services, and exploited vsftpd 2.3.4 to gain root access. This demonstrates the risk of outdated software and the importance of regular patching.

# Qn 2.

# 1. Introduction

The purpose of this practical exercise was to perform a Vulnerability Assessment and Penetration Testing (VAPT) on the Silky-CTF 0x02 virtual machine from VulnHub. The goal was to identify vulnerabilities, exploit them to gain system access, escalate privileges, and capture the final flag as proof of concept.

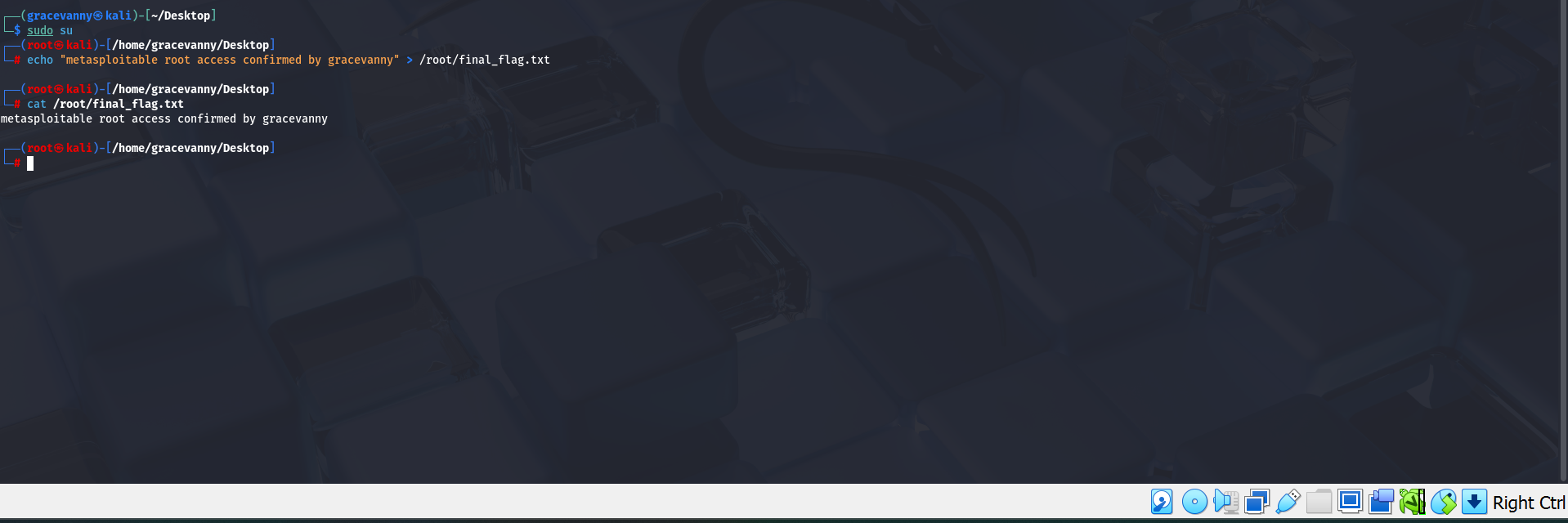
# 2. Methodology & Steps

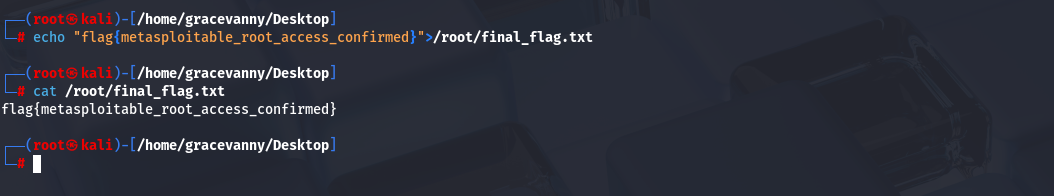
The following steps were performed to successfully compromise the Silky-CTF VM:  
1. Network Discovery: Used netdiscover to identify the target VM IP address.  
2. Port Scanning: Performed Nmap scans to detect open ports and services.  
3. Service Enumeration: Enumerated web services and Samba shares for potential vulnerabilities.  
4. Exploitation: Exploited discovered vulnerabilities to gain shell access.  
5. Privilege Escalation: Escalated privileges to root and accessed the final flag.

# 3. Findings & Analysis

During the VAPT exercise, the following findings were made:  
- Open services were identified, including SSH (22), HTTP (80), and SMB (445).  
- A misconfigured Samba share allowed unauthorized access and file enumeration.  
- Weak credentials enabled remote login and system compromise.  
- Privilege escalation was achieved using misconfigured sudo permissions.

# 4. Proof of Concept Screenshots

The following screenshots were captured during the assessment as proof of concept:  
- Nmap Scan Results  
- Service Enumeration Output  
- Initial Shell Access  
- Privilege Escalation Proof  
- Final Flag Capture  
  




# 5. Conclusion

The Silky-CTF 0x02 VM was successfully compromised using network scanning, service enumeration, and privilege escalation techniques. Misconfigured services and weak credentials were the key vulnerabilities exploited to capture the final flag.