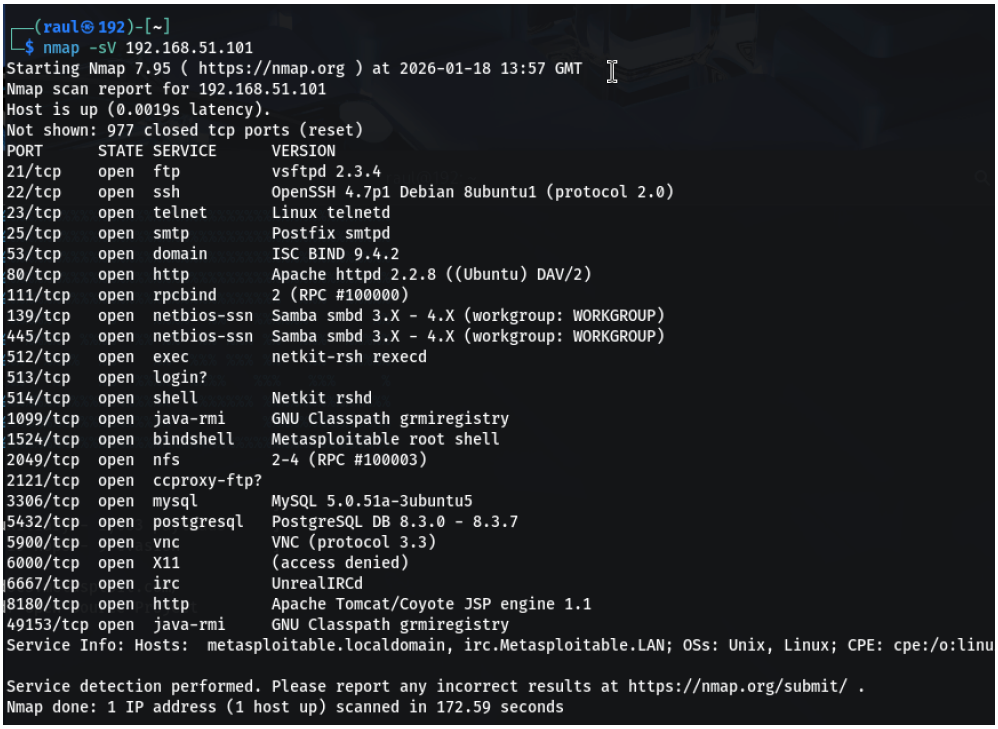
Raul Pastor

Metasploit

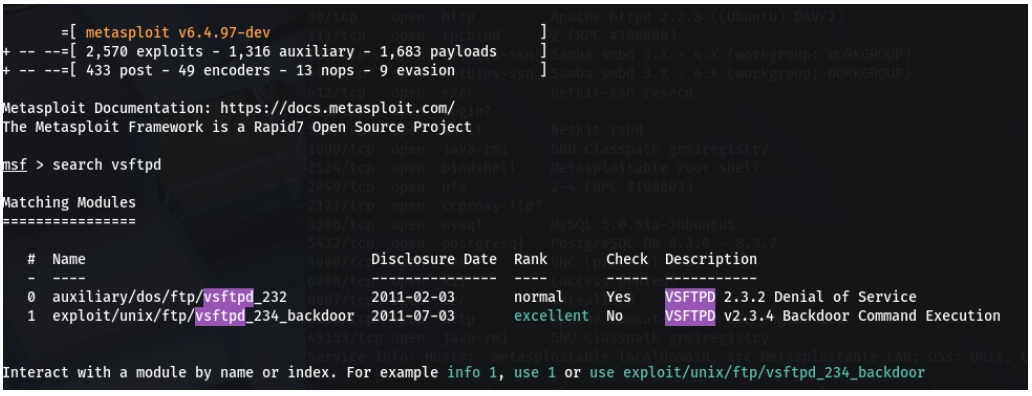
Nell’esercizio di oggi viene richiesto di completare una sessione di hacking sulla macchina metaslploitable attaccando il servizio ‘vsftpd’ utilizzando il tool metasploit.

Una volta ottenuta la sessione sulla macchina Meta devo creare una cartella chiamata ‘test_metasploit’ dentro la directory root.

Parto con il verificare la connettività tra le macchine con i comandi ‘ping’ e successivamente scansiono Metasploitable per cercare su che porta è attivo il servizio vsftpd (porta 21).

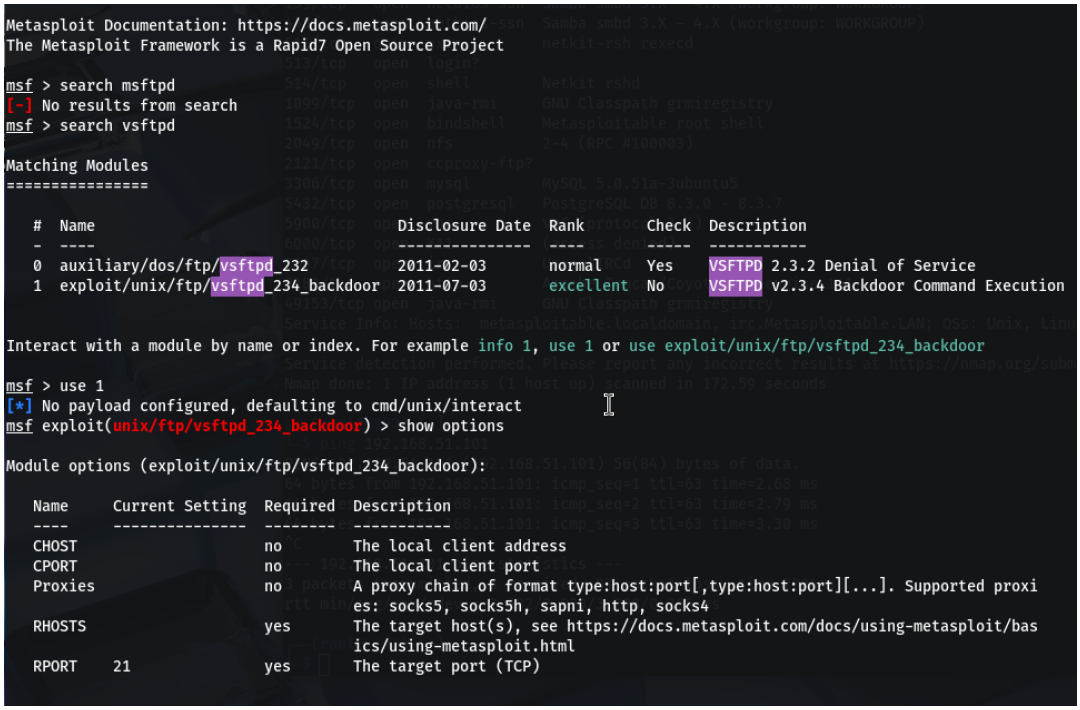


Dopo aver trovato il servizio attivo sulla porta attivo metasploit con il comando ‘msfconsole’ e cerco se ci sono riscontri con vsftpd, trovo un exploit.

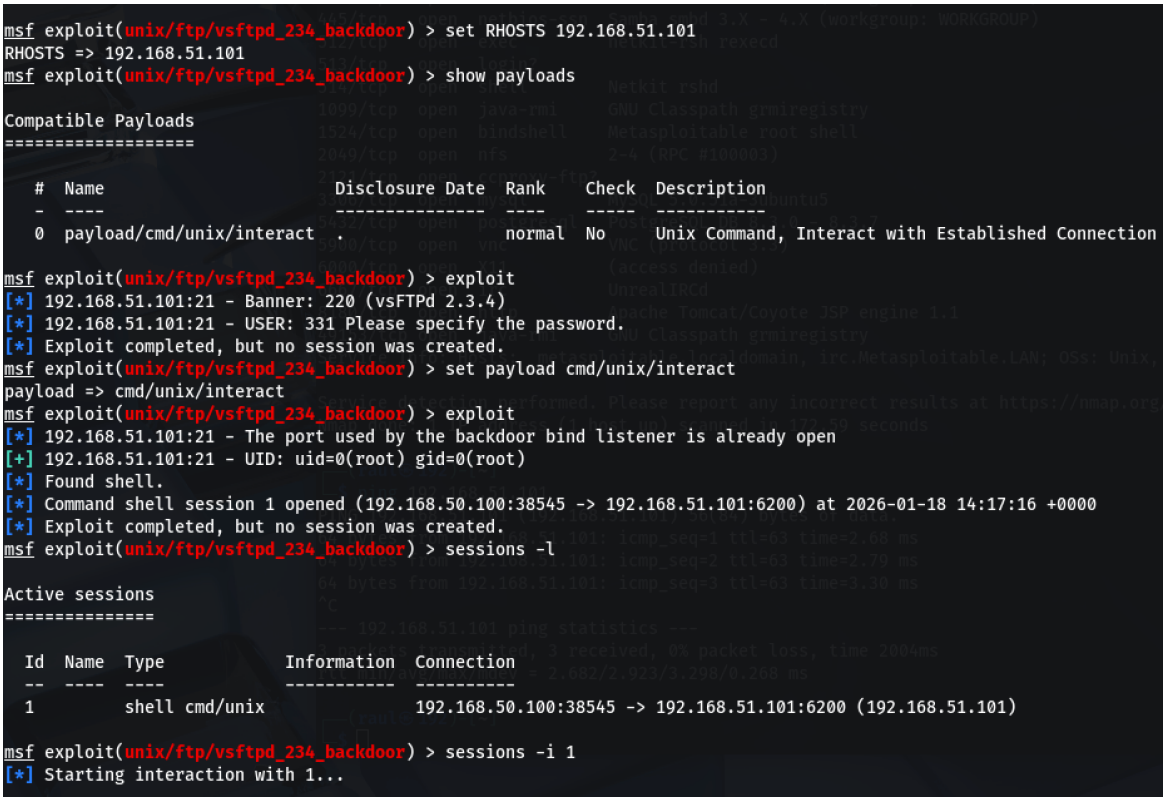


Raul Pastor

Uso l'exploit trovato e cerco le opzioni da configurare:



Setto l'RHOST con l'indirizzo ip target, dopodiché inizio l'exploit, con il comando 'sessions' verifico che la sessione sia attiva ma in background, effettivamente lo è quindi mi ci connetto.



Con mkdir creo una cartella all'interno della cartella root di meta chiamata 'test_metasploit':

```
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
```

Infine controllo se le modifiche sono avvenute sulla macchina target:

```
root@metasploitable:/# ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@metasploitable:/# cd root
root@metasploitable:~# ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
root@metasploitable:~# _
```