**DevTCM walkthrough**

# **Index**

[Index 1](#_Toc203410477)

[List of pictures 1](#_Toc203410478)

[Disclaimer 2](#_Toc203410479)

[Reconnaissance 2](#_Toc203410480)

[Initial foothold 3](#_Toc203410481)

[User flag 4](#_Toc203410482)

[Privilege escalation 6](#_Toc203410483)

[Personal comments 7](#_Toc203410484)

# **List of pictures**

[Figure 1 - nMap scan results (part 1) 2](#_Toc203410488)

[Figure 2 - nMap scan results (part 2) 2](#_Toc203410489)

[Figure 3 - Ffuf scan results 3](#_Toc203410490)

[Figure 4 - Configuration files found 3](#_Toc203410491)

[Figure 5 - DB credentials found 4](#_Toc203410492)

[Figure 6 - New path found on port 8080 4](#_Toc203410493)

[Figure 7 - Local File Inclusion exploited 5](#_Toc203410494)

[Figure 8 - Folder mounted via NFS service 5](#_Toc203410495)

[Figure 9 - Zip password cracked 6](#_Toc203410496)

[Figure 10 - Todo.txt file 6](#_Toc203410497)

[Figure 11 - Sudoers info 6](#_Toc203410498)

[Figure 12 - Root flag 7](#_Toc203410499)

# **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 are willing and curious to know and learn about Ethical Hacking, Security and Penetration Testing.

Just to say: I am not an English native person, so sorry if I did some grammatical and syntax mistakes.

# **Reconnaissance**

The results of an initial nMap scan are the following:

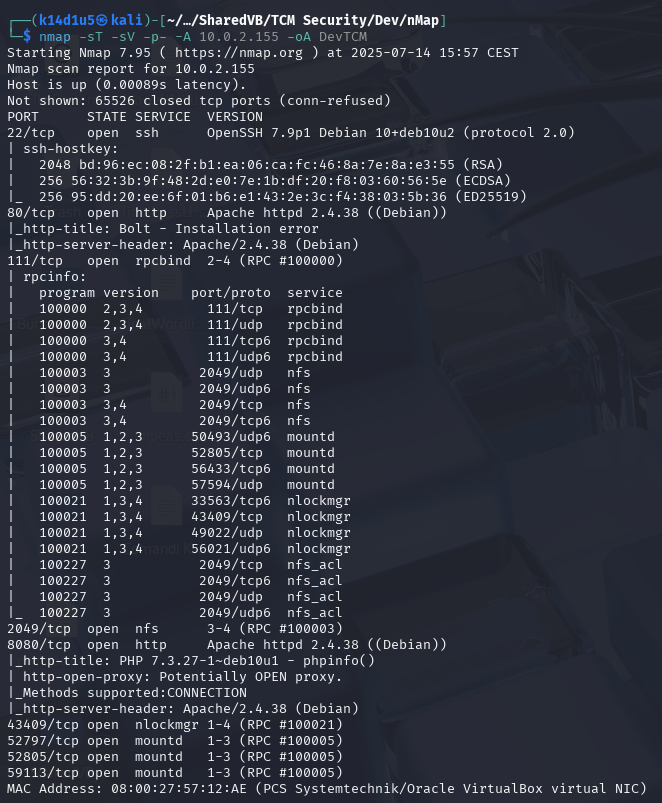


Figure 1 - nMap scan results (part 1)

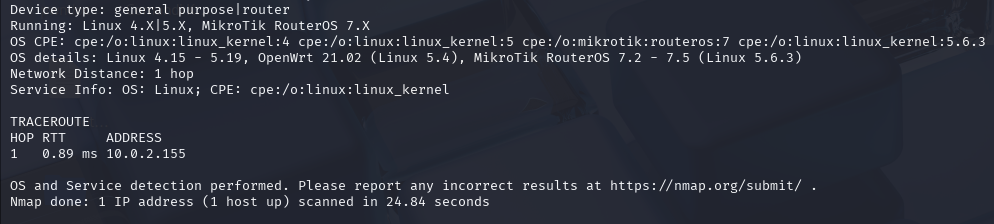


Figure 2 - nMap scan results (part 2)

Open ports are 22, 80, 111, 2049, 8080, 43409, 52797, 52805, 59113. Therefore, SSH (22) and RPC (111, 2049, 43409, 52797, 52805 and 59113) services are enabled. Also, two web application are running (80 and 8080). Lastly, nMap recognized Linux as operative system.

# **Initial foothold**

I started to analyze web application running on port 80. Using ffuf tool, I was able to find some paths:

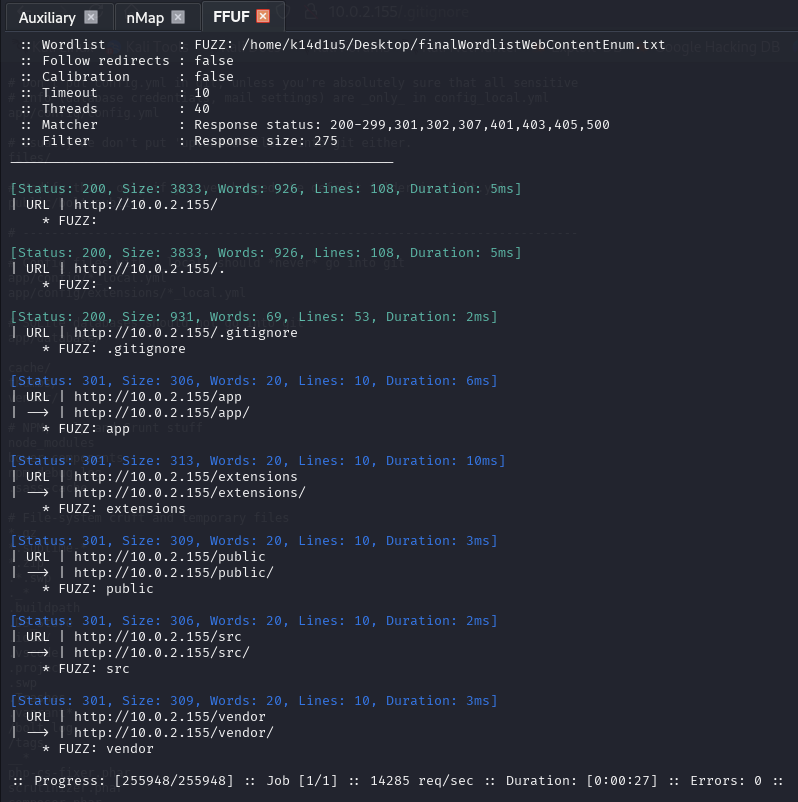


Figure 3 - Ffuf scan results

In particular, in the path, I found some interesting configuration files:

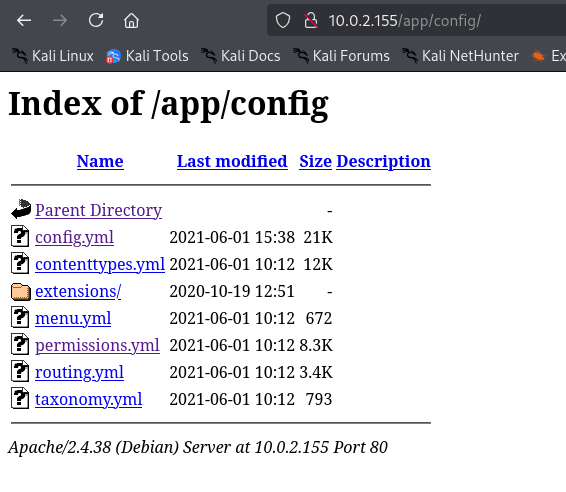


Figure 4 - Configuration files found

I investigated all of them and I was able to find DB credentials, as shown in the following:

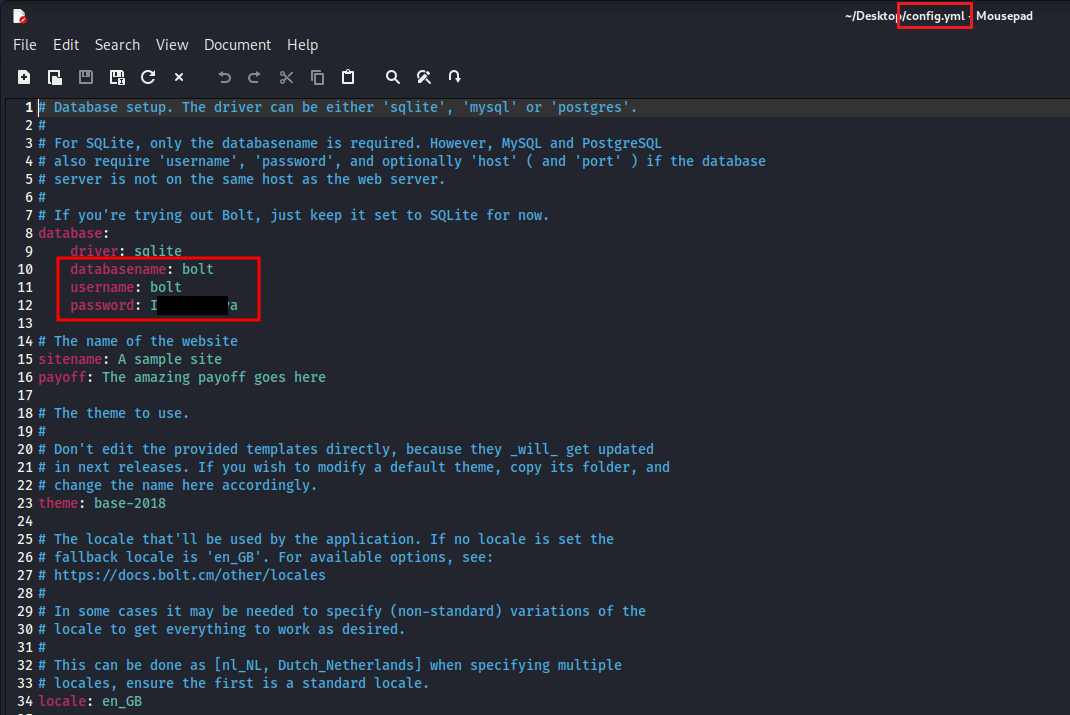


Figure 5 - DB credentials found

At this point, I started to analyze web application running on port 8080. On this one, I found the path of a web application working:

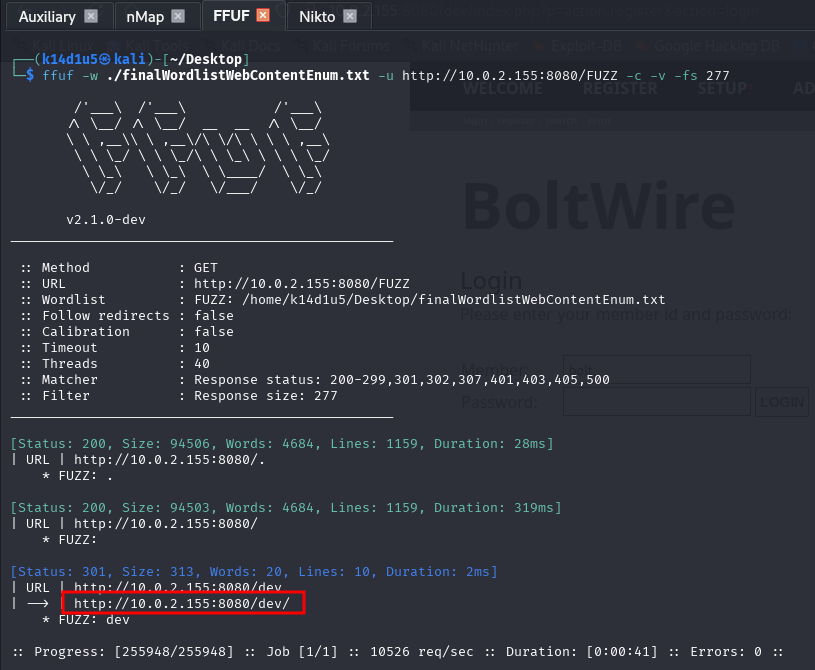


Figure 6 - New path found on port 8080

# **User flag**

I tried to login in the web application on port 8080 using the credentials I found, but this try was unsuccessful. Therefore, I decided to register a new account. After a little bit of analysis using Burp Suite tool and browsing the web application, I looked for a public exploit against the web application, that was called BoltWire. Luckily, I found an interesting exploit using searchsploit. This exploit was relative to a Local File Inclusion vulnerability. I tried it and luckily it worked. In particular, I was able to read the file, as shown in the following figure:

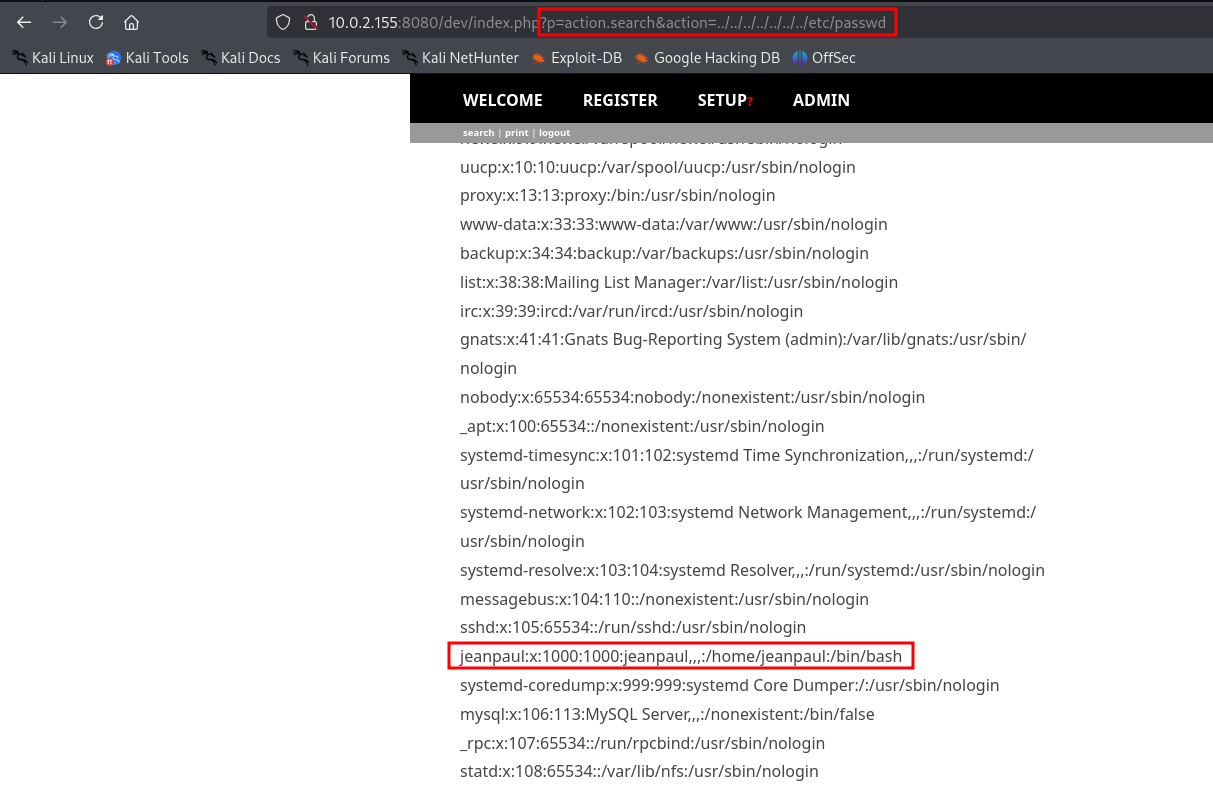


Figure 7 - Local File Inclusion exploited

In this way I was able to found out the user on the machine. Therefore, I tried to login via SSH service using this username and the password I previously found, but I was unsuccessful. Since I had no other idea about what I was able to do on the web application, I started to investigate the NFS service. Therefore, I found out I was able to mount a folder. I did it and I found a zip file in it:

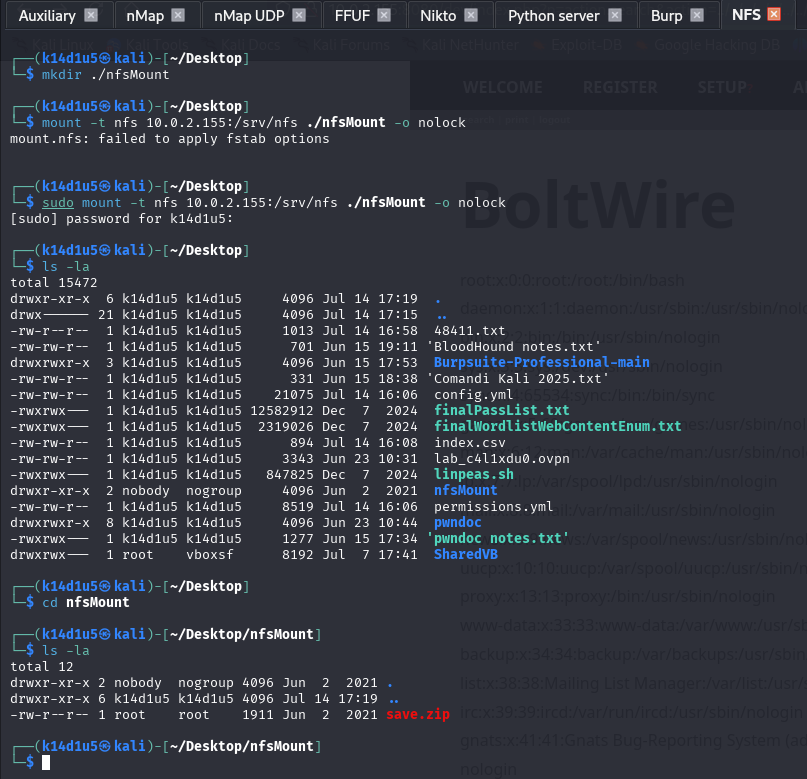


Figure 8 - Folder mounted via NFS service

I tired to open the zip file, but it was protected by password. Again, I tried to use the password I previously found, but it still didn’t work. Therefore, I tried to crack it using JohnTheRipper tool:

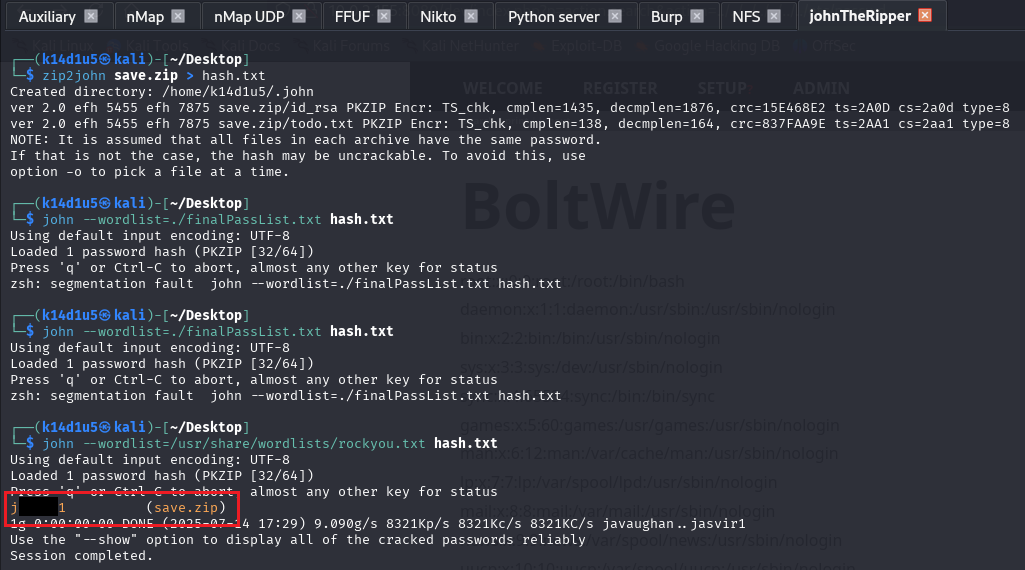


Figure 9 - Zip password cracked

Using this password, I was able to unzip the file. I found an RSA key and a todo.txt file. I tried to use the RSA key to login via SSH as user. However, the key required a password. Luckily, the first password I found, the one relative to the DB access, worked this time and I obtained a shell.

# **Privilege escalation**

At this point I opened the tod.txt file I just found in the archive:

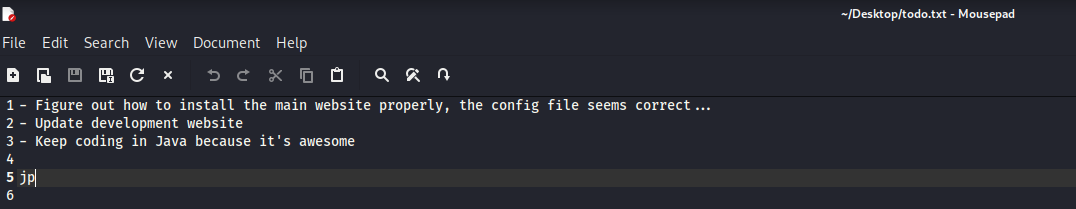


Figure 10 - Todo.txt file

It seemed that there was a website in developing phase. Since I didn’t find anything in the user home, I tried to investigate the web application folder. Sadly, I didn’t find anything useful there. Therefore, I started the basic checks to try to escalate my privileges. Luckily, the user was able to run the program as sudo:

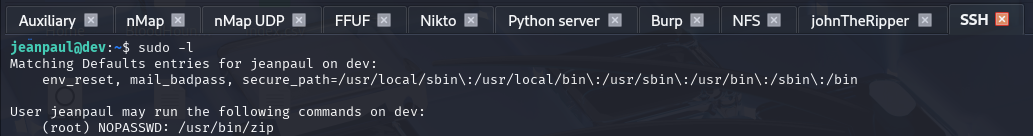


Figure 11 - Sudoers info

At this point I looked for an exploit path on GTFObins and I just followed instruction. In this way, I obtained the root shell and I read the flag:

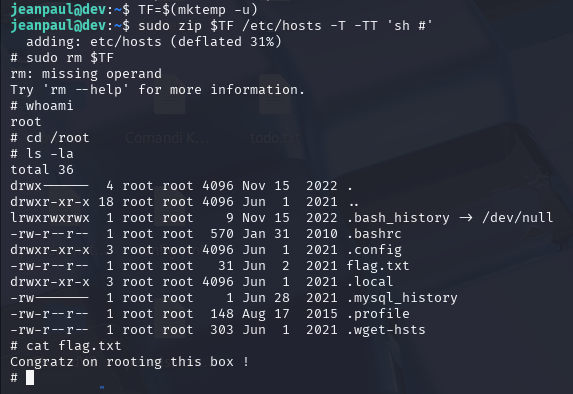


Figure 12 - Root flag

# **Personal comments**

This box was very nice and involved zip password cracking and Local File Inclusion vulnerability, two concept I didn’t find very often. Therefore, I consider it a funny and interesting box, it let you to keep in mind important topics. Overall, I evaluate this box as easy.