**OpenAdmin walkthrough**

# **Index**

[Index 1](#_Toc176604157)

[List of pictures 1](#_Toc176604158)

[Disclaimer 2](#_Toc176604159)

[Reconnaissance 2](#_Toc176604160)

[Initial foothold 2](#_Toc176604161)

[User flag 3](#_Toc176604162)

[Privilege escalation 9](#_Toc176604163)

[Personal comments 9](#_Toc176604164)

[References 10](#_Toc176604165)

# **List of pictures**

[Figure 1 - nMap scan results 2](#_Toc176604139)

[Figure 2 - ffuf scan results 2](#_Toc176604140)

[Figure 3 - Administrative login page found 3](#_Toc176604141)

[Figure 4 - ONA exploit 3](#_Toc176604142)

[Figure 5 - User list on target 4](#_Toc176604143)

[Figure 6 - Password found 4](#_Toc176604144)

[Figure 7 - SSH login as Jimmy 5](#_Toc176604145)

[Figure 8 - Virtual host found 5](#_Toc176604146)

[Figure 9 - Credentials found 5](#_Toc176604147)

[Figure 10 - Password cracked 6](#_Toc176604148)

[Figure 11 - Chisel on my Kali attacker machine 6](#_Toc176604149)

[Figure 12 - Chisel on target machine 6](#_Toc176604150)

[Figure 13 - Internal domain home page 7](#_Toc176604151)

[Figure 14 - RSA key 7](#_Toc176604152)

[Figure 15 - Johanna RSA key cracked 8](#_Toc176604153)

[Figure 16 - Log in as Johanna ad user flag 8](#_Toc176604154)

[Figure 17 - Info to escalate privileges 9](#_Toc176604155)

[Figure 18 - Privilege escalation and root flag 9](#_Toc176604156)

# **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.

Just as note: 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:

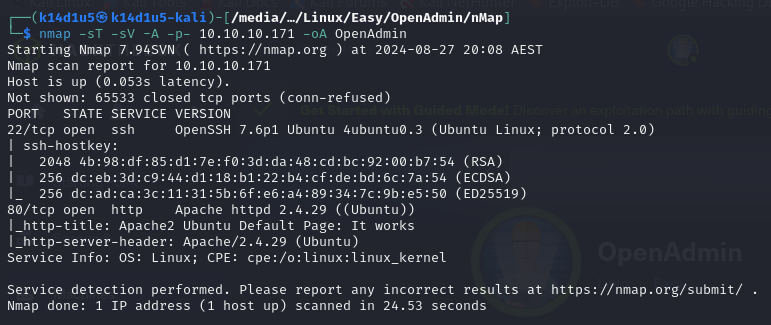


Figure 1 - nMap scan results

Open ports are 22 and 80. So, this box has SSH service (port 22) enabled and a web application running on port 80. Also, nMap provided me Linux as OS identified. However, nMap didn’t provide me further information about the OS.

# **Initial foothold**

Exploring the published web sites, it looks like has nothing to do on it. So, I searched some “hidden” content using **ffuf** tool. In this way, as you can see in the following picture, I found some interesting new web pages:

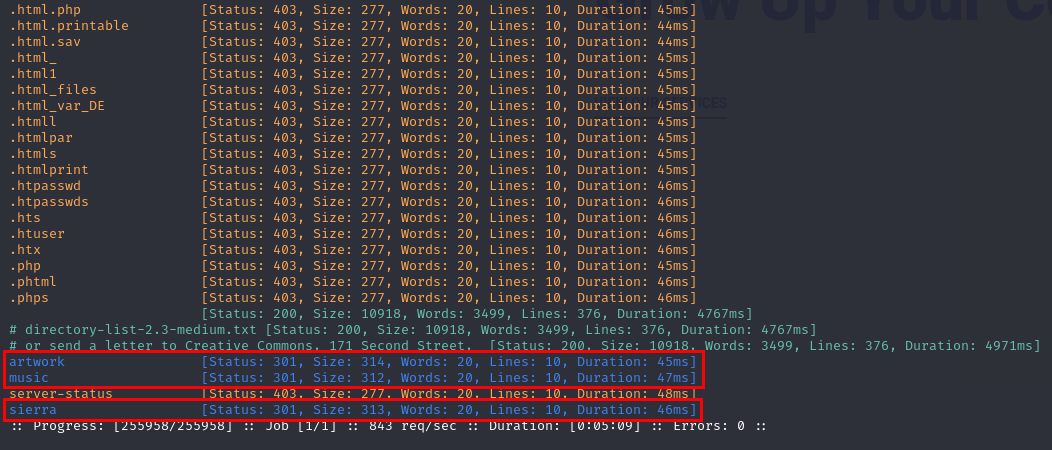


Figure 2 - ffuf scan results

The command I used was the following:

The new web paths I found was **/artwork**, **/music** and **/sierra**. I diligently analyzed these new pages and I noted that the Login button on the **/music** path home page is linked to a new login page at the link , as you can see in the following picture:

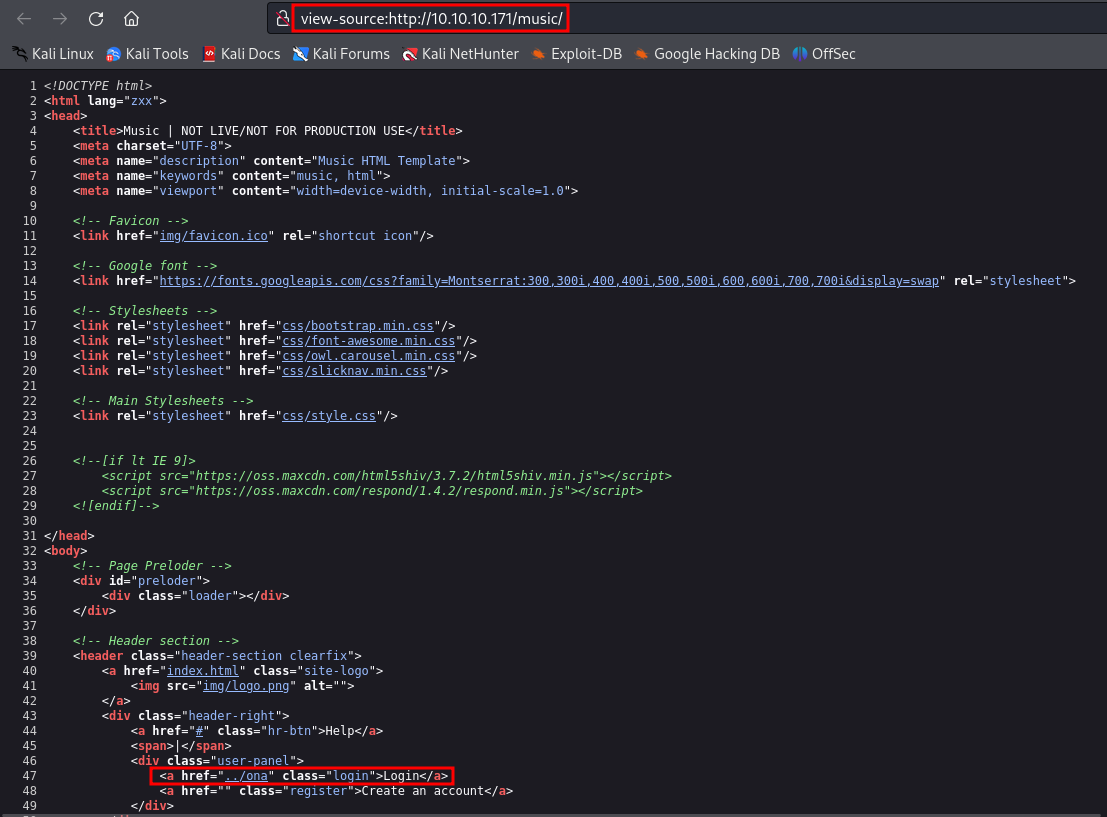


Figure 3 - Administrative login page found

# **User flag**

At this point I searched on the Internet some interesting information and plausible exploit about ONA. Luckly, I found an interesting exploit to provide RCE. So, I downloaded and run it:

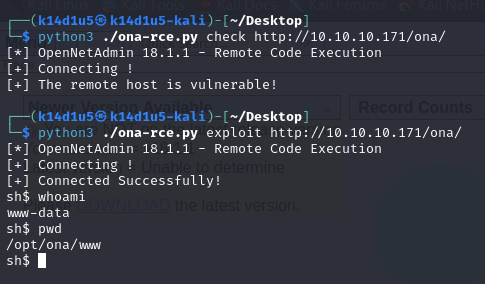


Figure 4 - ONA exploit

I this way, I obtained a shell on the target. However, I opened a new shell uploading a msfvenom payload, opened a new listener and running the payload. I created the new payload running the following command:

Looking for some interesting information on the target machine, I found which users are on the target:

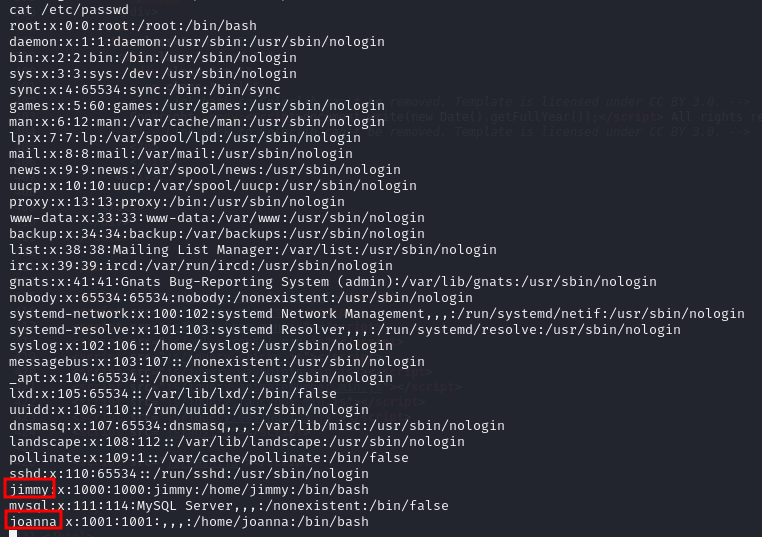


Figure 5 - User list on target

after a long search, I found an interesting password, as shown in the following picture:

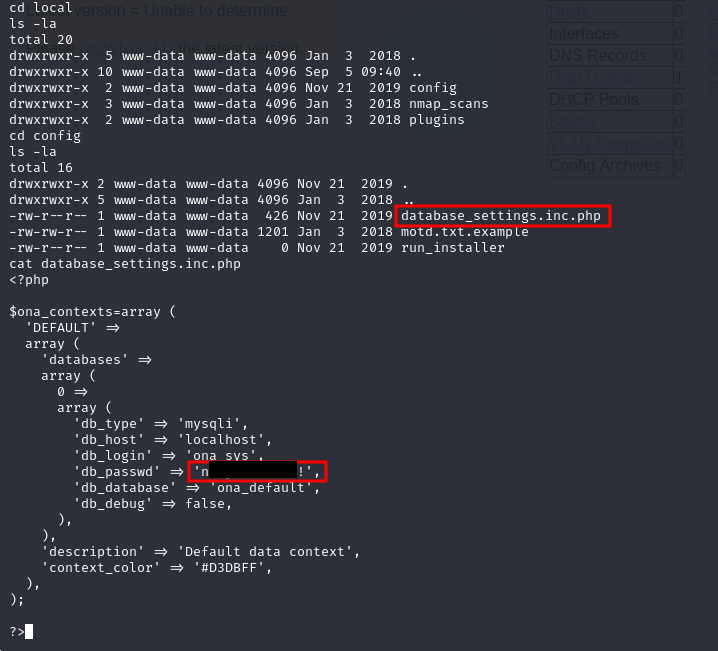


Figure 6 - Password found

Since I found this (and another password actually), I tried it to log I as jimmy:

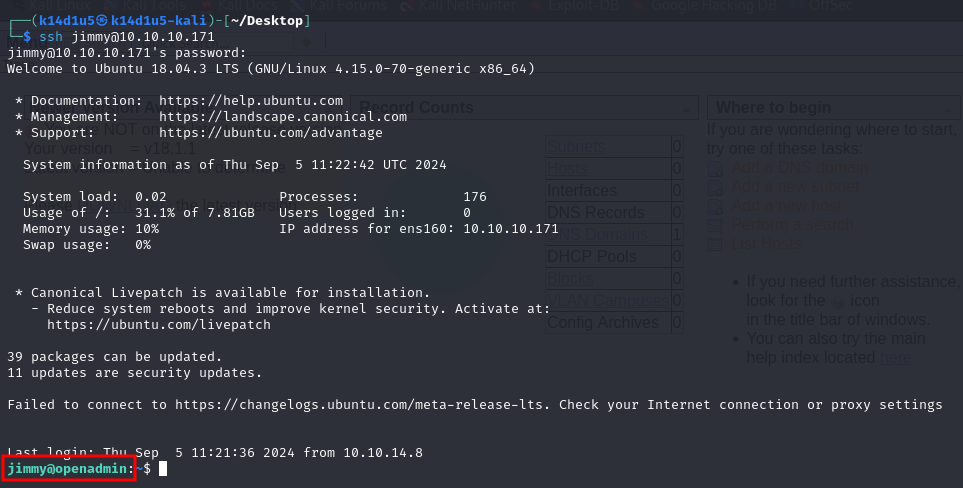


Figure 7 - SSH login as Jimmy

Finally, I am a user o the target. However, jimmy user has not the user flag. This can only mean I have to became Joanna. So, I started again to search other interesting information. In particular, observing the active processes, I found one running on the loopback on port 52846. So, I looked for some other information about it, and I found out that it is a virtual host:

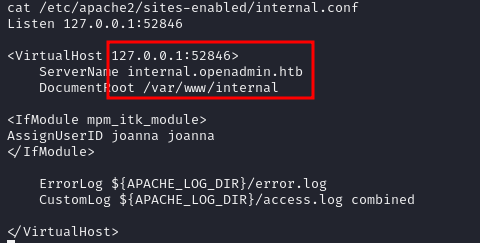


Figure 8 - Virtual host found

At this point, I looked for his home directory, where I found a credentials in his **index.php** file:

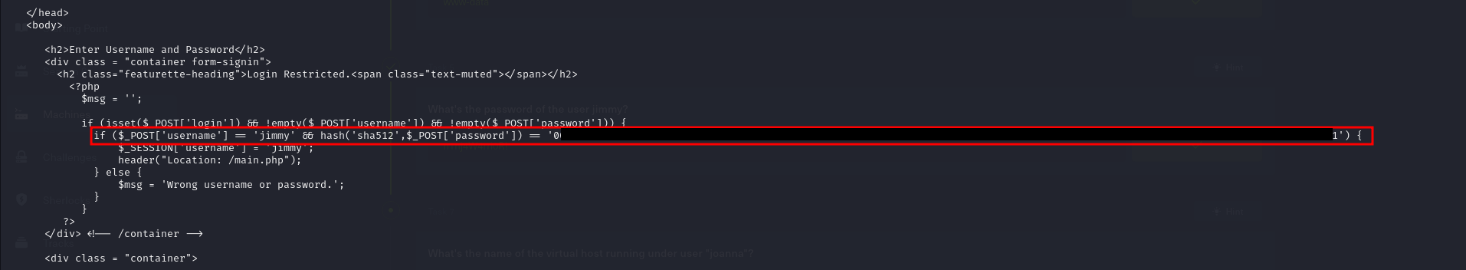


Figure 9 - Credentials found

At this point I tried to crack it. I tried with success to do it using crack station web site:

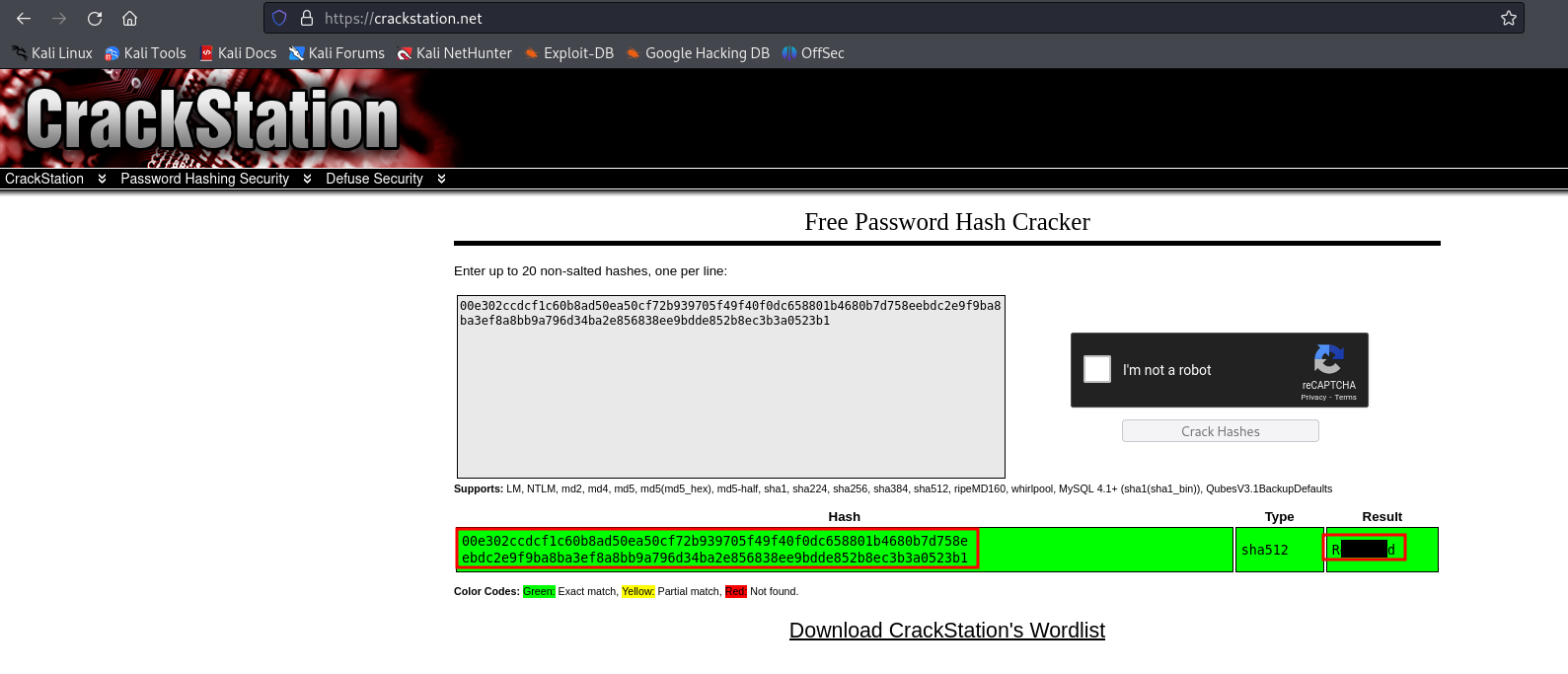


Figure 10 - Password cracked

It looked like as I found credentials to log in the internal domain. So, I need a port forwarding to reach it. To implement the port forwarding, I used Chisel. I download the ARM version to run it on the victim machine (I obviously uploaded it on the target) and the Intel version (correct one for me) to run it on my Kali machine. So, on my Kali machine I run Chisel using the command

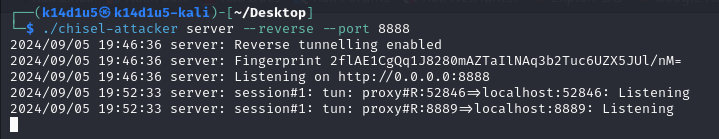


Figure 11 - Chisel on my Kali attacker machine

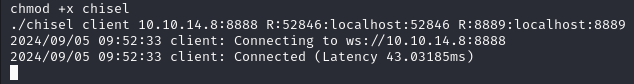


Figure 12 - Chisel on target machine

At this point I can access to the internal domain simply using a browser on my Kali machine and browse to page:

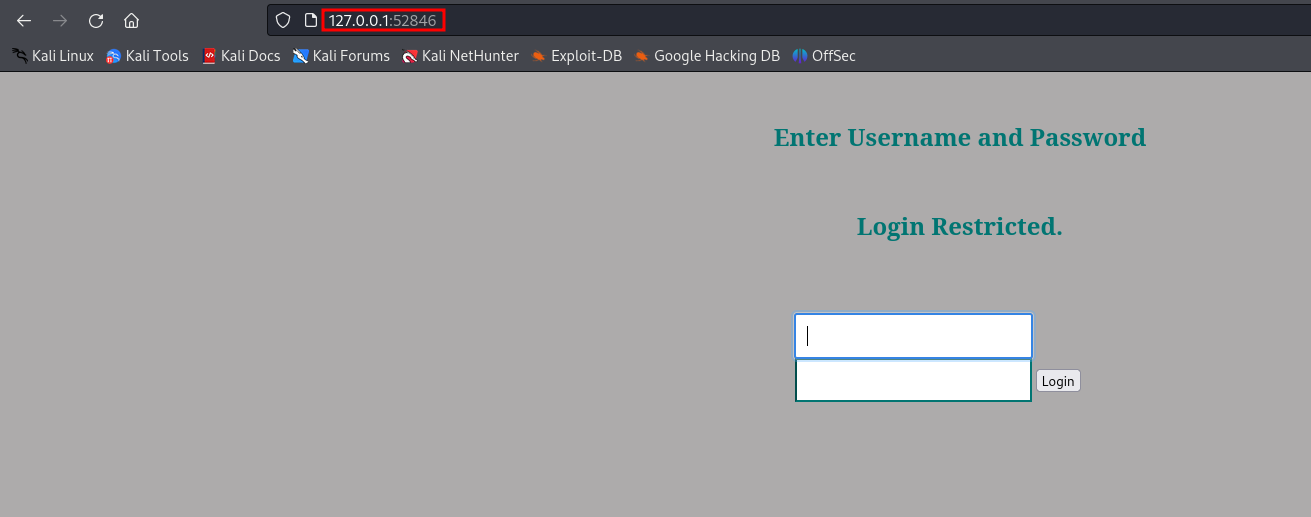


Figure 13 - Internal domain home page

Once I logged in using the credentials I found, I was very surprised that it provided me an RSA key, as shown:

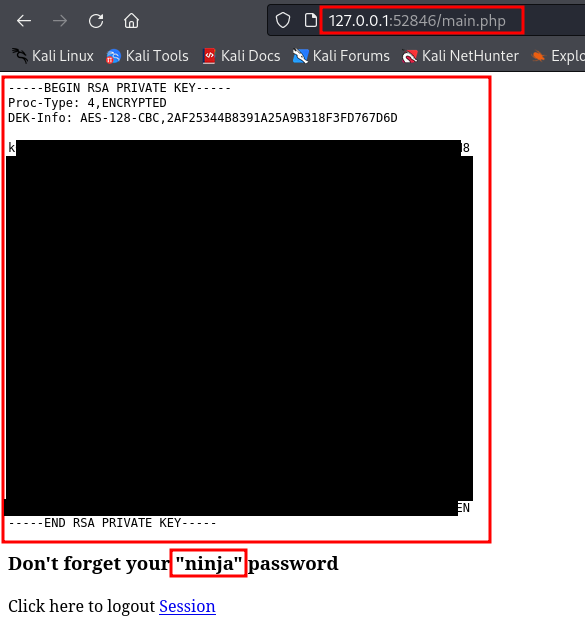


Figure 14 - RSA key

Analyzing the main page from the shell, I found that this RSA key is related to Joanna user. Also, this page informed me that a password is needed. So, I copied the RSA key in a TXT file, I created a JohnTheRipper compatible file and I tried to crack it using JohnTheRipper:

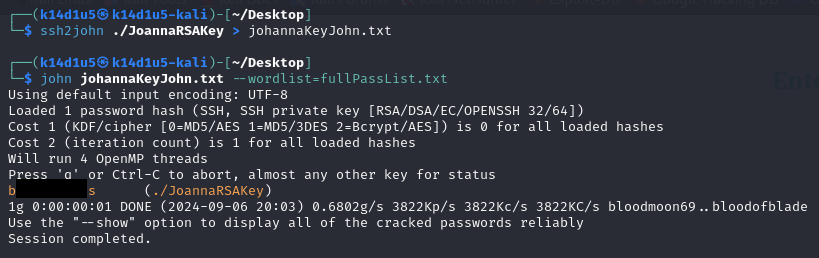


Figure 15 - Johanna RSA key cracked

Finally, I have Johanna credentials and I can log in via SSH as her and retrieve the user flag:

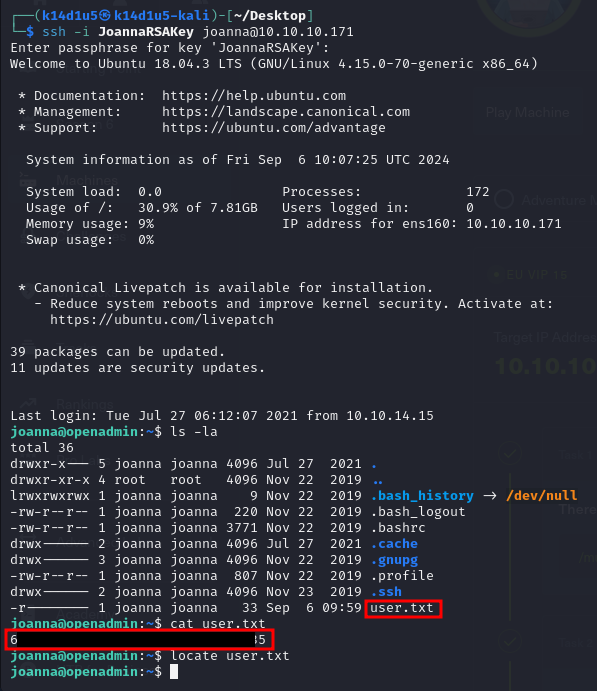


Figure 16 - Log in as Johanna ad user flag

# **Privilege escalation**

Once I obtained the user flag, I needed to escalate my privileges. Luckly, it was a very easy task. In fact, I found that Johanna was able to read a specific file using **nano** tool as user:

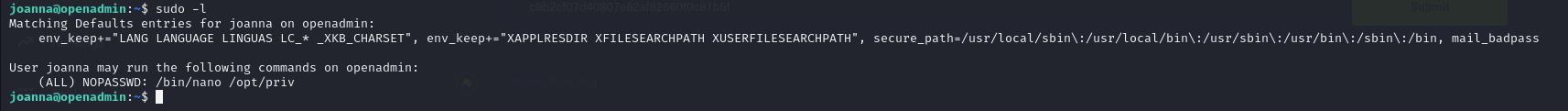


Figure 17 - Info to escalate privileges

So, all I needed to do was read this file and using the **nano** tool to open a shell and retrieve the root flag:

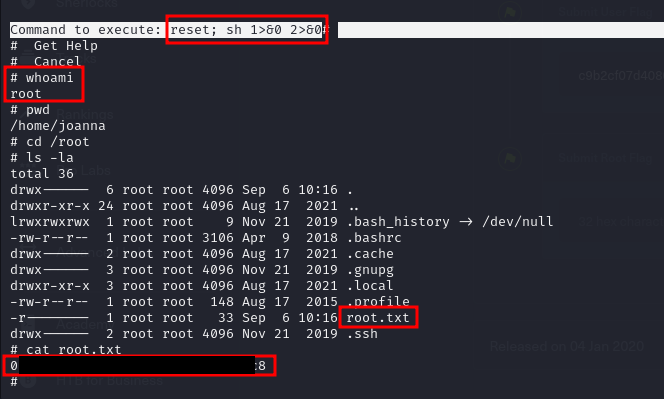


Figure 18 - Privilege escalation and root flag

Please, note that to run the command you see in the previous picture you need to open the right “**nano** section” using first and after .

# **Personal comments**

This box, in my opinion, is mainly based on finding of information on the target machine. For me, this is a quite hard task because I have to find a structured way to do it and improve my methodology for this task. Also, I think this box is quite challenging because the ONA link is present only on the /music path home page and NOT in the other pages on the same /music path. This is, in my opinion, very unrealistic and make me lost a lot of time (I checked the login link in other pages and the ONA link was not present, so I searched more and more). Also, the flag values I found as described didn’t work, so I was not able to insert them on HackTheBox site and rate this box. Anyway, due to this box require several tasks to retrieve the user flag, the login link matter I described before and the need to use port forwarding, I consider this box as **medium** difficulty and not easy as you can find on HackTheBox site. Also, I created a more comprehensive wordlist to use it in brute force attacks.

# **References**

ONA exploit - <https://github.com/amriunix/ona-rce>

Chisel download - <https://github.com/jpillora/chisel/releases>

Crackstation - <https://crackstation.net/>

GTFOBins - <https://gtfobins.github.io/>