**AcademyTCM walkthrough**

# **Index**

[Index 1](#_Toc202889881)

[List of pictures 1](#_Toc202889882)

[Disclaimer 2](#_Toc202889883)

[Reconnaissance 2](#_Toc202889884)

[Initial foothold 2](#_Toc202889885)

[User flag 3](#_Toc202889886)

[Privilege escalation 5](#_Toc202889887)

[Personal comments 6](#_Toc202889888)

# **List of pictures**

[Figure 1 - nMap scan results 2](#_Toc202889911)

[Figure 2 - FTP share content 2](#_Toc202889912)

[Figure 3 - Note file content 3](#_Toc202889913)

[Figure 4 - Password cracked 3](#_Toc202889914)

[Figure 5 - Academy website 3](#_Toc202889915)

[Figure 6 - User profile exploited 4](#_Toc202889916)

[Figure 7 - RCE 4](#_Toc202889917)

[Figure 8 - New credentials found 4](#_Toc202889918)

[Figure 9 - PSPY output 5](#_Toc202889919)

[Figure 10 - Script tampered 5](#_Toc202889920)

[Figure 11 - Root flag 5](#_Toc202889921)

# **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

Open ports are 21, 22 and 80. Therefore, enabled services are FTP (21) and SSH (22). Also, a web application is running on port 80. Lastly, nMap recognized Linux as operative system.

# **Initial foothold**

The first service I analyzed was FTP. I tried to perform an anonymous login and, luckily, it worked. All I found in the FTP share was a note file:

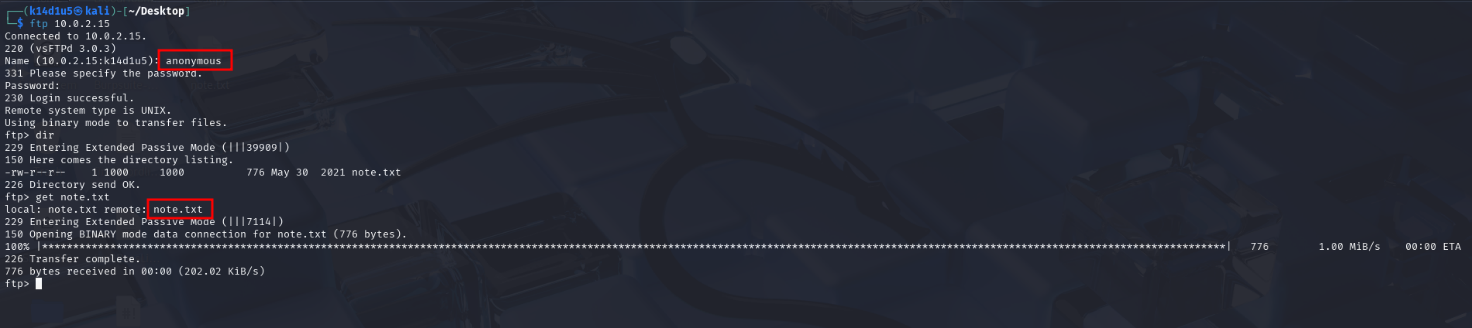


Figure 2 - FTP share content

I was able to retrieve interesting information by this file:

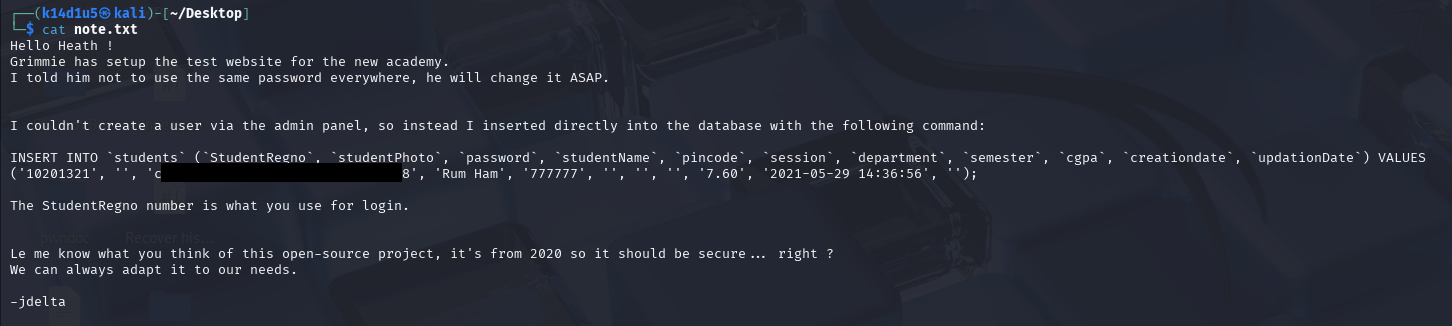


Figure 3 - Note file content

In particular, I found some credentials, I learnt that Grimmie could use the same password everywhere and the application was an open-source project that could be vulnerable. Since the password was hashed, I tried to crack it. Luckily, CrackStation was able to do it and I obtained the plaintext password:

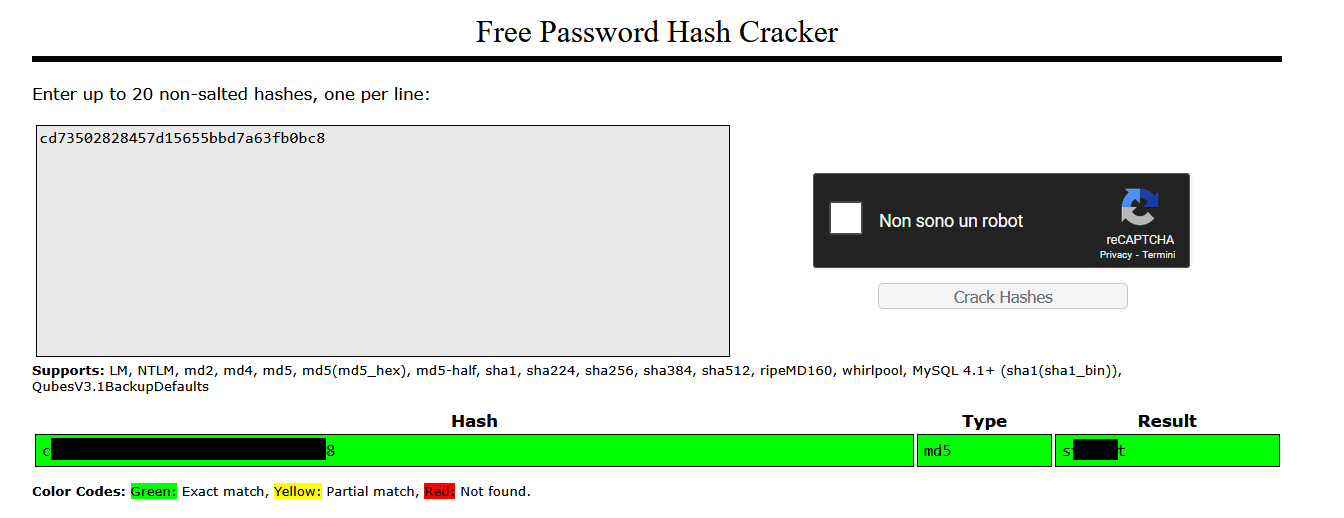


Figure 4 - Password cracked

Lastly, I run FFUF to find hidden web content and I found out two paths: and .

# **User flag**

Once I found the academy URL, I was able to login using the credentials I cracked. At this point, I remembered that the academy site was an open-source project. I supposed that its name was something similar to the name I found on the login page:

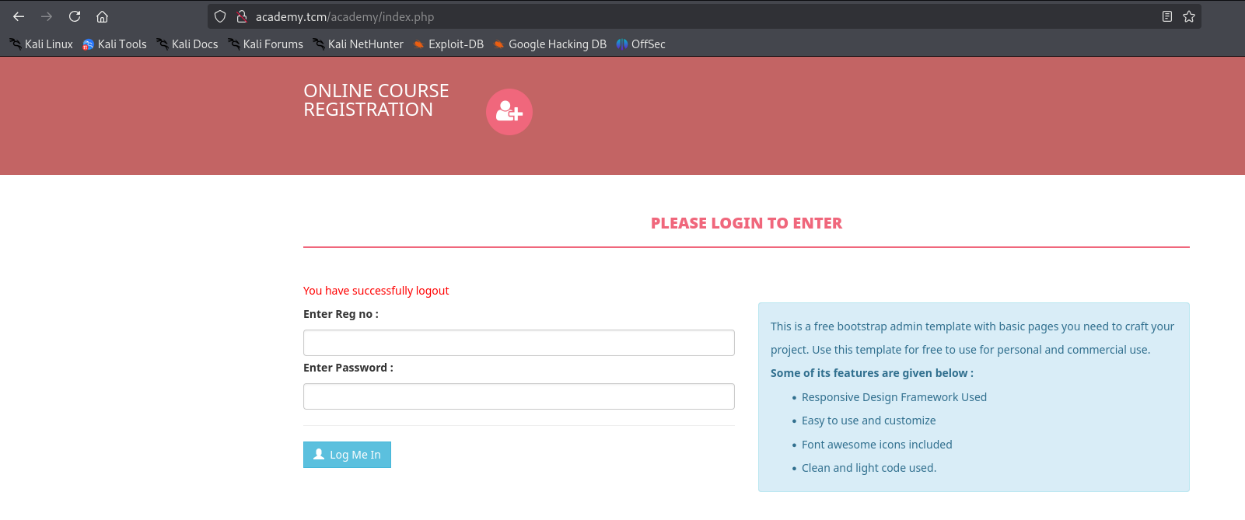


Figure 5 - Academy website

I looked for it on the Internet and I found an interesting exploit. I run it and luckily it worked. It uploaded a web shell in the profile image of the user:

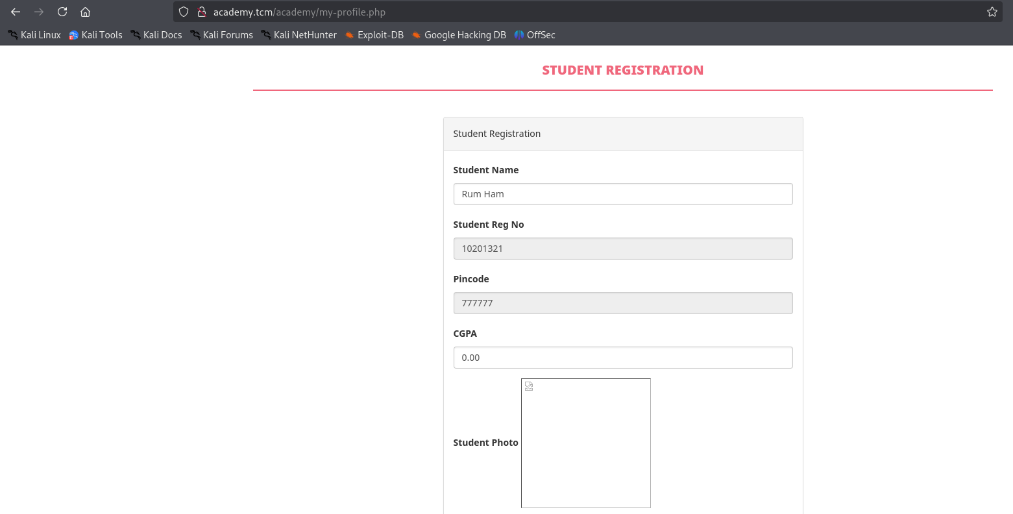


Figure - User profile exploited

I can interact with it using the URL <http://academy.tcm/academy/studentphoto/kaio-ken.php?telepathy=>. In the parameter I can send a command to execute:

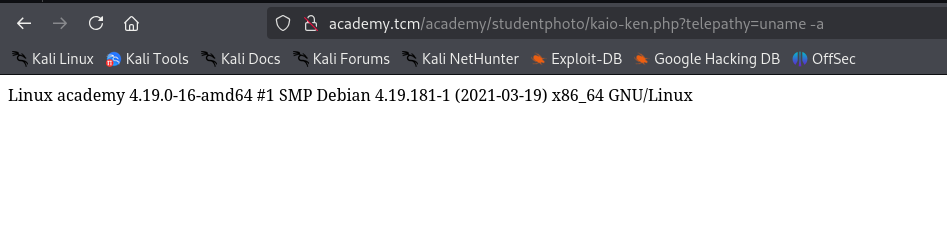


Figure 7 - RCE

In this way, I was able to get a reverse shell on my local Kali machine. Using it, I explored the file system and I found a new pair of credentials:

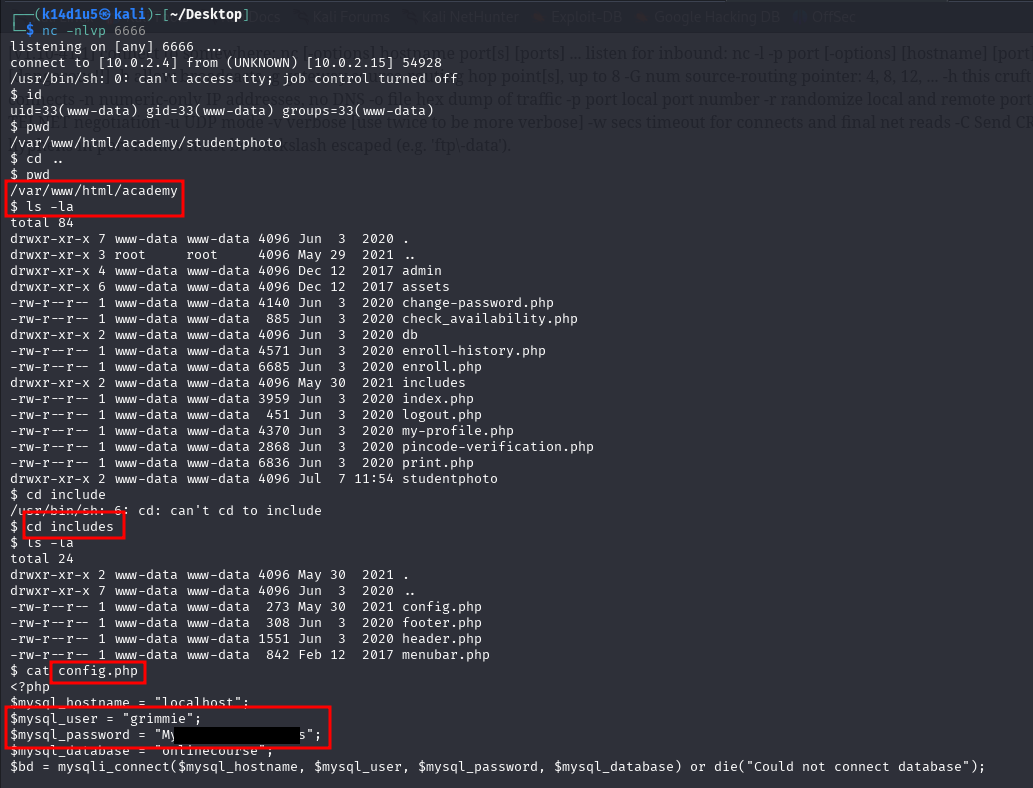


Figure 8 - New credentials found

Again, I remembered that Grimmie used to set the same password everywhere. Therefore, I tried to connect via SSH as user. I was successful. In contrast with Hack The Box platform, TCM box hadn’t a user flag.

# **Privilege escalation**

I explored the file system as user and I found an interesting script in its home directory. This script performs a web application folder backup. I investigate deeper about it, and I found out that it is periodically invoked by user with UID , that means user. I obtained this information using tool, as shown in the following picture:

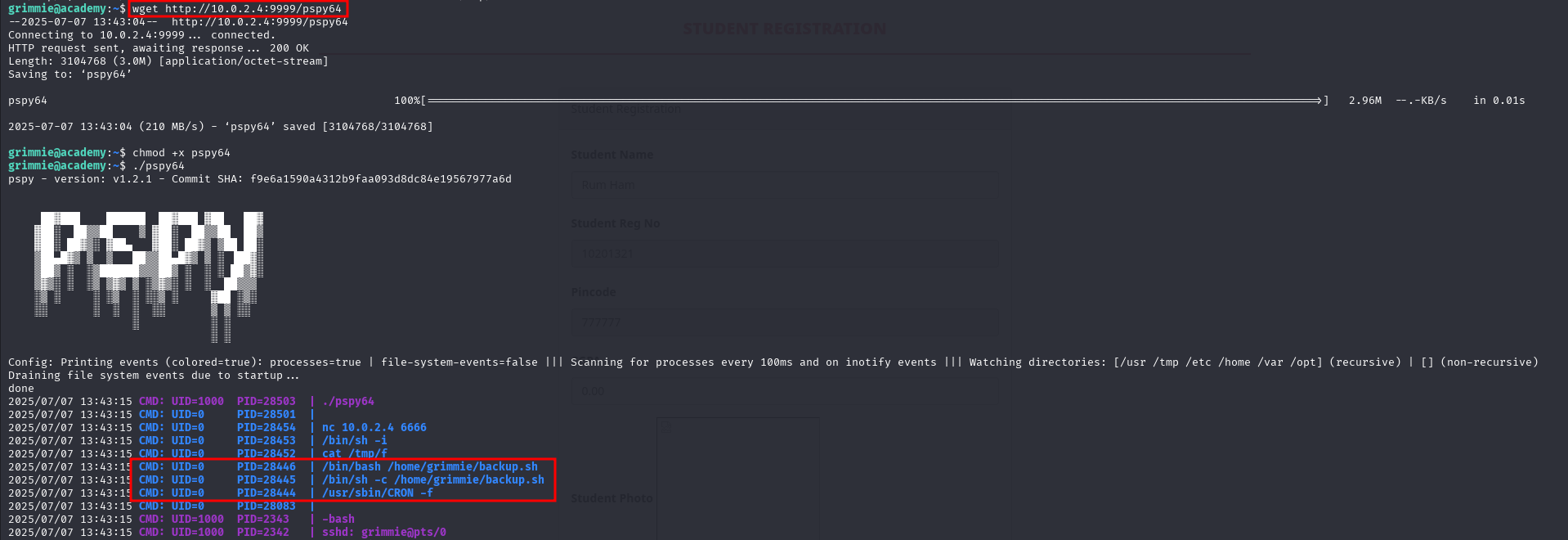


Figure 9 - PSPY output

At this point, all I needed was tampering the backup script and I added a reverse shell command:

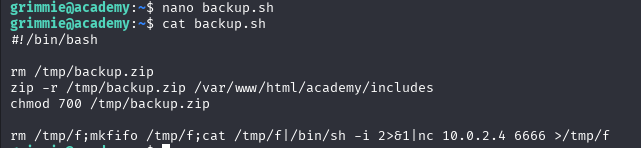


Figure 10 - Script tampered

In this way, I needed just to wait for a while with a listener opened and I obtained a shell as . Using it, I retrieved the TCM flag:

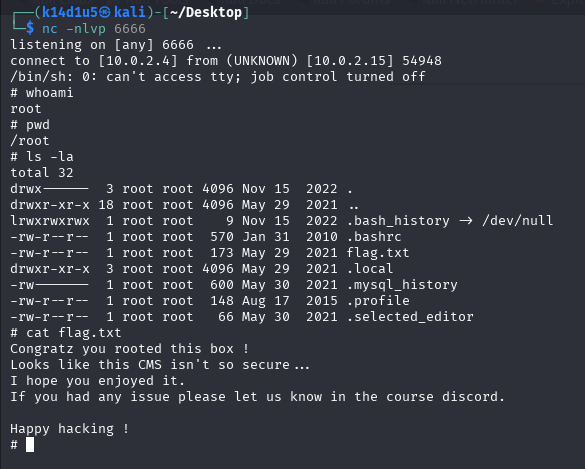


Figure 11 - Root flag

# **Personal comments**

It was a very nice box. I consider it easy, but it let you to learn something interesting in penetration testing field. For example, I personally learnt about , a very useful tool. This was the first Linux box I completed to accomplish the PNPT certification.