**Friendzone walkthrough**

# **Index**

[Index 1](#_Toc181733043)

[List of pictures 1](#_Toc181733044)

[Disclaimer 2](#_Toc181733045)

[Reconnaissance 2](#_Toc181733046)

[Initial foothold 3](#_Toc181733047)

[User flag 5](#_Toc181733048)

[Privilege escalation 8](#_Toc181733049)

[Personal comments 8](#_Toc181733050)

[References 8](#_Toc181733051)

# **List of pictures**

[Figure 1 - nMap scan results (part 1) 2](#_Toc181733014)

[Figure 2 - nMap scan results (part 2) 3](#_Toc181733015)

[Figure 3 - Investigation on Samba service 3](#_Toc181733016)

[Figure 4 - Credentials found 4](#_Toc181733017)

[Figure 5 - New subdomains found 4](#_Toc181733018)

[Figure 6 - Upload subdomain 4](#_Toc181733019)

[Figure 7 - Administrator1 subdomain 5](#_Toc181733020)

[Figure 8 - Local File Inclusion 5](#_Toc181733021)

[Figure 9 - Web shell uploaded 5](#_Toc181733022)

[Figure 10 - New payload uploaded 6](#_Toc181733023)

[Figure 11 - New payload executed 6](#_Toc181733024)

[Figure 12 - Shell obtained 6](#_Toc181733025)

[Figure 13 - User flag 7](#_Toc181733026)

[Figure 14 - Credentials found 7](#_Toc181733027)

[Figure 15 - Shell as friend user 7](#_Toc181733028)

[Figure 16 - Exploit 8](#_Toc181733029)

[Figure 17 - Privilege escalation and root flag 8](#_Toc181733030)

# **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:

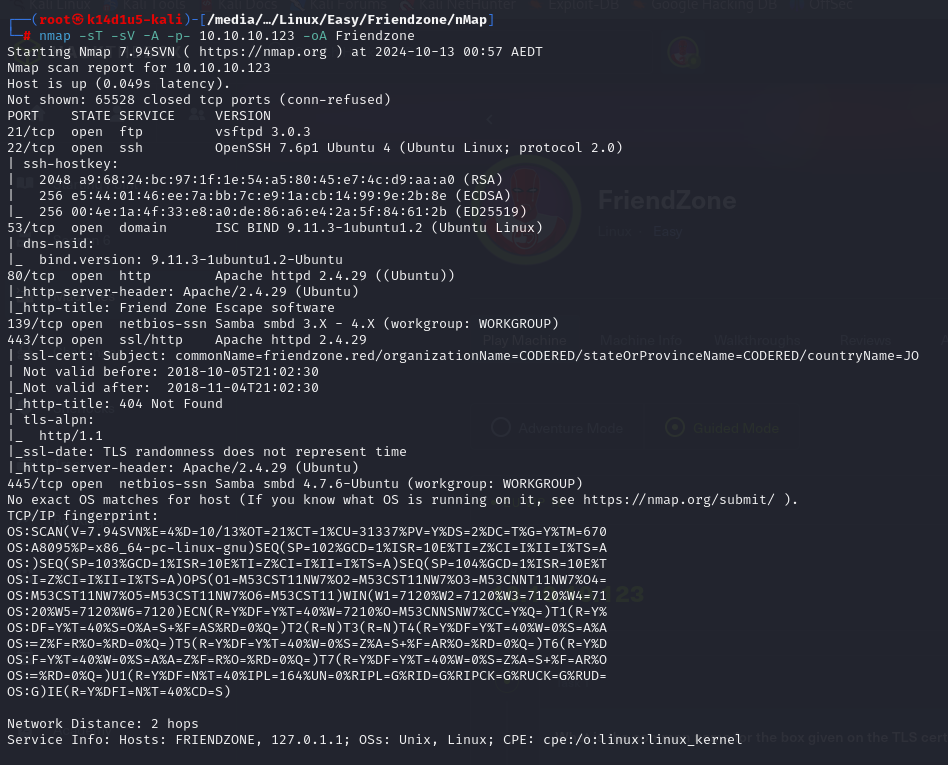


Figure 1 - nMap scan results (part 1)

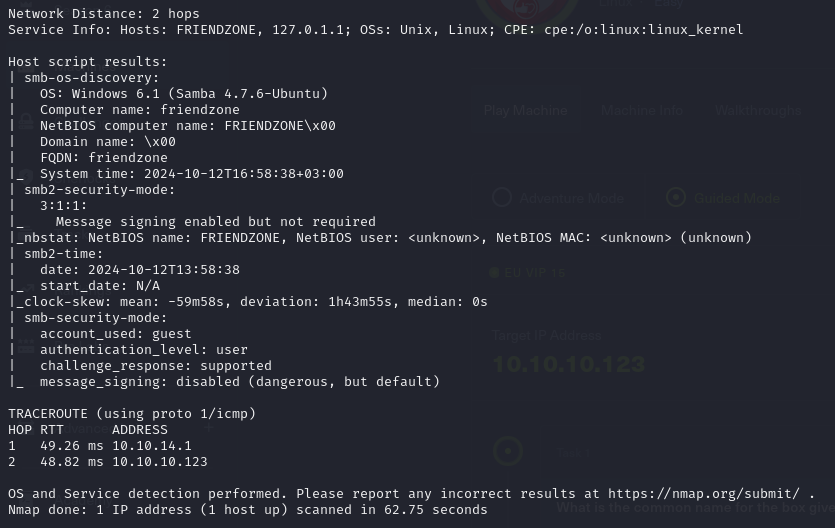


Figure 2 - nMap scan results (part 2)

Open ports are 21, 22, 53, 80, 139, 443, 445. So, this machine has FTP (21), SSH (22), DNS (53) and Samba (139 and 445) services enabled and a web application running on port 80 and 443. Also, nMap provide Linux as Operative System, but it didn’t provide any further details.

# **Initial foothold**

Based on which services are enabled, I first investigated the Samba one. I was able to retrieve some interesting information, such as which shares I was able to access to, as shown in the following:

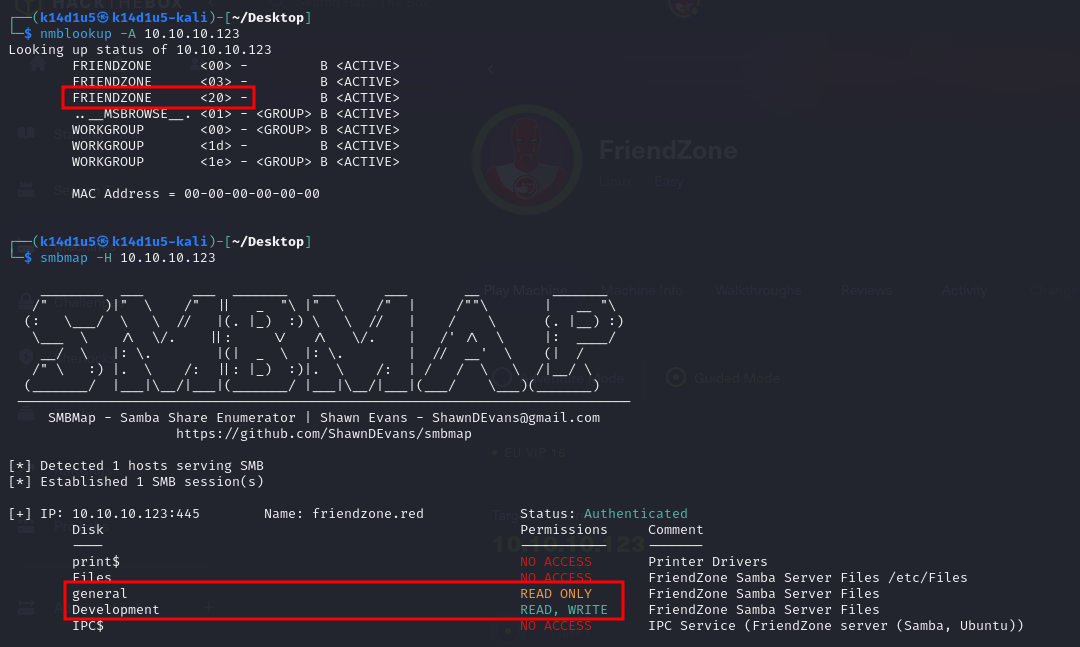


Figure 3 - Investigation on Samba service

In particular, I found the and shares. At this point is important to note that the share is stored in the path and I had the permission on the one. I tried to access to them, but I didn’t find anything in the one. However, when I accessed to the one I had more luck. In fact, I found some credentials in this share:

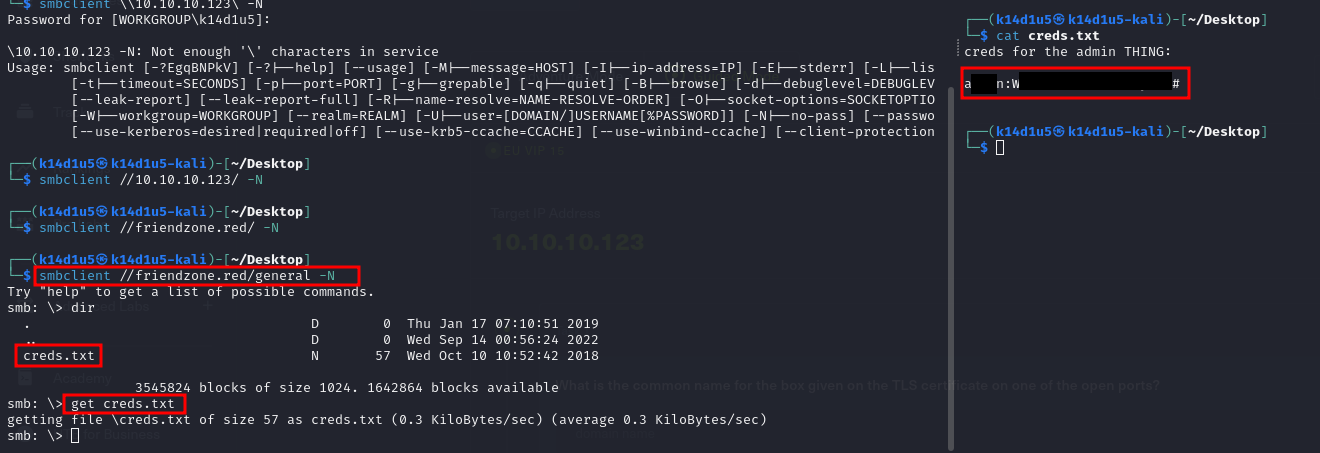


Figure 4 - Credentials found

At this point, I didn’t know where to use these credentials. So, I started to investigate a different service. The service I choose was DNS. Thanks to this analysis, I found some new and interesting subdomains:

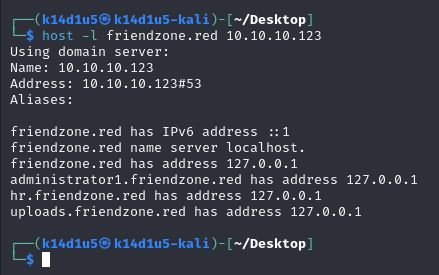


Figure 5 - New subdomains found

In particular, the subdomain allowed me to upload an image:

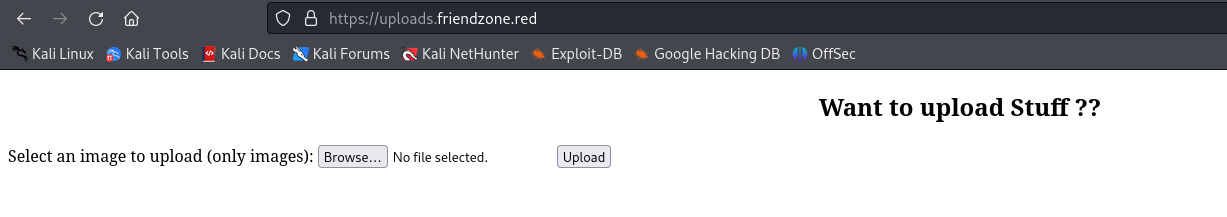


Figure 6 - Upload subdomain

On the other hand, the require a login and luckily some valid credentials are the ones I found before. Once I logged in, I was able to render some known images:

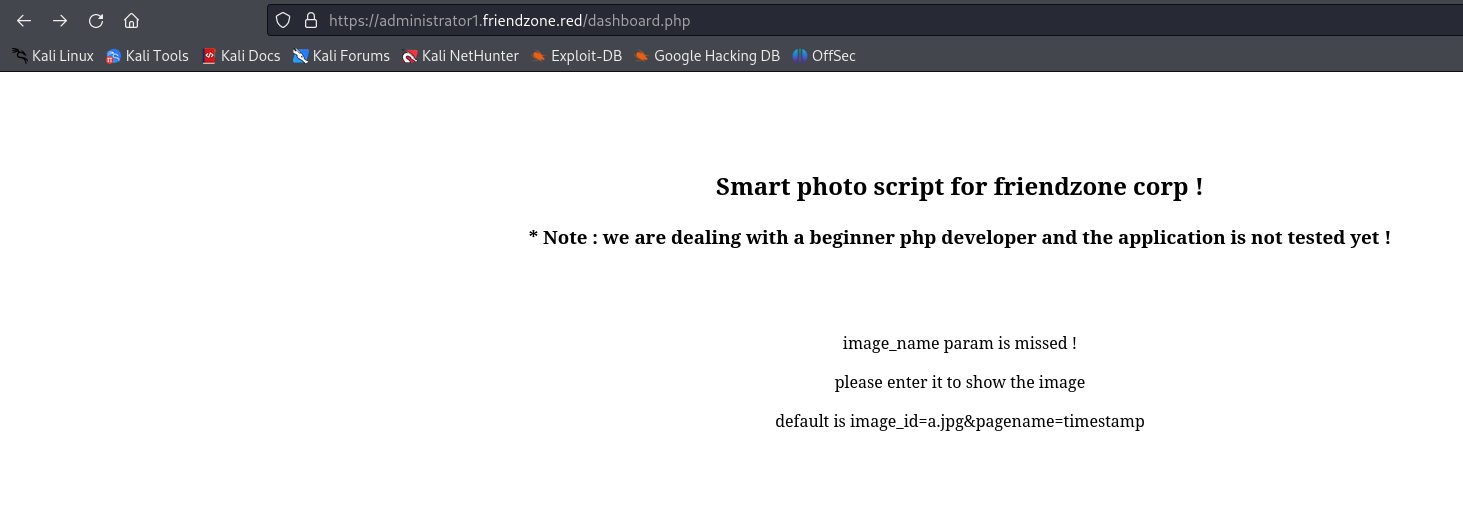


Figure 7 - Administrator1 subdomain

Here, it is really important to note that a page is referred in a parameter. In particular, I noted that there is a Local File Inclusion:

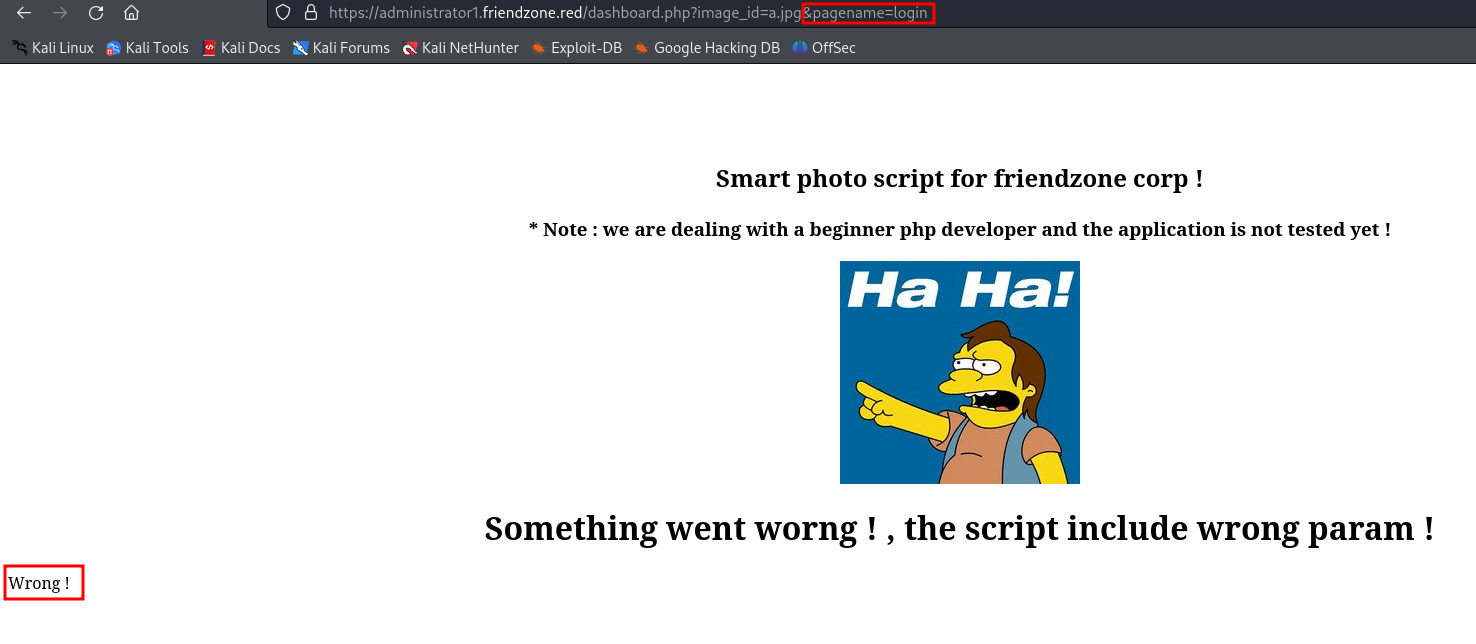


Figure 8 - Local File Inclusion

# **User flag**

Based on all information I found, I thought I was ready to exploit the box. Since I found a share where I was able to write, I uploaded on it a malicious PHP file to open a web shell:

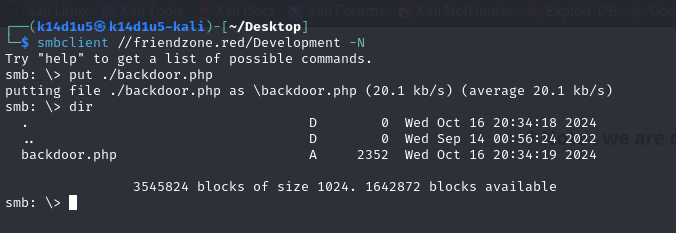


Figure 9 - Web shell uploaded

I was able to invoke it browsing to the URL. I hypothesized the share path based on the path of the share I found. In this way, I was able to execute an arbitrary command and in particular I uploaded a new payload I generated using :



Figure 10 - New payload uploaded

Using the web shell, I gave it execution permissions and I executed:

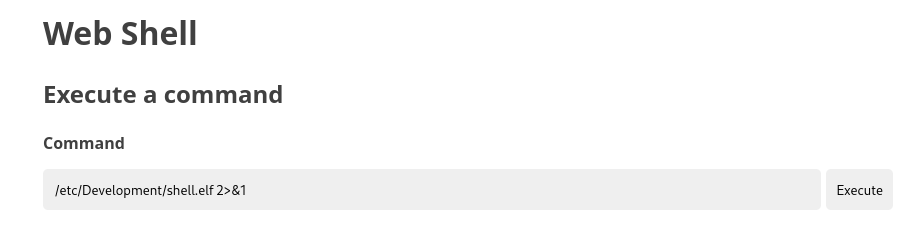


Figure 11 - New payload executed

In this way, I obtained a first shell as user:

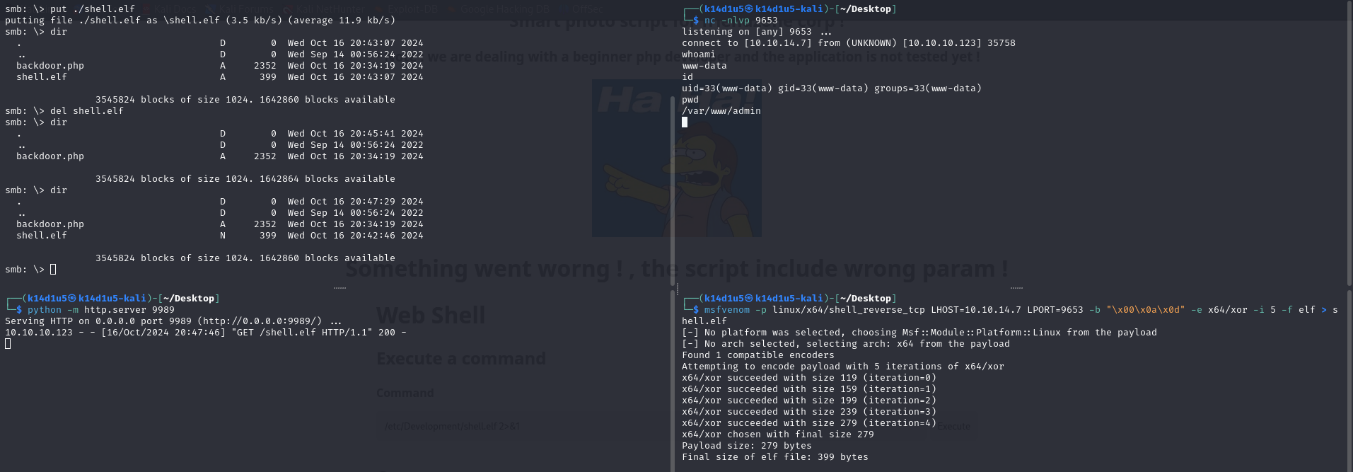


Figure 12 - Shell obtained

Even I was a service user, I tried to retrieve the user flag and unexpectedly I was able to retrieve yet:

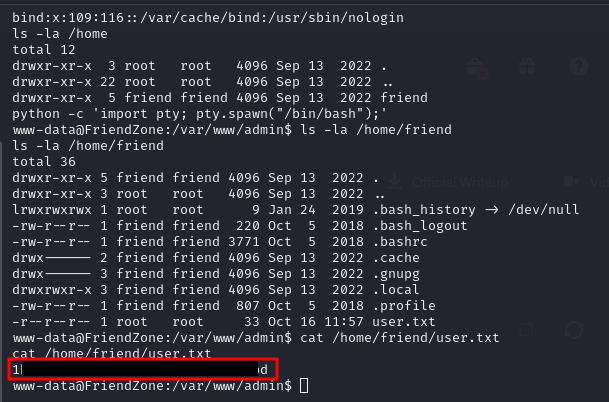


Figure 13 - User flag

Of course, I needed to became a common user on the machine. To do it, I explored the filesystem and I found a database file which contained credentials:

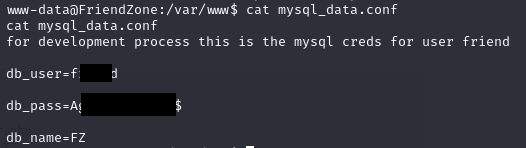


Figure 14 - Credentials found

These credentials are useful to connect to the database. However, I tried to use to login in SSH and it worked, as shown in the following figure:

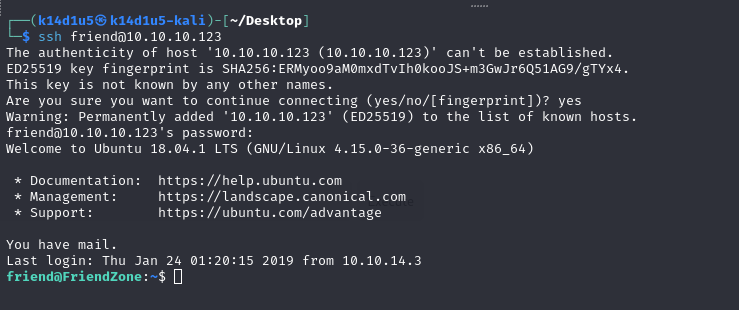


Figure 15 - Shell as friend user

# **Privilege escalation**

At this point, all I needed to do was escalating my privileges and retrieve the root flag. I investigated about some information and I found out that the friend user is in the group. This means that he can read logs from . So, I analyzed these logs and in the I found out that run the script and script is world writable. I analyzed the script and I found out that it imported the library. Luckily, this script is in Python 2. So, I just need to modify the library as shown in the following:



Figure 16 - Exploit

At this point, I just needed to wait a little bit with an open listener and I received the root shell where I retrieved the root flag:

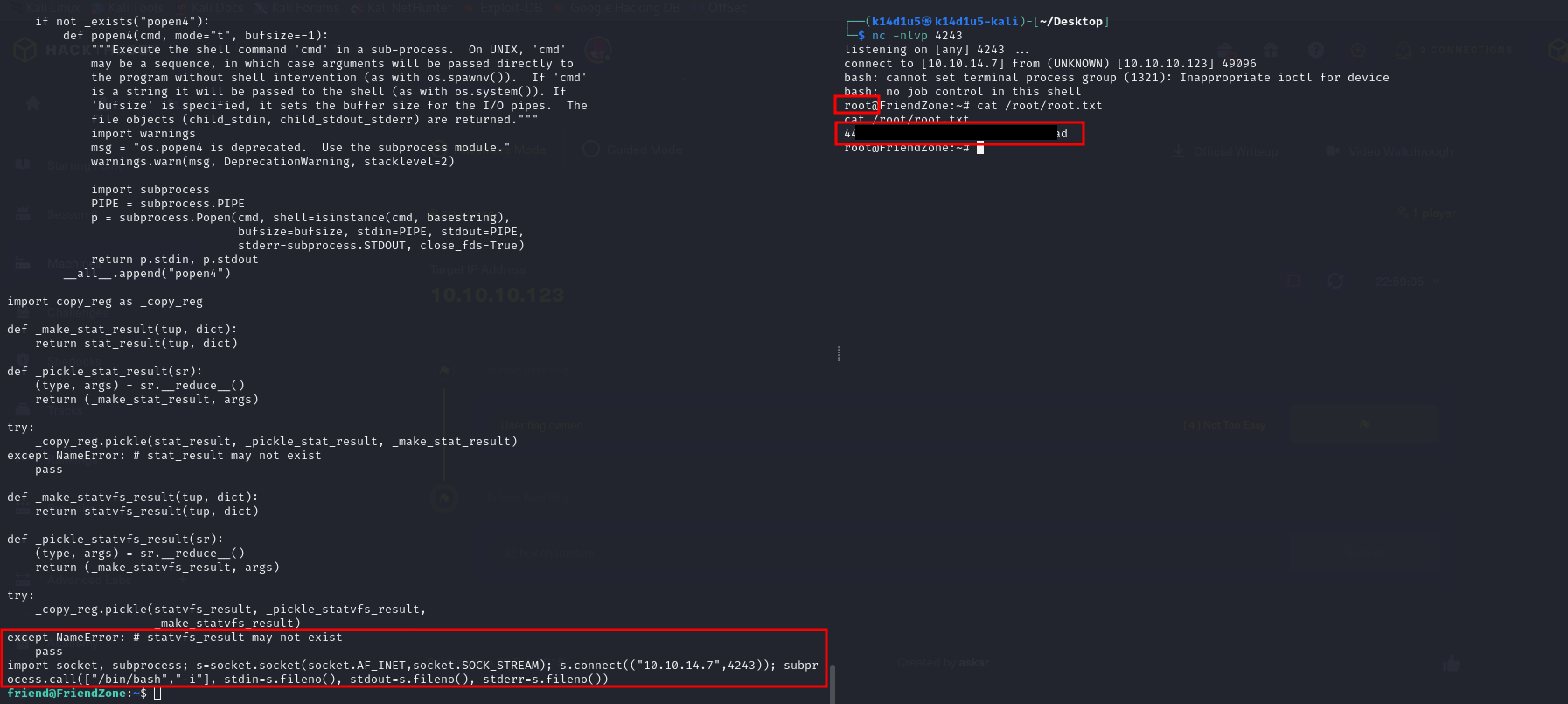


Figure 17 - Privilege escalation and root flag

# **Personal comments**

I enjoyed this box because challenged me on different aspects. It was very interesting the way to obtain the first shell and get me focused on the nMap output because in some point there were some points that make you think that it could be a Windows machine. So, it is important to be focused and pay attention. My overall evaluation is because you need to note an LFI, is world writable (but ONLY the Python2 version!) and script is periodically invoked (each few minutes).

# **References**

<https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe> -> Exploiting Linux groups