**Sau walkthrough**

# **Index**

[Index 1](#_Toc157412991)

[List of pictures 1](#_Toc157412992)

[Disclaimer 2](#_Toc157412993)

[Reconnaissance 2](#_Toc157412994)

[Initial foothold 2](#_Toc157412995)

[User flag 4](#_Toc157412996)

[Privilege escalation 5](#_Toc157412997)

# **List of pictures**

[Picture 1 - nMap scan results 2](#_Toc157413006)

[Picture 2 - Application on port 55555 3](#_Toc157413007)

[Picture 3 - Basket created 3](#_Toc157413008)

[Picture 4 - Basket created 3](#_Toc157413009)

[Picture 5 - Basket malicious configuration 4](#_Toc157413010)

[Picture 6 - Application on port 80 4](#_Toc157413011)

[Picture 7 - Exploit running 5](#_Toc157413012)

[Picture 8 - Reverse shell obtained and user flag 5](#_Toc157413013)

[Picture 9 - Useful information for privilege escalation 5](#_Toc157413014)

[Picture 10 - Privilege escalation 6](#_Toc157413015)

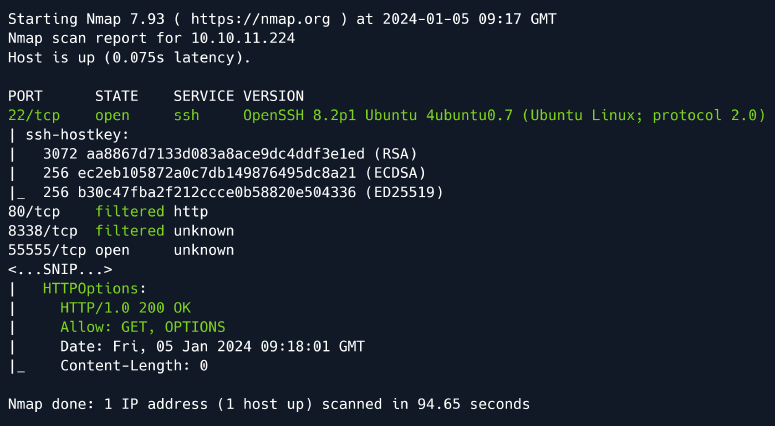
[Picture 11 - Root flag 6](#_Toc157413016)

# **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.

# **Reconnaissance**

The results of an initial nMap scan are the following:

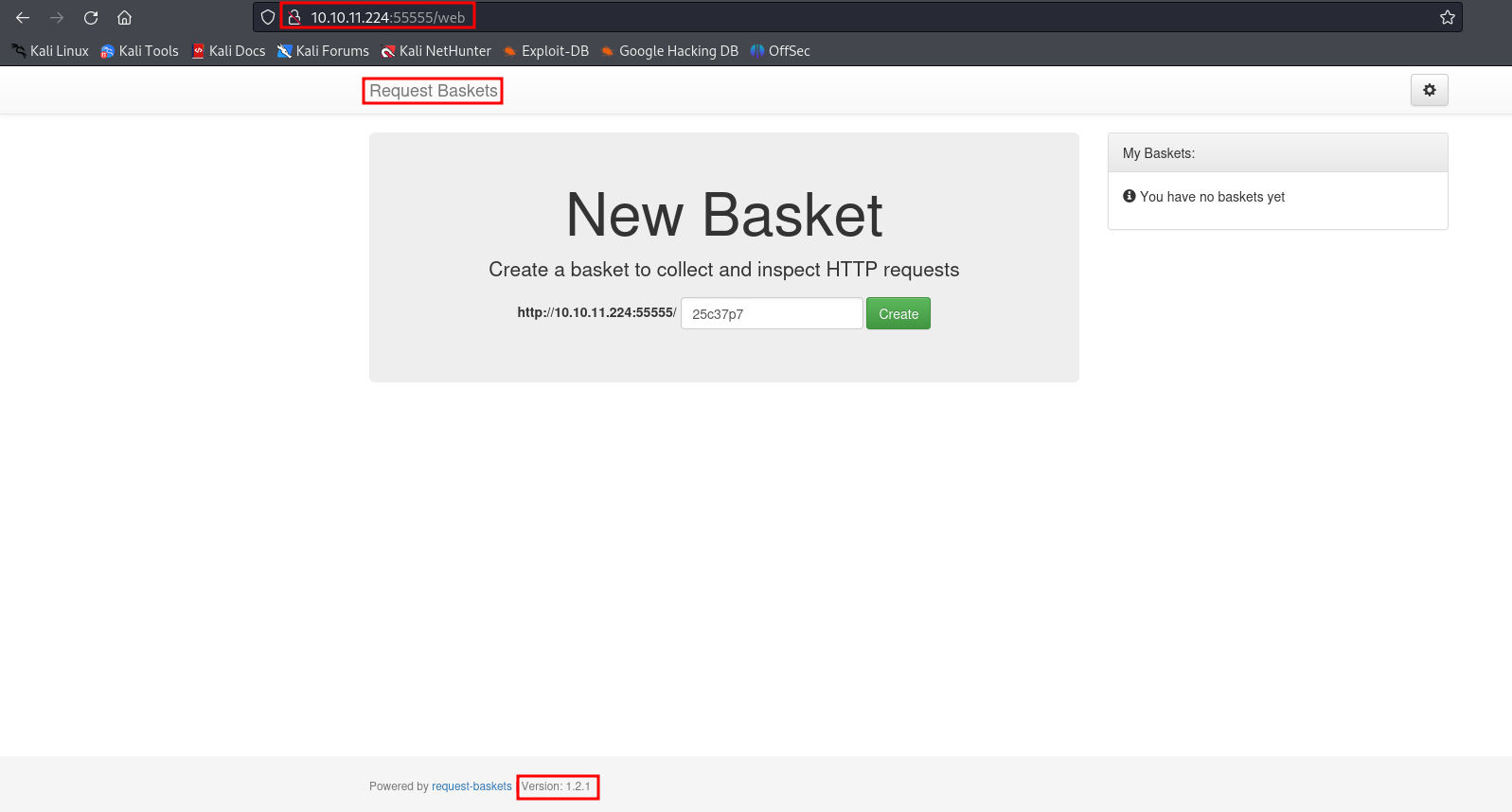


Picture 1 - nMap scan results

Open ports are 22 and 55555. Also, ports 80 and 8338 are filtered. So, the machine has SSH service enabled and an application is running on port 55555. NMap told me that operative system is Ubuntu.

# **Initial foothold**

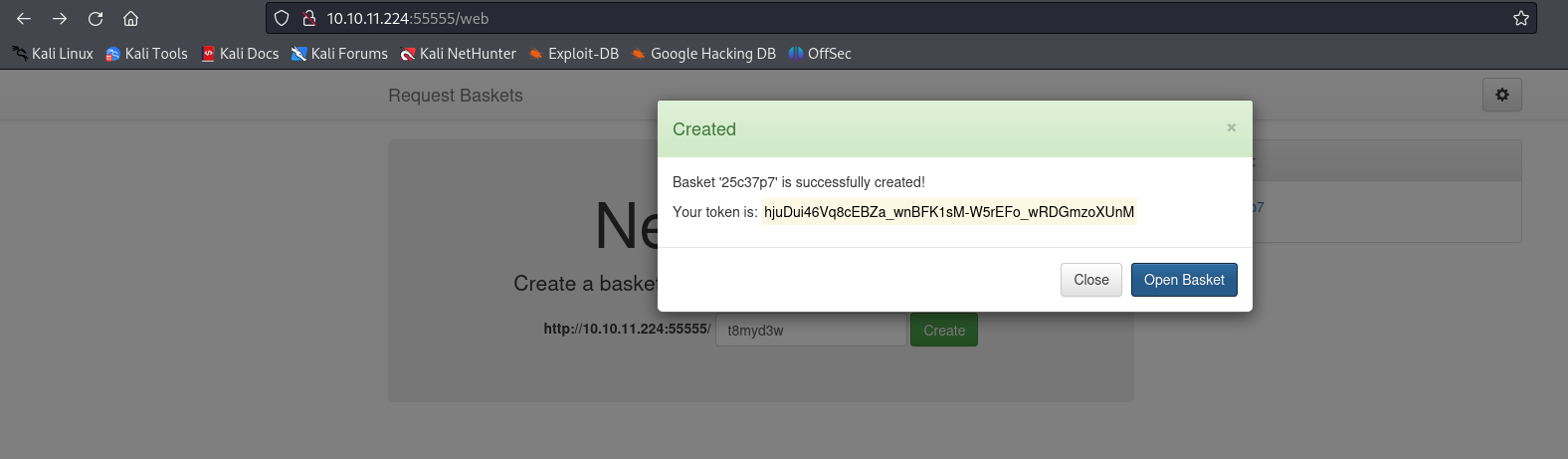
Browsing the web application, it is possible found that the application is “**Basket request**” version **1.2.1:**

****

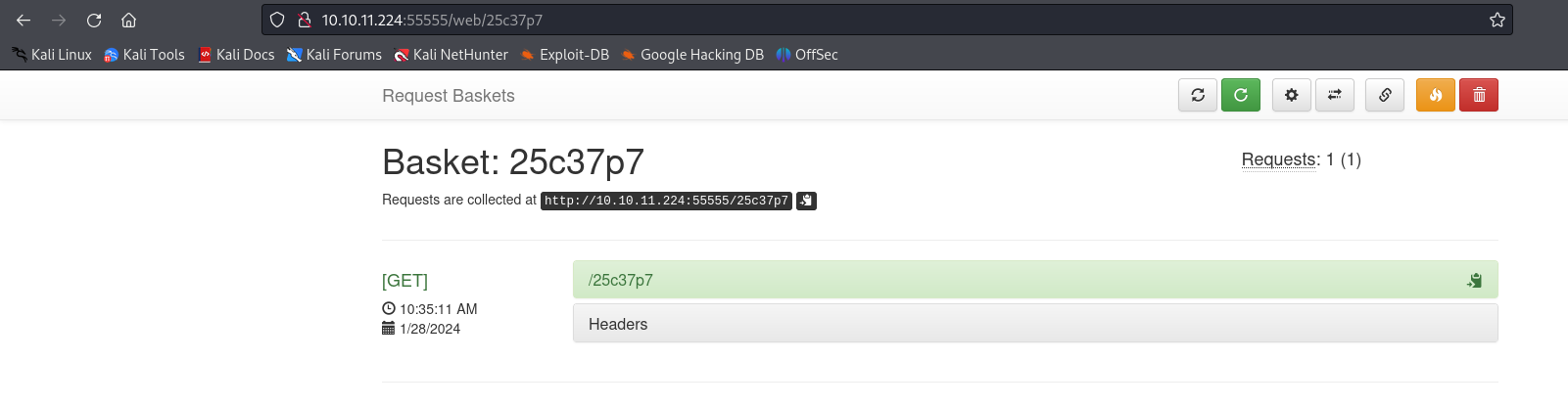
Picture 2 - Application on port 55555

This application let me to create and configure a basket. After a look on the Internet, I found [**CVE-2023-27163**](https://nvd.nist.gov/vuln/detail/CVE-2023-27163). It let me to execute a Server-Side Request Forgery attack. I exploited it to reach application on port 80. In fact, request basket is a web application built to collect and register requests on a specific route, so called basket. When creating it, the user can specify another server to forward the request. The issue here is that the user can specify unintended services, such as network-closed applications.

First, I had to create a new basket:

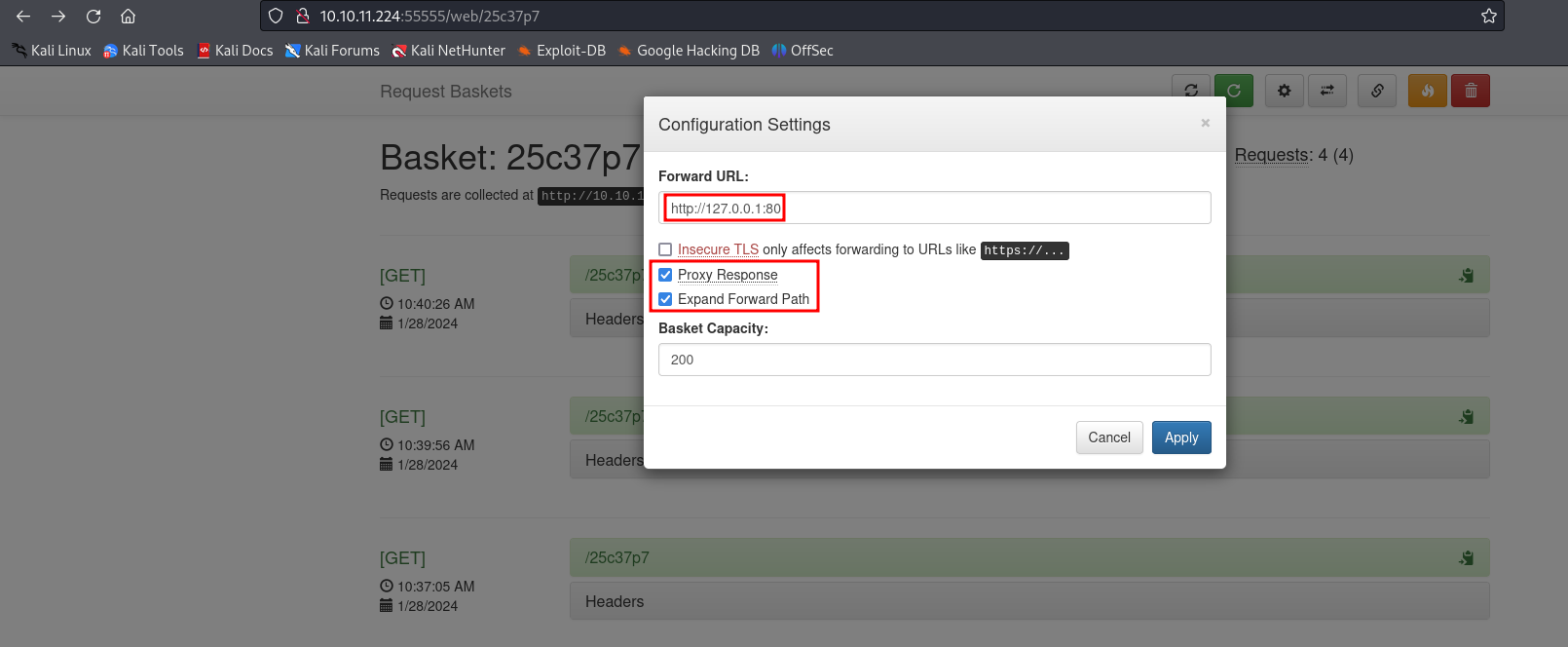


Picture 3 - Basket created



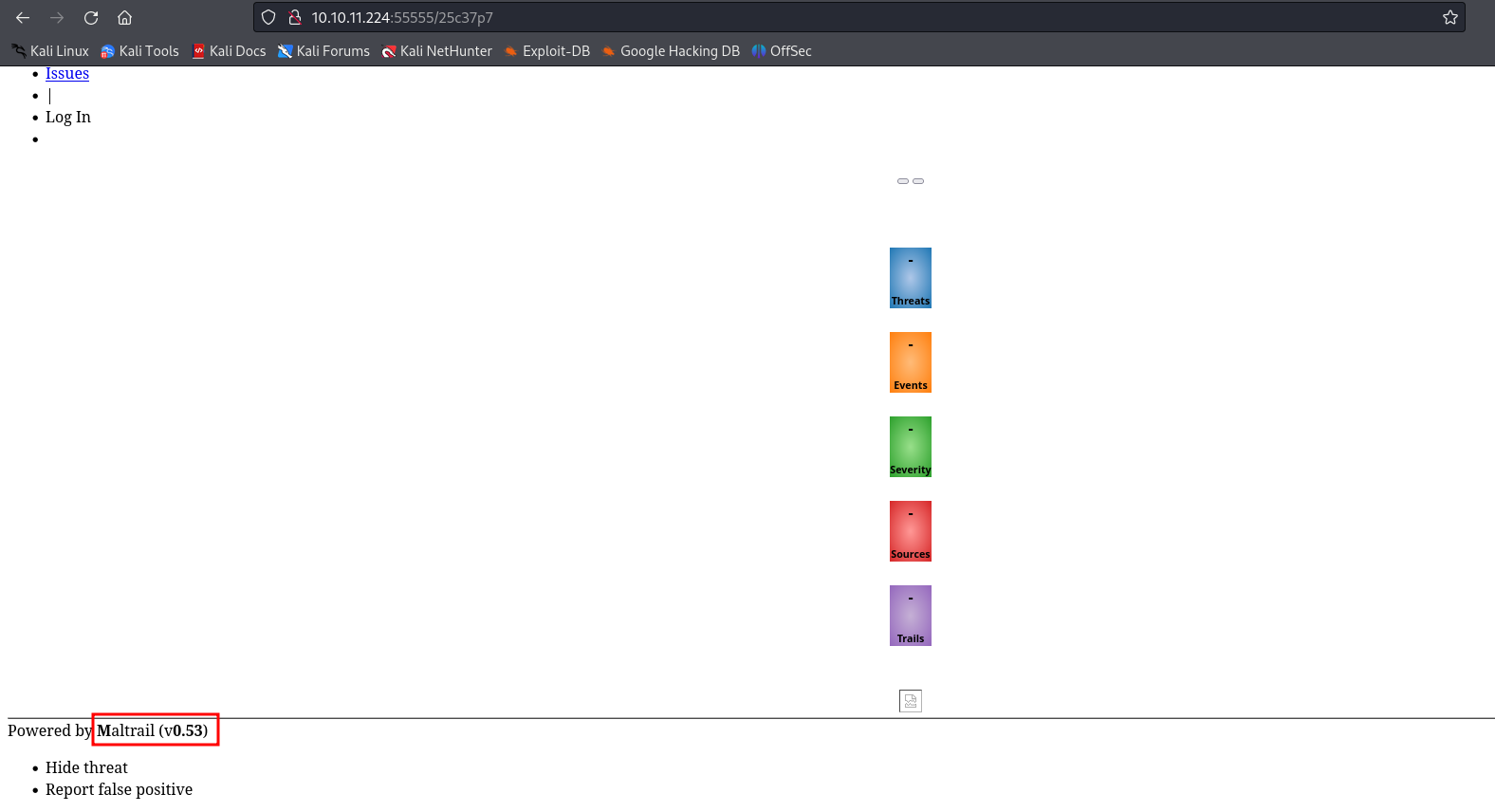
Picture 4 - Basket created

It is important take note about the basket id. After this, I configured it to reach service on port 80:



Picture 5 - Basket malicious configuration

At this point I was able to reach application on port 80 via <http://10.10.11.224:55555/25c37p7>. Application on port 80 is **Maltrail** version **0.53**:

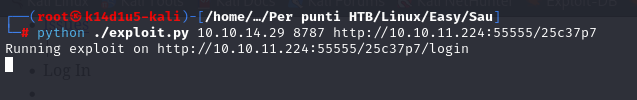


Picture 6 - Application on port 80

Again, I searched on the Internet some possible known vulnerabilities. I found this application is vulnerable to RCE and I downloaded an exploit in a file named **exploit.py**.

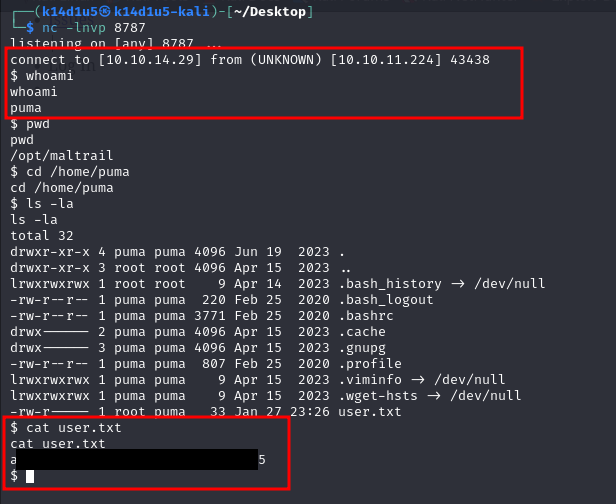
# **User flag**

This was the moment to run this exploit, as shown in the following picture:



Picture 7 - Exploit running

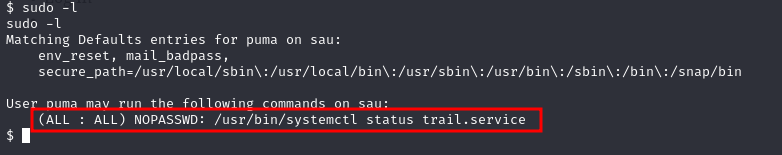
This exploit opened a reverse shell. From it, I obtained the user flag:



Picture 8 - Reverse shell obtained and user flag

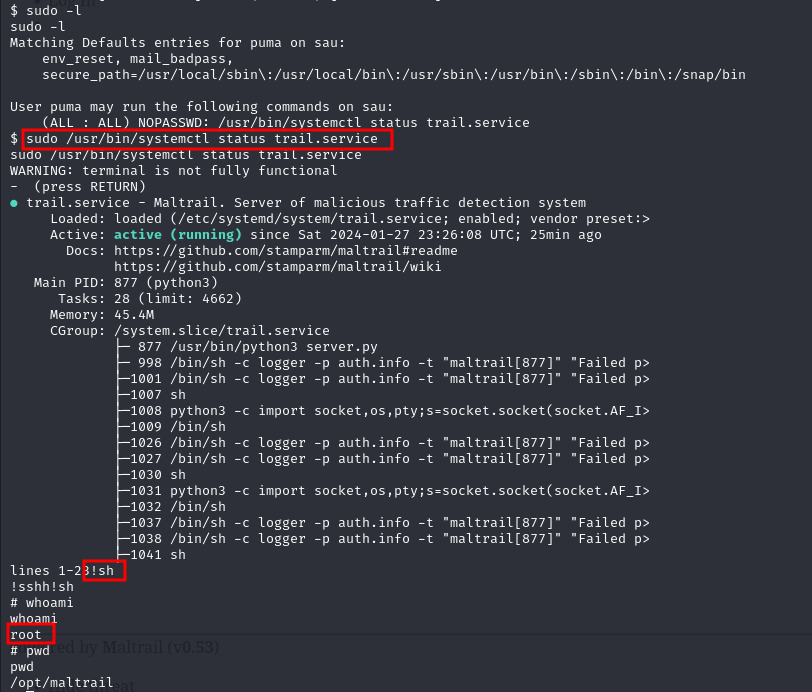
# **Privilege escalation**

At this point I started to search some useful information to escalate my privileges. For example, I uploaded **linpeas.sh** script. The useful information for privilege escalation is the following:



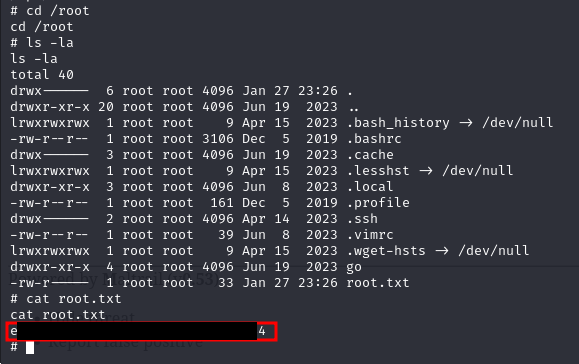
Picture 9 - Useful information for privilege escalation

When I run this command, his execution leaved me in an environment where I can execute command in a similar way I run command in **vi**. So, I run the **!/sh** command and I obtained a shell as root:



Picture 10 - Privilege escalation

Of course, from this shell I obtained the root flag:



Picture 11 - Root flag