**Analytics walkthrough**

# **Index**

[Index 1](#_Toc157088392)

[List of pictures 1](#_Toc157088393)

[Disclaimer 2](#_Toc157088394)

[Reconnaissance 2](#_Toc157088395)

[Initial foothold 2](#_Toc157088396)

[Exploring the application 2](#_Toc157088397)

[User flag 4](#_Toc157088398)

[Privilege escalation 5](#_Toc157088399)

# **List of pictures**

[Picture 1 - nMap scan results 2](#_Toc157088165)

[Picture 2 - Application login 3](#_Toc157088166)

[Picture 3 - Metasploit module configuration 3](#_Toc157088167)

[Picture 4 - User credentials 4](#_Toc157088168)

[Picture 5 - SSH login as not privileged user 4](#_Toc157088169)

[Picture 6 - User flag 5](#_Toc157088170)

[Picture 7 - Info useful to escalate privileges 5](#_Toc157088171)

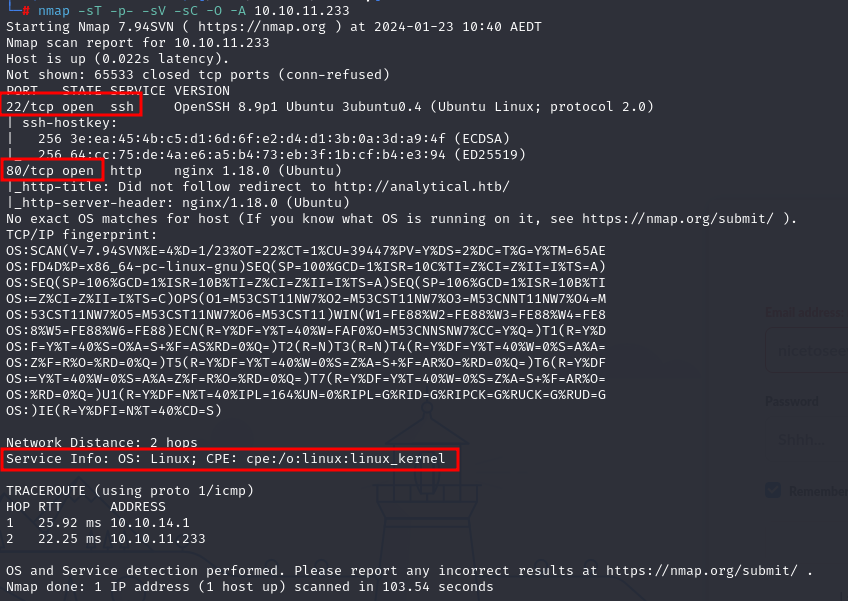
[Picture 8 - Privilege escalation and root flag 5](#_Toc157088172)

# **Disclaimer**

I do these boxes 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 walkthroughes 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

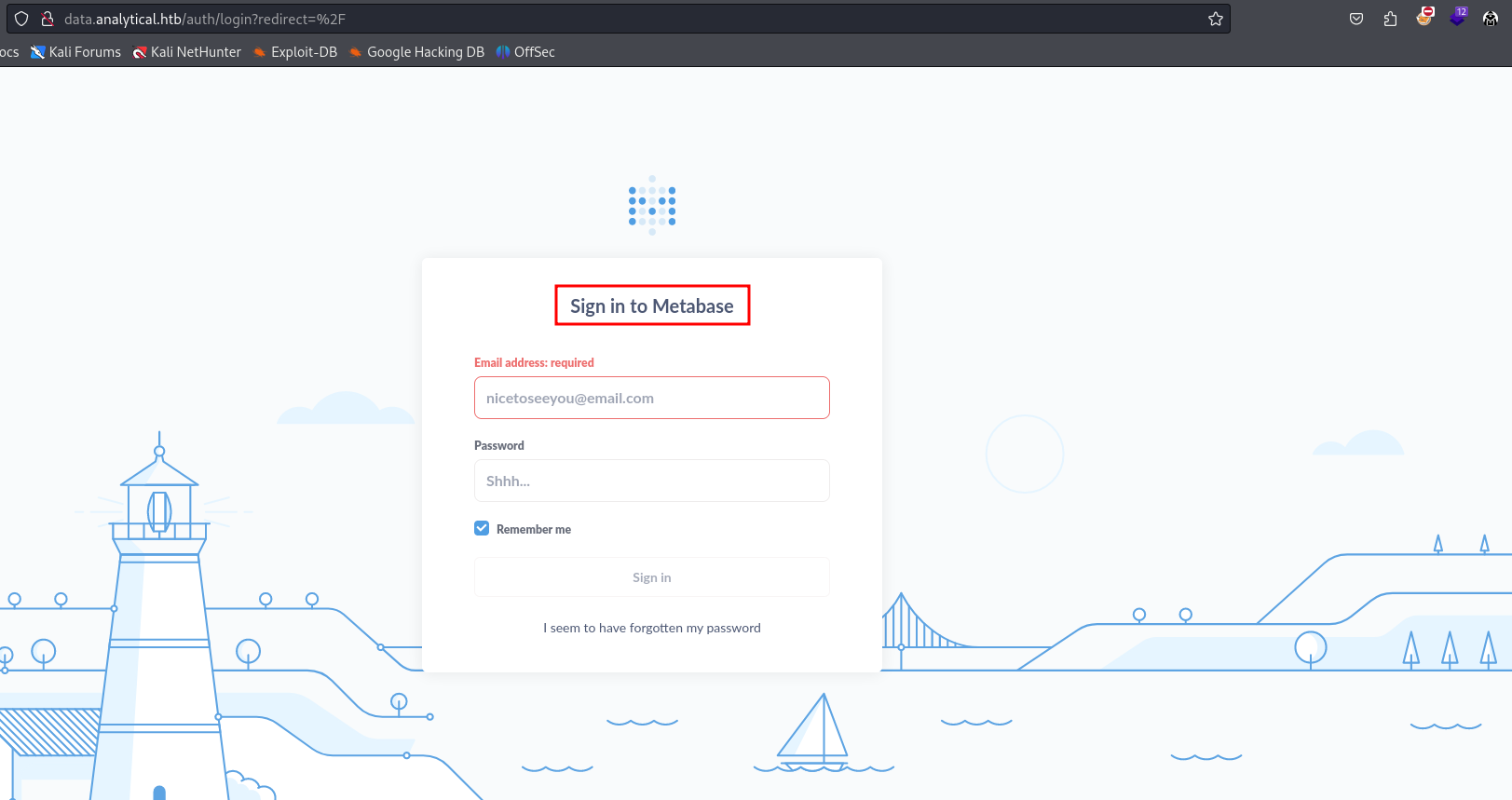
Ports open are number 22 and 80. So, the box has SSH enabled and an application running on port 80. Also, the operative system is Ubuntu.

To access to the application, it is needed to add a new entry in the host file:

# **Initial foothold**

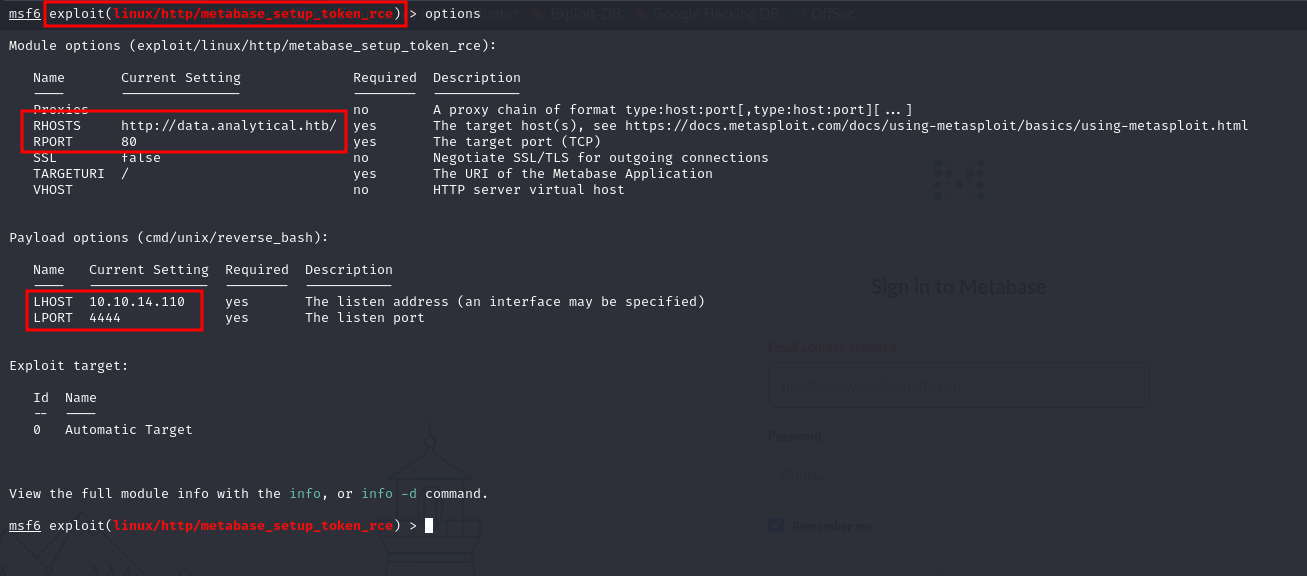
## **Exploring the application**

Exploring the application, I found the following login page via Burp requests interception:



Picture 2 - Application login

This login page is based on Metabase, an open source business intelligence tool. I tried some default credentials found on the Internet, but they didn’t work. Next step was to search some know exploit for Metabase. I discovered Metabase has a disclosed pre-authentication RCE vulnerability and the relative CVE is [**CVE-2023-38646**](https://nvd.nist.gov/vuln/detail/CVE-2023-38646). This bug in Metabase involved a retained ***setup-token*** post-installation, accessible to unauthenticated users. This flaw, resulting from a codebase refactoring oversight, allowed exploitation via SQL injection in the H2 database driver during the Metabase setup phase. The exploit enabled pre-authentication Remote Code Execution (RCE) by manipulating database connection validation steps. To exploit this vulnerability, I used the ***metasploit\_setup\_token\_rce*** Metasploit module. I configured it as shown in the following picture:

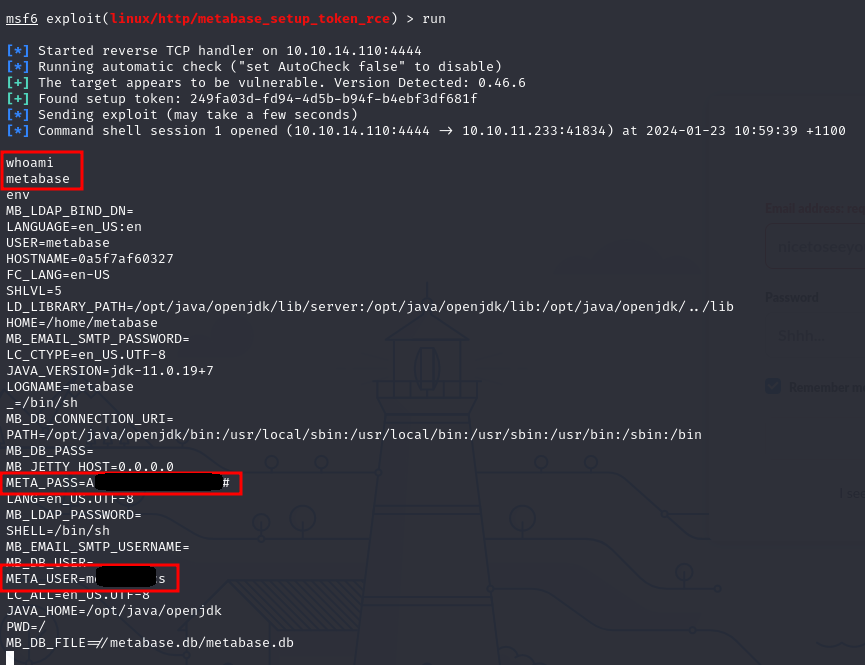


Picture 3 - Metasploit module configuration

Running this Metasploit module, I gained a shell on the target.

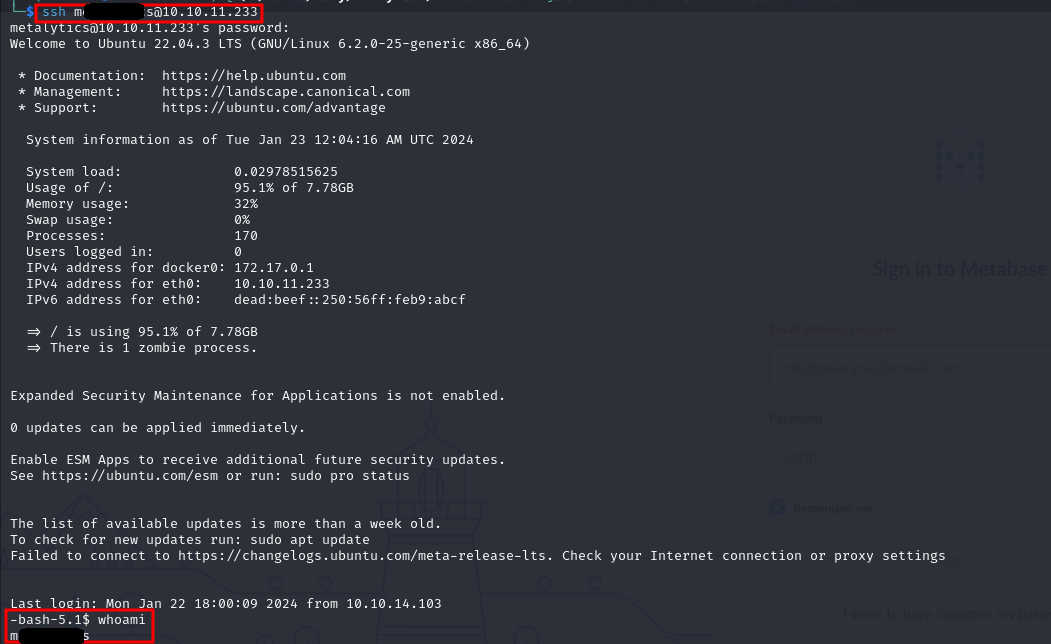
# **User flag**

I had this shell with user ***metabase***. I explored the system with this user, but I didn’t find the user flag. So, I started to search some other useful information. In particular, I found new credential in the environment variables, as shown in the following picture:



Picture 4 - User credentials

This user and password can be used to login to the system in SSH:



Picture 5 - SSH login as not privileged user

This time, I found the user flag in his home directory:



Picture 6 - User flag

# **Privilege escalation**

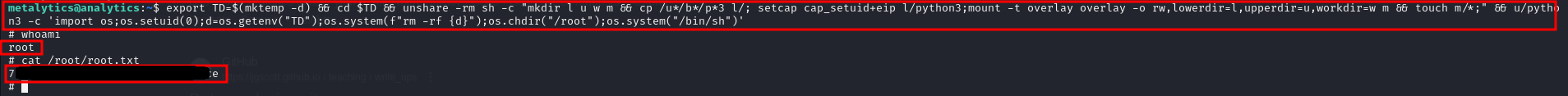
Since I found the user flag, I started to search some useful information to escalate my current privileges to root privileges. I executed ***linpeas.sh*** script, but it was not useful. The valuable information to execute a privilege escalation is the system operative version:



Picture 7 - Info useful to escalate privileges

In fact, I found an exploit for this Ubuntu version on the Internet. To accomplish my goal I used the following command:

In this way, I became ***root*** on the machine and I found the root flag in his home directory:



Picture 8 - Privilege escalation and root flag