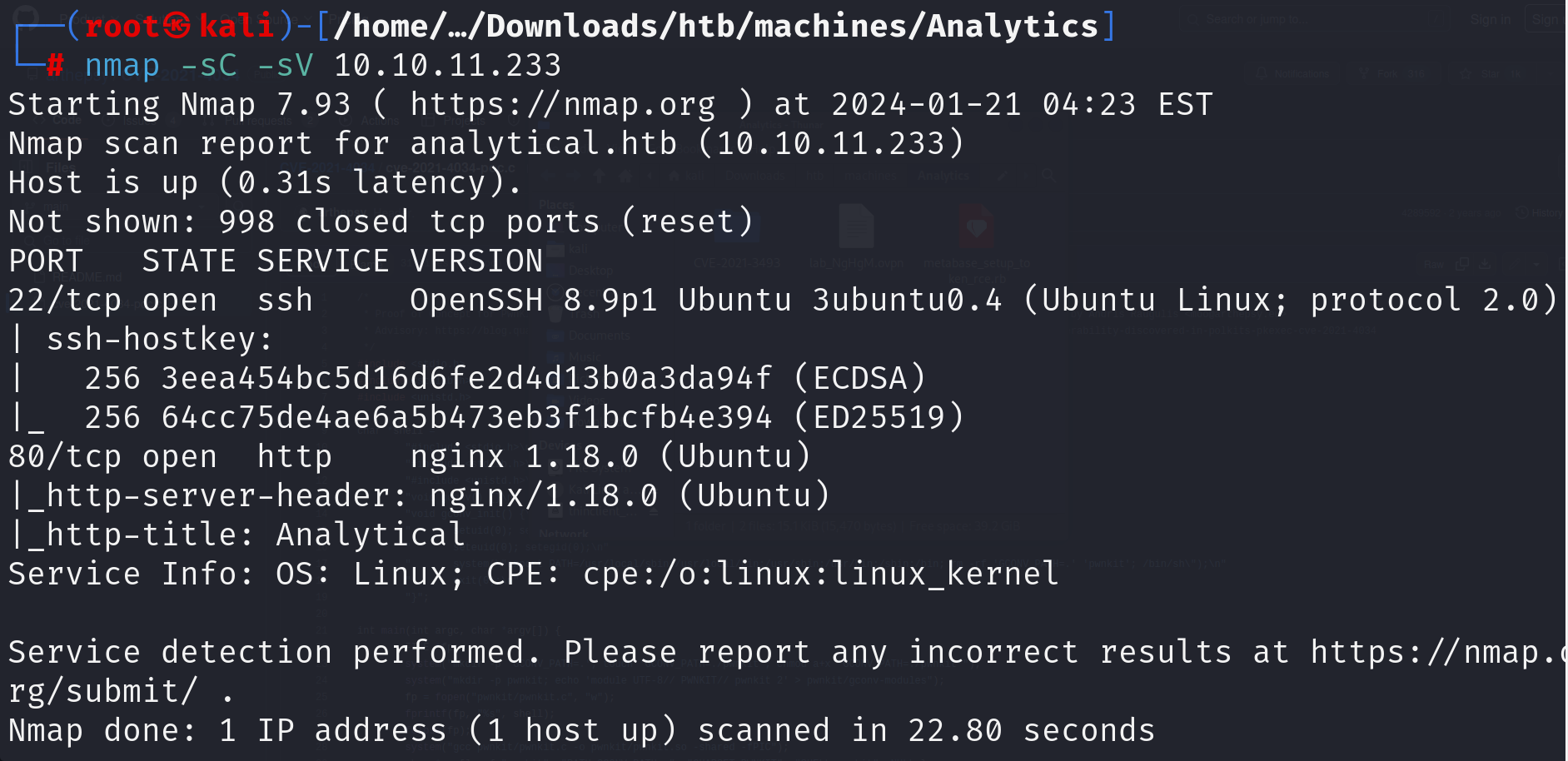
**WRITE-UPS FOR Analytics –** *solve on 01/21/2024*

1. **Metabase Exploitation (CVE-2023-38646)**

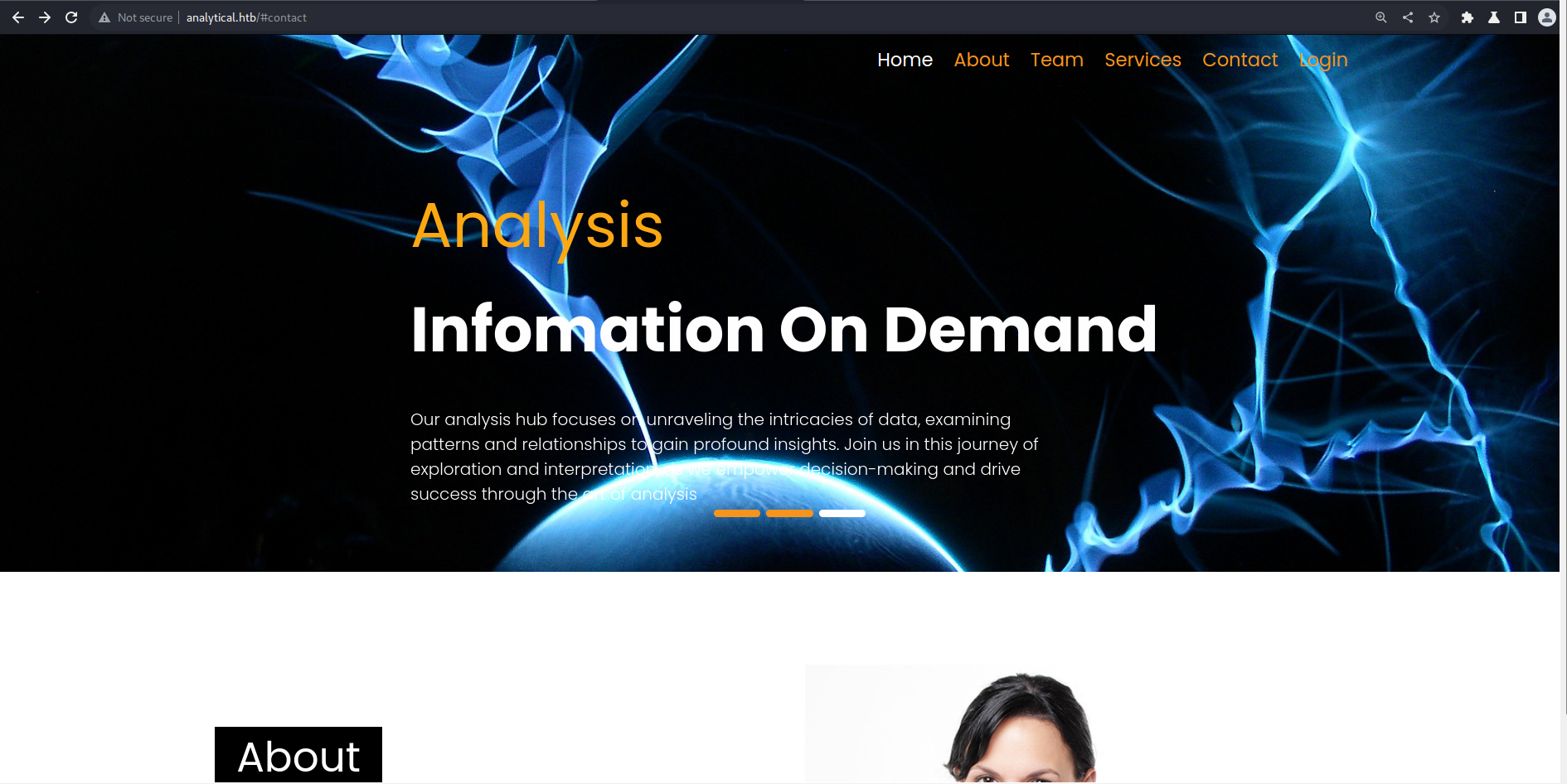
First, we use nmap to scan for open ports.



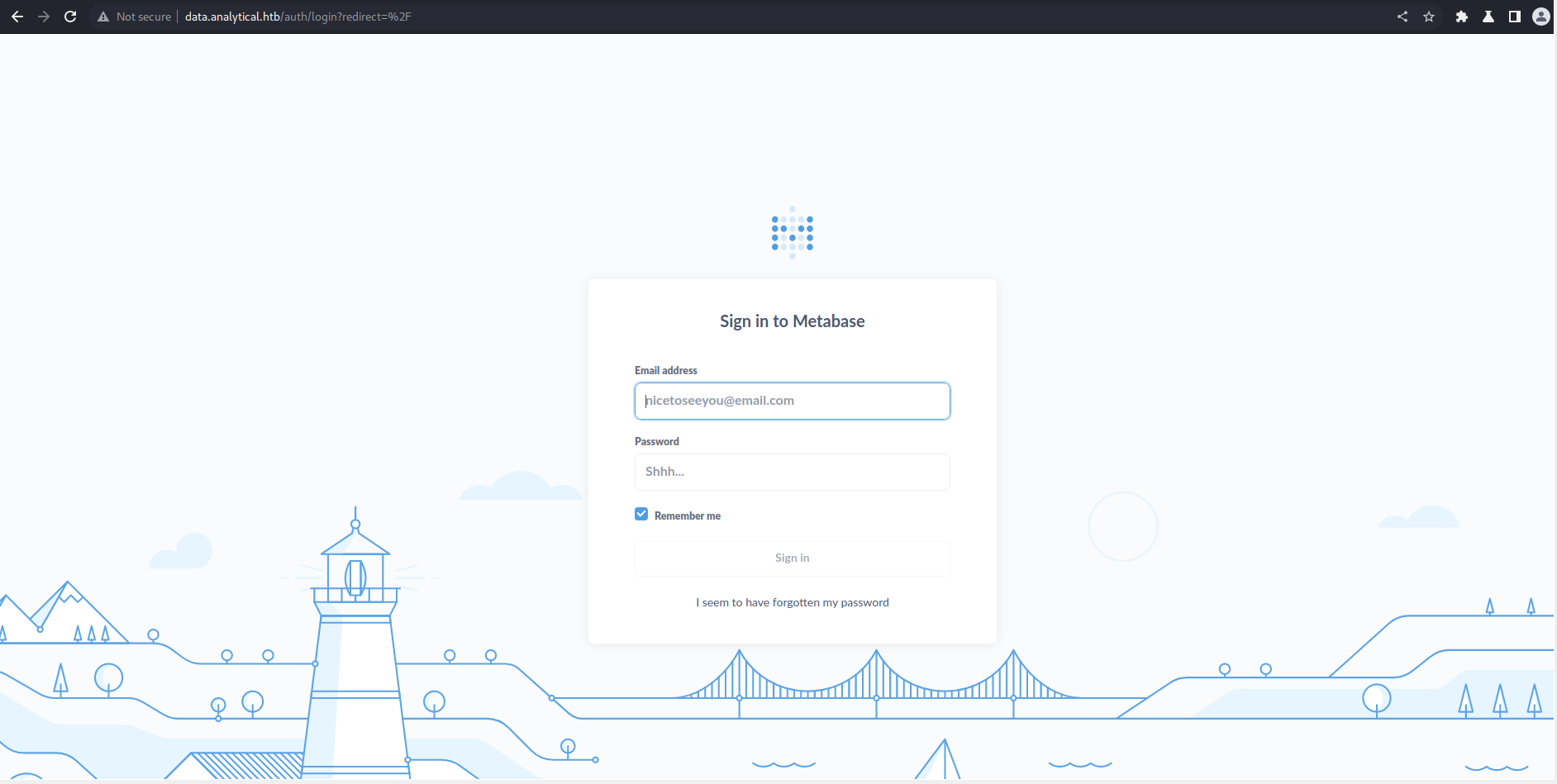
Alright, lets right the domain of the target to our /etc/hosts file



Try to look around the website. Find nothing ☹. Obviously the form doesn’t help as it targets nowhere.



Luckily, there’s a login page. Let’s try a few SQL injections, but nothing really can be done. So we turn to google to find some vulnerabilities of the *Metabase.*



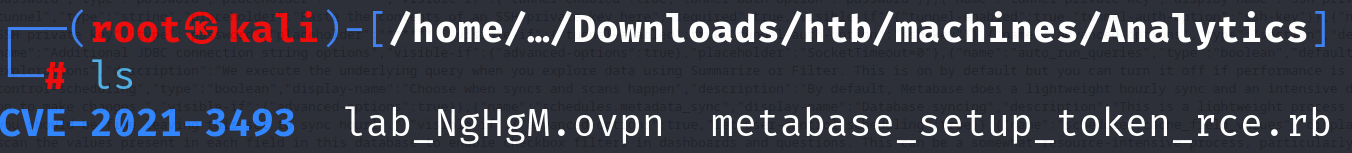
*GOT IT!!!*

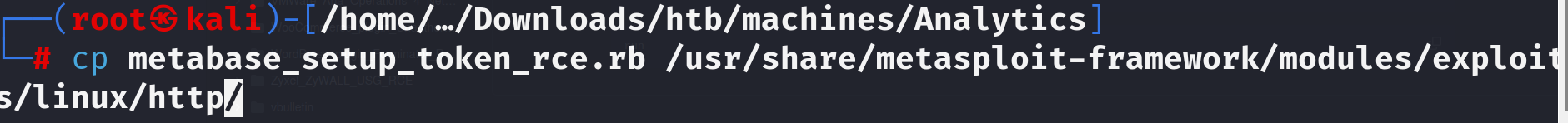
**CVE-2023-38646**

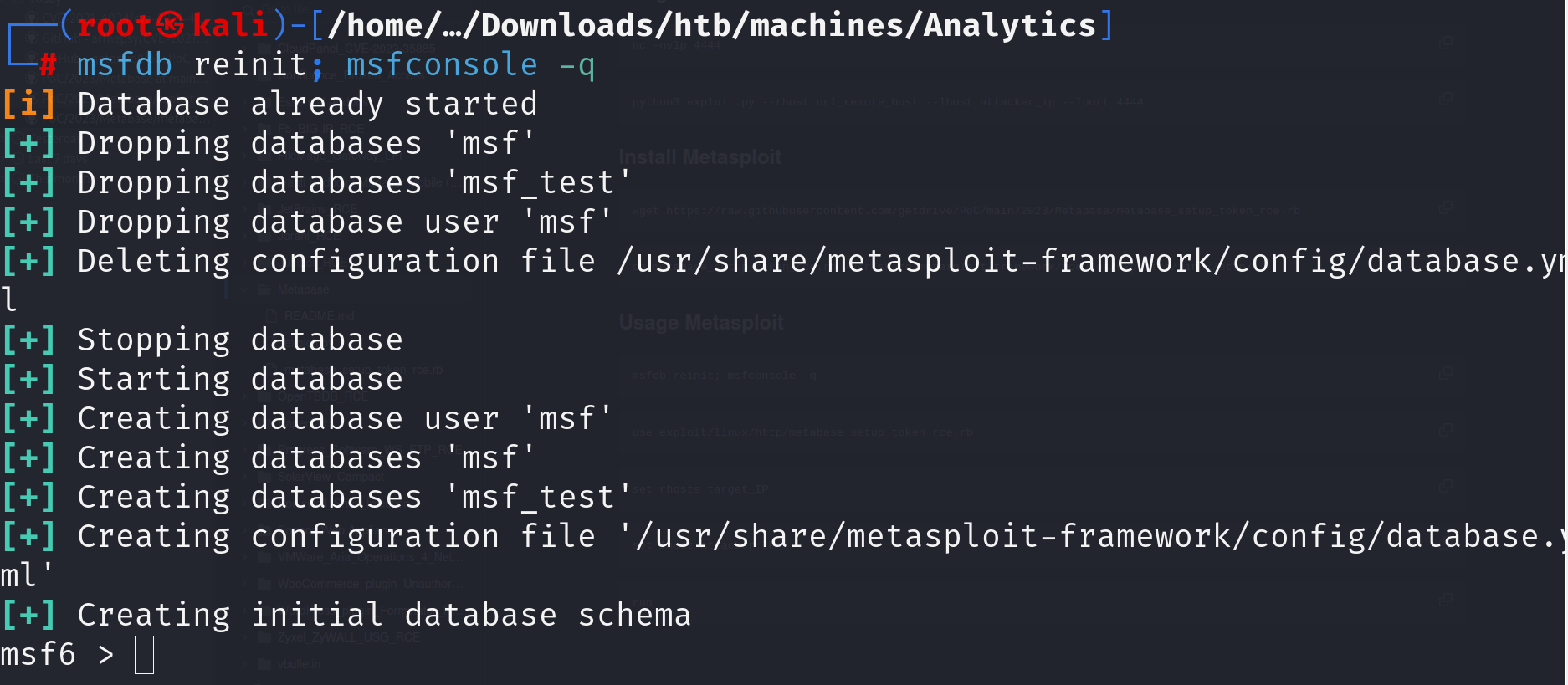
<https://github.com/getdrive/PoC/tree/main/2023/Metabase>

Now let’s follow the instruction to exploit Metabase =))







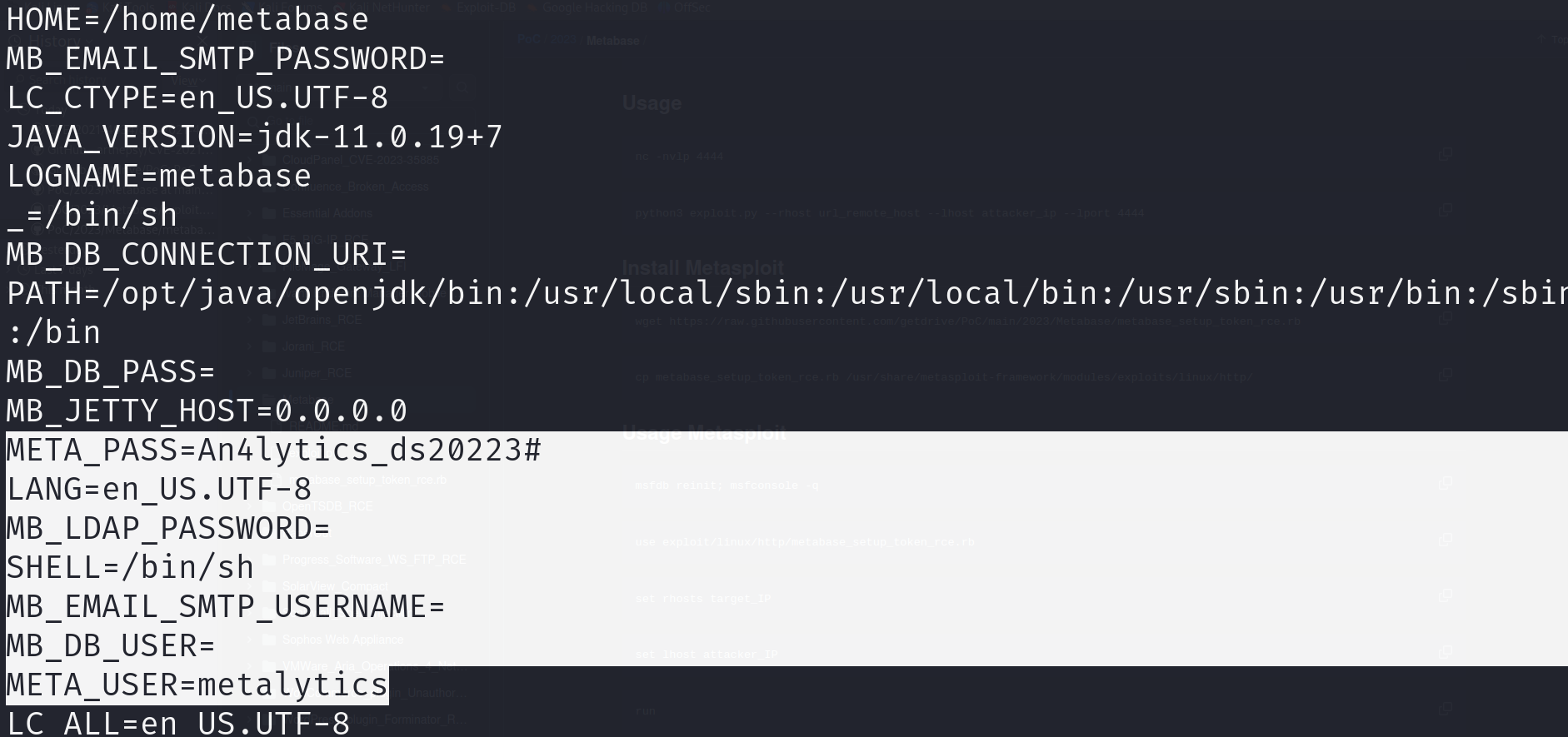




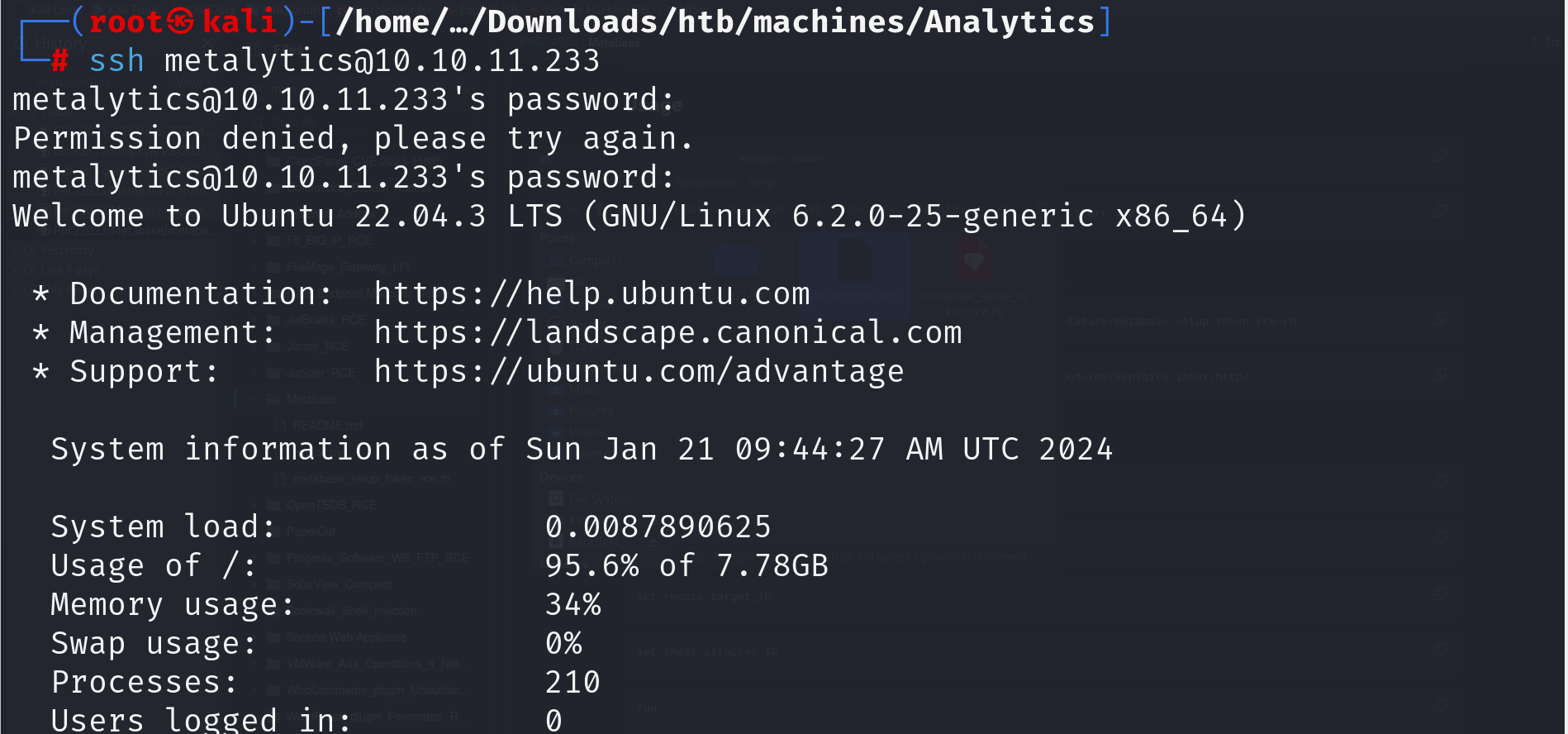
Now we’ve successfully got the reverse shell as user metabase. Unfortunately, after looking a around for a while, we cannot find anything useful. Don’t worry, let’s try to see if environment variables contain anything.



And hurrayyy, a username and a password



Use it to connect to server using ssh



And now the ***user flag*** is in our hand. Congratulation!!!



1. **Privilege Escalation**

To know more about the machine, try to get the version of it. Search the web to find whether any vulnerability of it. And luckily, I found one.

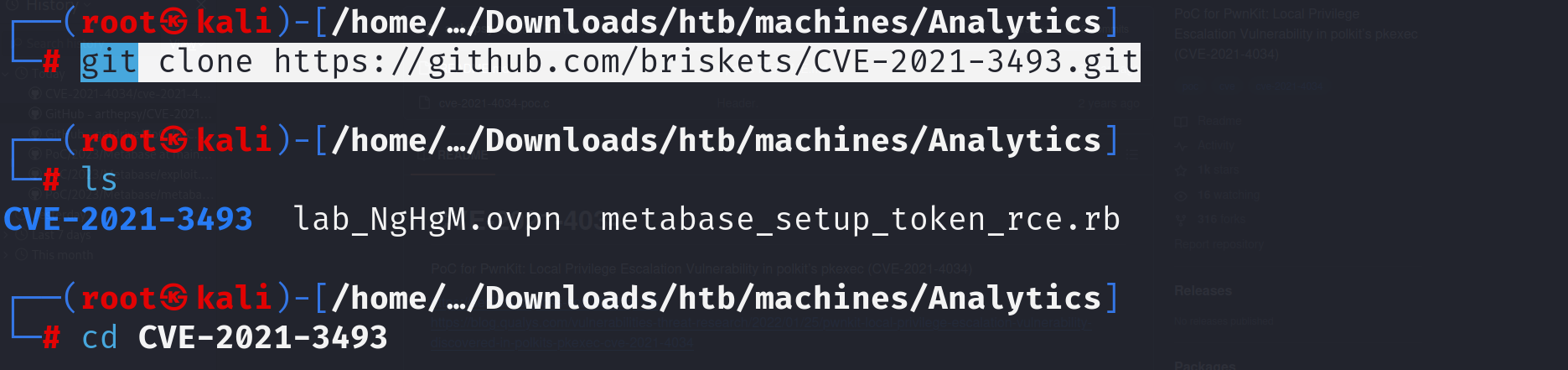


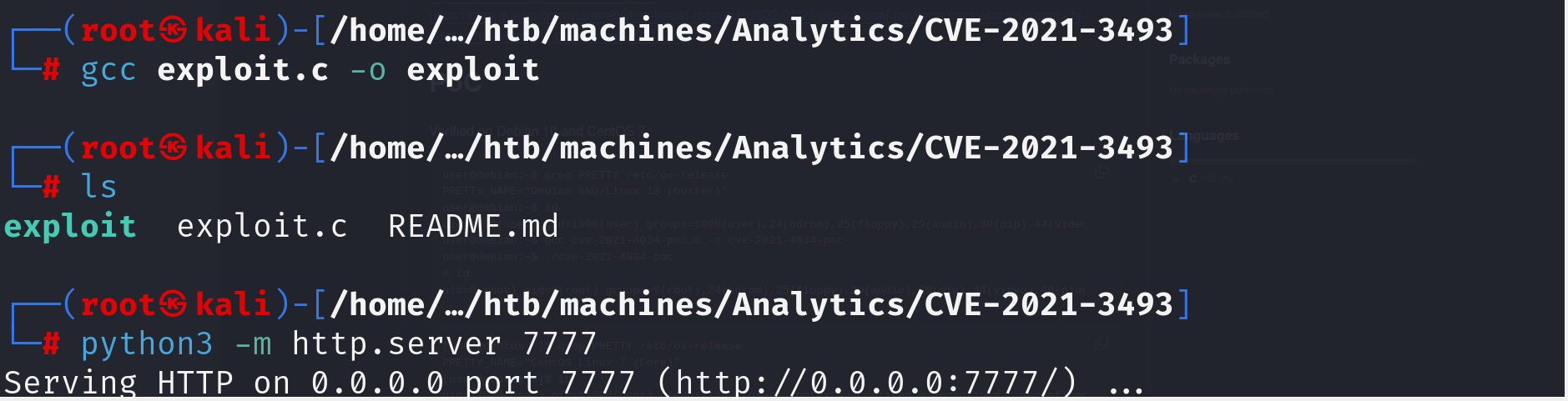
**CVE-2021-3493**

[briskets/CVE-2021-3493: Ubuntu OverlayFS Local Privesc (github.com)](https://github.com/briskets/CVE-2021-3493?source=post_page-----bd3421cba76d--------------------------------)

The last part is trivial.

* Download *exploit.c*
* Compile it with *gcc*
* Open a web server for the victim to connect to
* Download the *exploit* file to the victim machine







On the victim machine, we’ll try:

* Give the execute rule for the *exploit* file
* Execute *exploit*

And yeahh, as expected, we have the root privilege of the machine. All things done!!!



1. **Conclusion**

* Use *CVE-2023-38646* get the reverse shell
* Try looking at the environment variables of the system => username and password
* Connect to the system through ssh => *user.txt*
* Get the ubuntu version and find the vulnerabilities => *CVE-2021-3493*
* Set up a server to transfer file between the attacker and the victim
* Do as the exploitation documentation and get the root privilege => *root.txt*