1. **Introduction**

* Ethical hacking is the process of trying to find vulnerabilities in the system that the customer requests. As the hacker conducts such an attack, they must follow ethical rules and if they fail to do so, they will have to face consequences. This means that hackers should not try to break and breach a network just because they can, they should not try to steal personal data for personal gain. For example, if a hacker gives a task to try to attack in a bank server to find security hole to patch, after the attack, he writes a report about the hack and send it to the bank, but he has stolen the information of customers of the bank use it to sell for financial gain. Such crime will be punished with a large amount of money or even worse, many years in jail (Meredith, D. (n.d.). *Ethics in hacking*). So as an ethical hacker, we must all consider the ethic in it and try to make it as successful as possible by following 5 phases: Reconnaissance, Scanning, Gaining Access, Maintaining Access, Clearing Track.

1. **Reconnaissance**:

* To begin a penetration test, a hacker often starts with footprint the system and finds out as much information about the victim system as possible. This information includes what the organization requests, the configuration of the victim machine, the network and login information. To be more specific, what hacker documents to the conduce the attack are:
  + Naming conventions
  + Services on the network
  + Servers handling workloads in the network
  + IP Address
  + Name and login credentials of users connected to the network.
  + The physical location of the target machine

(www.linkedin.com. (n.d.). *The Art of Reconnaissance in Ethical Hacking: Unveiling the Secrets of Information Gathering*)

* You can perform reconnaissance either by active or passive.

Active reconnaissance is the process of directly interacting with the victim computer system to gain information with a high risk of being detected by the system admin (Tutorialspoint.com. (2019). *Ethical Hacking - Reconnaissance - Tutorialspoint*).

Passive reconnaissance is about gathering information without interacting with the victim machine and this reduces the risk of being caught by the system admin (Tutorialspoint.com. (2019). *Ethical Hacking - Reconnaissance - Tutorialspoint*).

* There are a few tools that can help hacker conduce reconnaissance more effectively, some of these tools are:
* Google
* Maltego CE
* FireCompass
* Recon-NG
* Shodan
* Censys
* nMap
* Spiderfoot
* Datasploit

1. **Scanning:**

* After finishing the footing process, the ethical hacker will begin to test the potential attack surfaces of the network and machine of the victims. To accomplish this, it is recommended to use automated scanning tools to gather details of all machines, users, and services within the network. In the process of scanning, there are typically 3 types of scans:
* Network Mapping:

This method is used to get the network topology, which includes host information, servers, routers, and firewall within the host network.

* Port Scanning:

Port scan is to find open ports on the network by using automated tool. This is an effective way to enumerate the services and live systems in a network and establishing connection with these components.

* Vulnerability Scanning:

Like port scan, vulnerability scan is to identify system weakness that can be exploited to conduct an attack using automated tool.

(www.linkedin.com. (n.d.). *The Art of Reconnaissance in Ethical Hacking: Unveiling the Secrets of Information Gathering*)

* To able to process with the scanning phase, hacker often use these techniques:
* TCP connect scan.
* TCP syn port scan
* Network Scanning
* Vulnerability Scanning
* There are 2 types of scanning a hacker can do, either active scanning or passive scanning. Passive scanning is a type of network scan that does not involve directly interacting with the network but tries to find information that is already available. Unlike passive scanning, active scanning is all about interacting with the victim network or machine to gather the information needed for conducting attacks (GeeksforGeeks. (2022). *What are Scanning Attacks?* ).
* There are many tools available for the scanning phase, here are a few popular and commonly used one:
* Nmap
* Nikto
* Nessus
* SNMP Sweepers
* Ping sweeps
* Network mappers
* Vulnerability scanners

(FireCompass (2020). *Top 10 Tools for Reconnaissance*)

1. **Gaining Access:**

* After hackers have gathered enough information thought the 2 first phases, they will begin to attempt exploiting this information for administration access. To be able to gain access to the victim system, hackers send a malicious payload through the network, an adjacent subnet, or physically using a connected network. There many ways a hacker can gain the access of the victim system, here are some of the more popular techniques that hacker use:
* Buffer overflows: This attack is caused by sending a large amount of data correctly by the CPU, which causes the CPU to overflow and redirect the return address. By using this vulnerability, hackers can call the malicious payload they inject in the CPU or use gadget that is in the CPU with the ROP attack.
* Phishing: Is a type of Social Engineering attack to steal sensitive data such as bank account numbers, username, passwords, and credit card details. Phishing means sending fake email that appears from a legitimate to the victim that contain a malicious payload or a fake login page for the user to put their credentials in (GeeksforGeeks. (2019). *Phishing in Ethical Hacking*).
* Injection attacks: This type of attack allows the attacker to inject a malicious code into the victims’ system or service such as website or program, this code then will be executed remotely to change or get data (IBM (2013). *Injection Attacks*).

If these attacks were successful, the attacker can take control of the victim system and may use further attacks such as data breaches and Distributed Denial of Service (www.linkedin.com. (n.d.). *The Art of Reconnaissance in Ethical Hacking: Unveiling the Secrets of Information Gathering*).

1. **Maintaining Access:**

Before the last phase of ethical hacking, attackers must be able to maintain access to the system, this will help hackers to find more vulnerabilities in the future. This can be achieved by either installing software or making changes in the target system, this helps hacker can be continuous from where they left it and not have to redo the whole process from scratches(www.linkedin.com. (n.d.). *The Art of Reconnaissance in Ethical Hacking: Unveiling the Secrets of Information Gathering*).

* For hacker to maintain their access, these tools are often use:
* pwnat
* weevely
* powersploit
* sbd

(GeeksforGeeks. (2023). *Maintaining Access Tools in Kali Linux*)

1. **Clearing Tracks:**

* After completing the attack on the target system and had discover all of vulnerabilities that it has, the final task for the hacker is not to be discover be clearing their track. These include:
* Uninstalling scripts/applications used to carry the attack.
* Modifying register values
* Clearing logs
* Deleting folders created during the attack.

(www.linkedin.com. (n.d.). *The Art of Reconnaissance in Ethical Hacking: Unveiling the Secrets of Information Gathering*)

1. **Conclusion:**

* In conclusion, to be able to perform ethical hacking as successfully as possible, hackers need to follow the 5 phases about. After finishing the 5 phases then hacker must write a report document on the vulnerabilities that they found and suggesting solutions/advice to patch those holes in the system. To be able to understand more clearly about these phases, I will demo an attack to a machine called Nibbles in hackthebox website.

1. **Demo:**

To start the attack, I will combine the 2 first phase into 1, which is enumeration. First, I will Nmap to find which port the ip is open with the command.



Figure 1: nmap command

By using –sV, I can see the open port in top 1000 port and –sC for default scrip and here is the result:

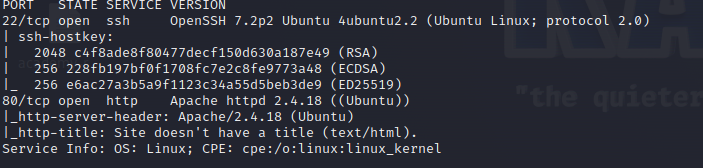


Figure 2: nmap result

Looking at the result we can see that the ip opens at port 22 with ssh service and port 80 with http service. Knowing the ip is running http service, I then use whatweb to identify the web application with the command.

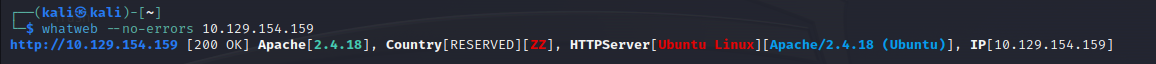


Figure 3: Whatweb result

The result shows the web is running Apache ver 2.4.18 and running Linux OS. Try accessing the ip thought http service in Firefox, I get.

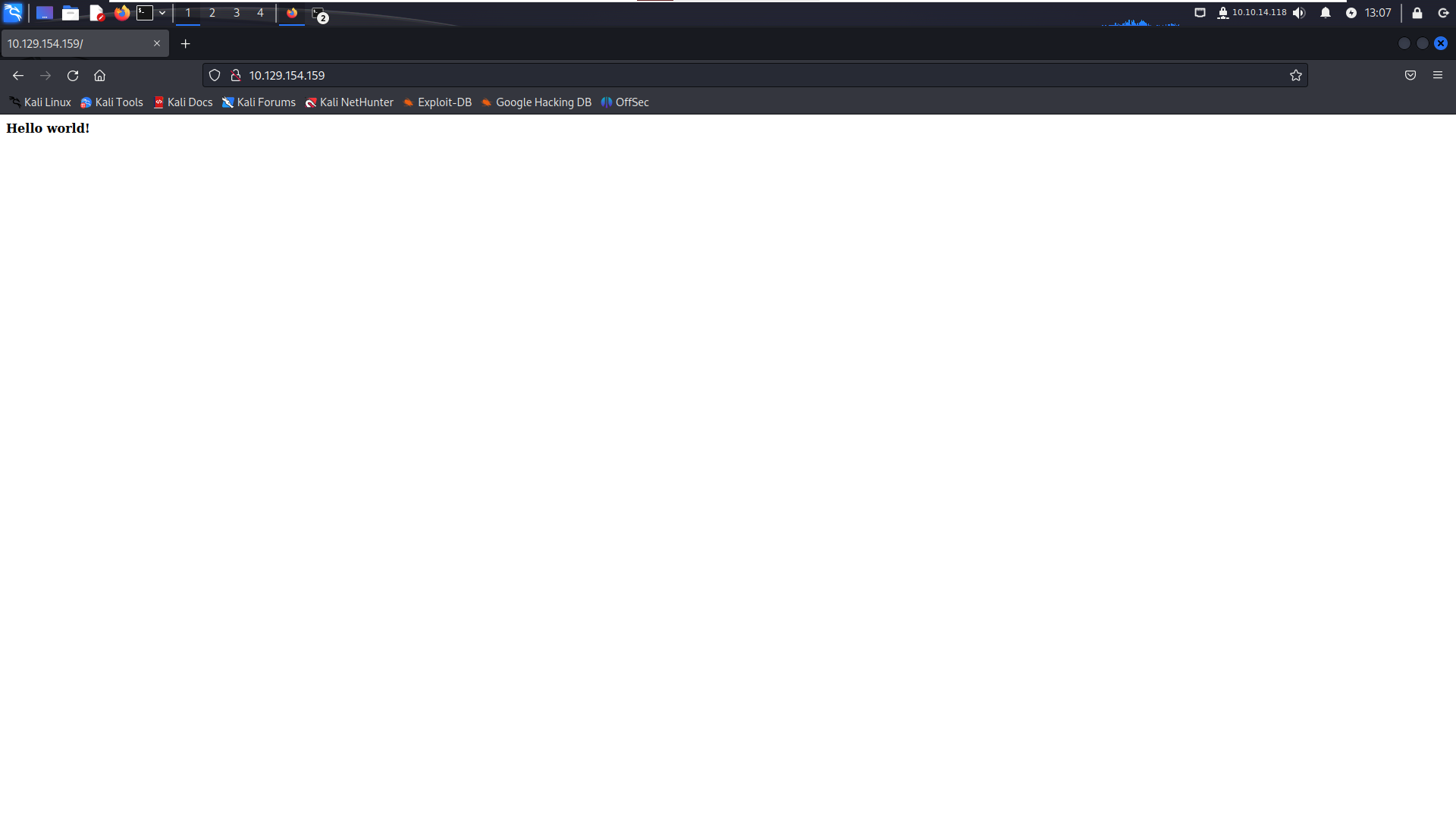


Figure 4: The ip website

Which is just a blank page with the phrase “Hello World!”, for further investigation, I decide to view it source page

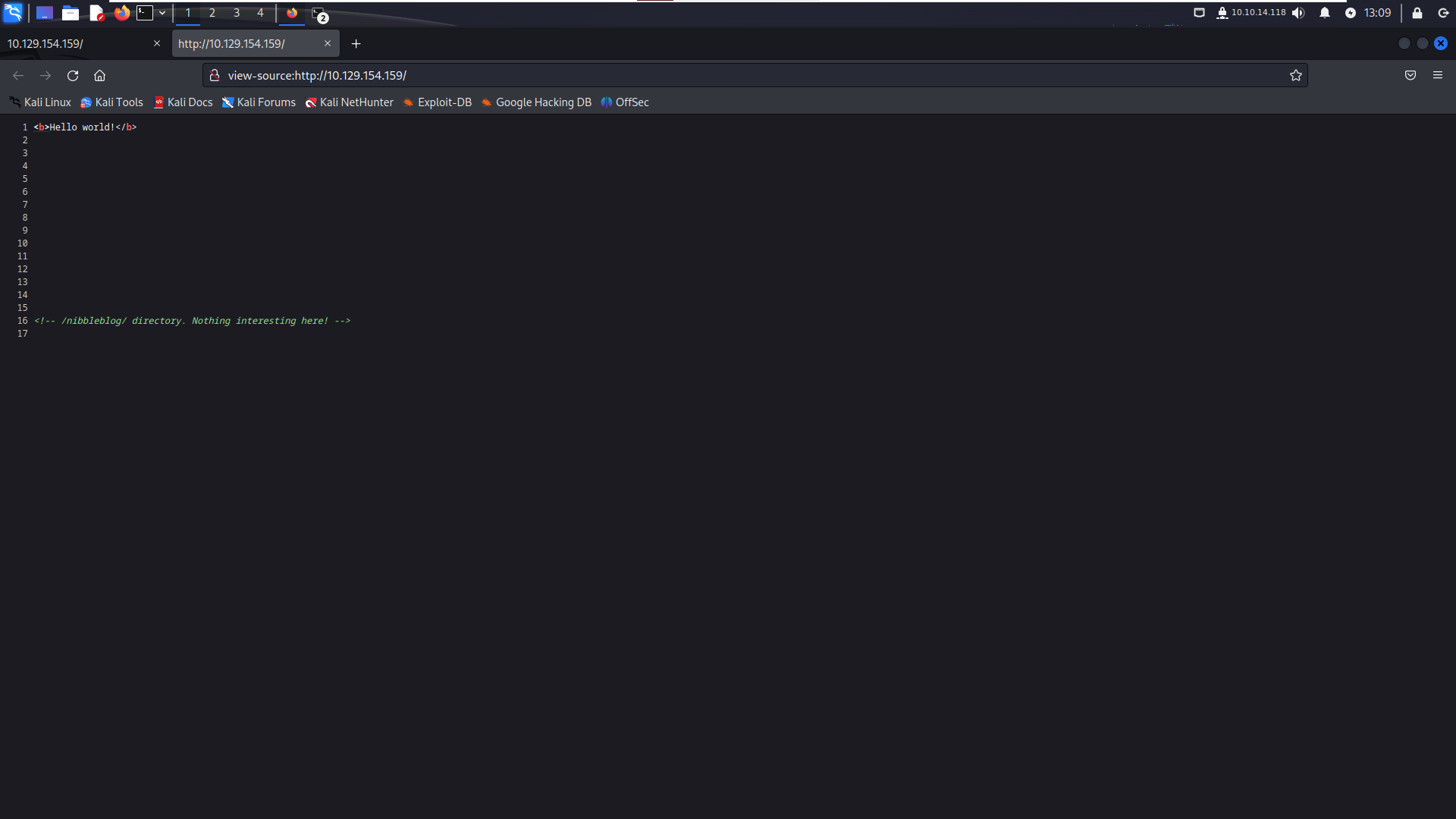


Figure 5: the source page of the website

Looking at this, I can see that the web developer forgot to erase a directory name /nibbleblog/, let try access it.

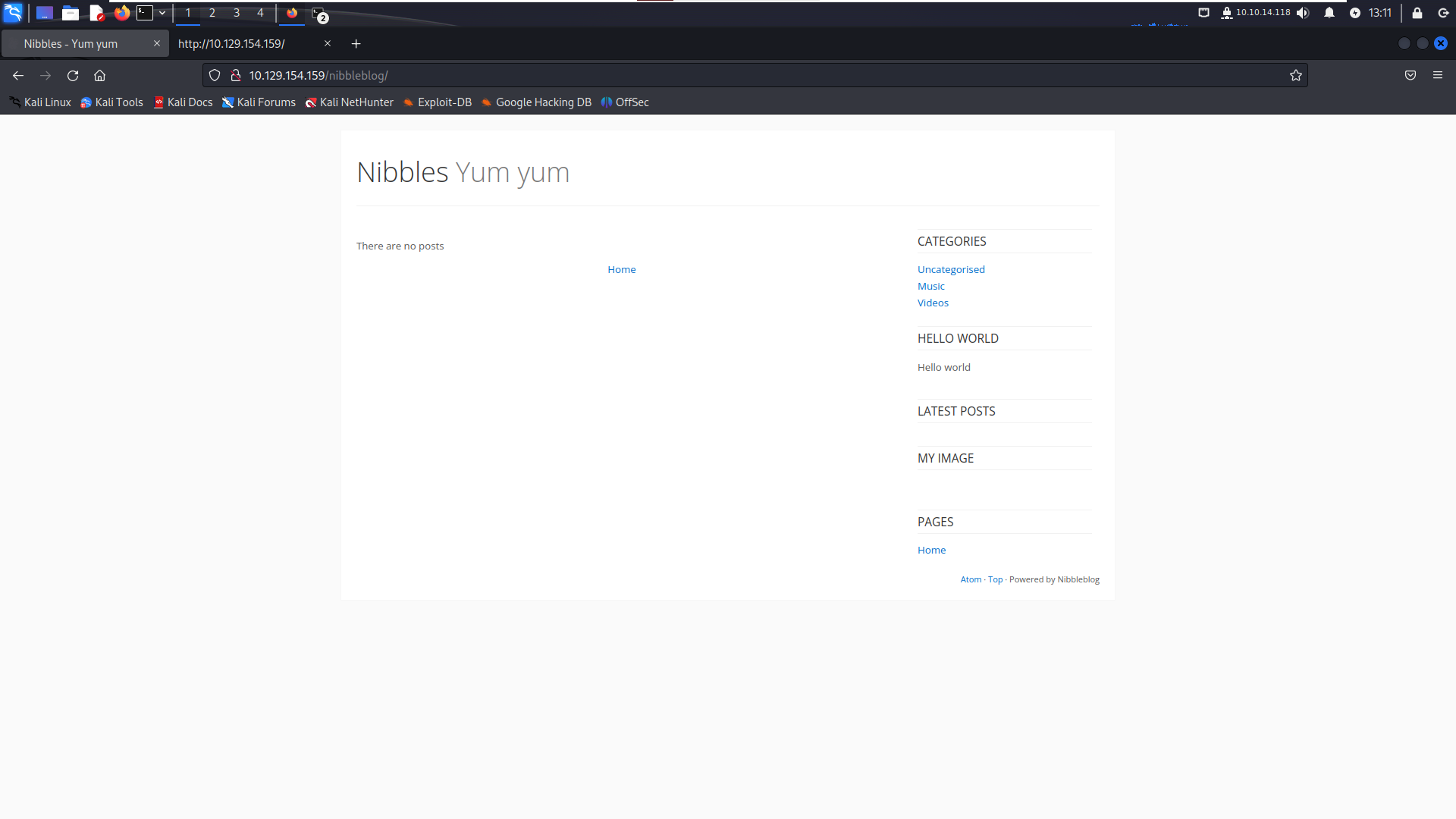


Figure 6: The web with nibbleblog directory

By entering the directory, we enter the web main page, but by the look of it, there litter we can use to attack further. So, to look deeper into this, I try to find any other directory that the web has with gobuster.



Figure 7: the gobuster result

Using gobuster, I enter the common.txt word list that include in SecList word list to Bruce force the web in DIR mode to find all its directory that fit the word list, 3 directories that interest me is admin.php, content, admin. Accessing the admin.php directory bring me to the login page.

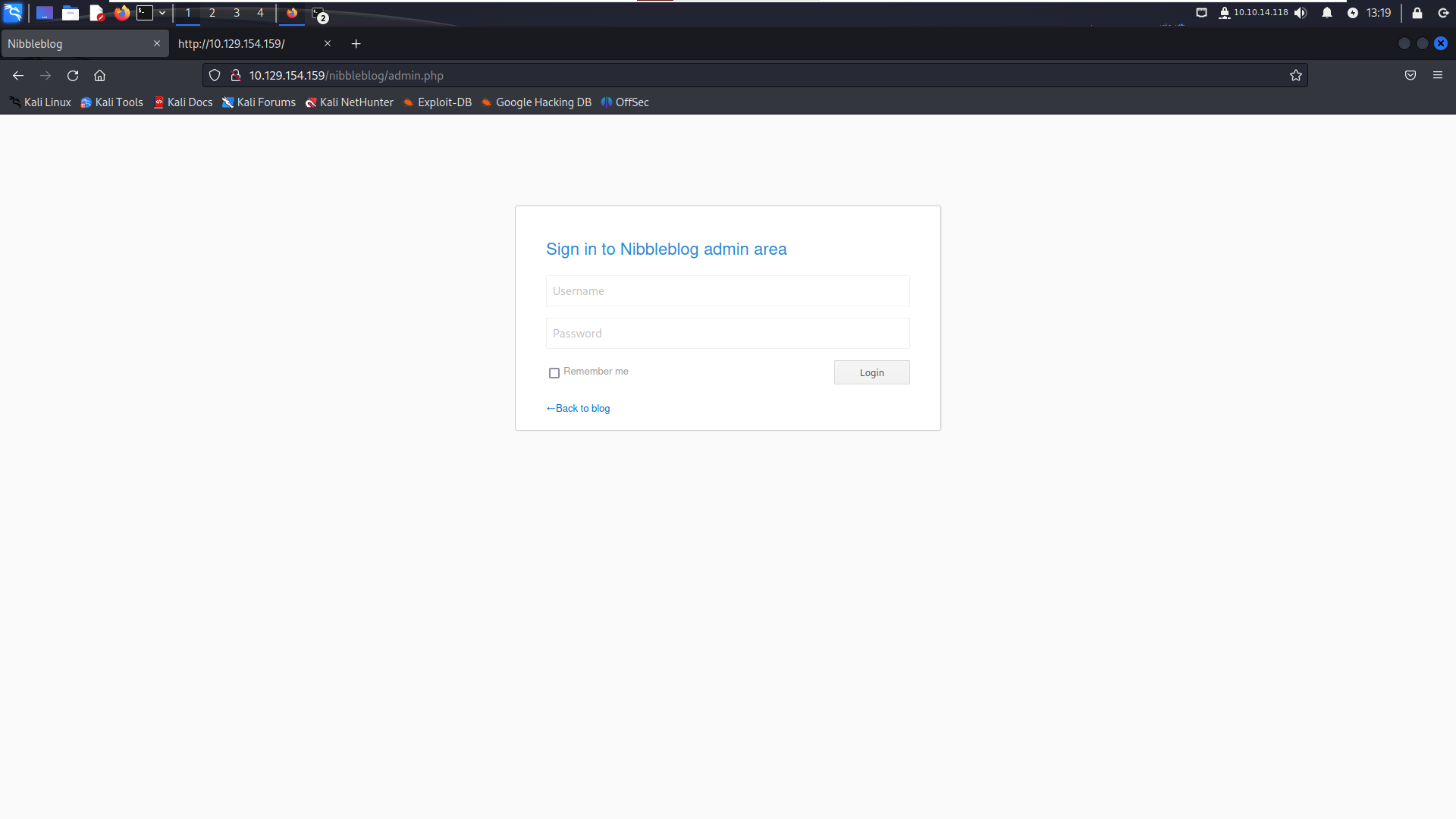


Figure 8: The admin login page

Now to able to get in, I can either by guessing or Bruce forces the way in, but I will try to find information first before try either way. After that I try admin directory

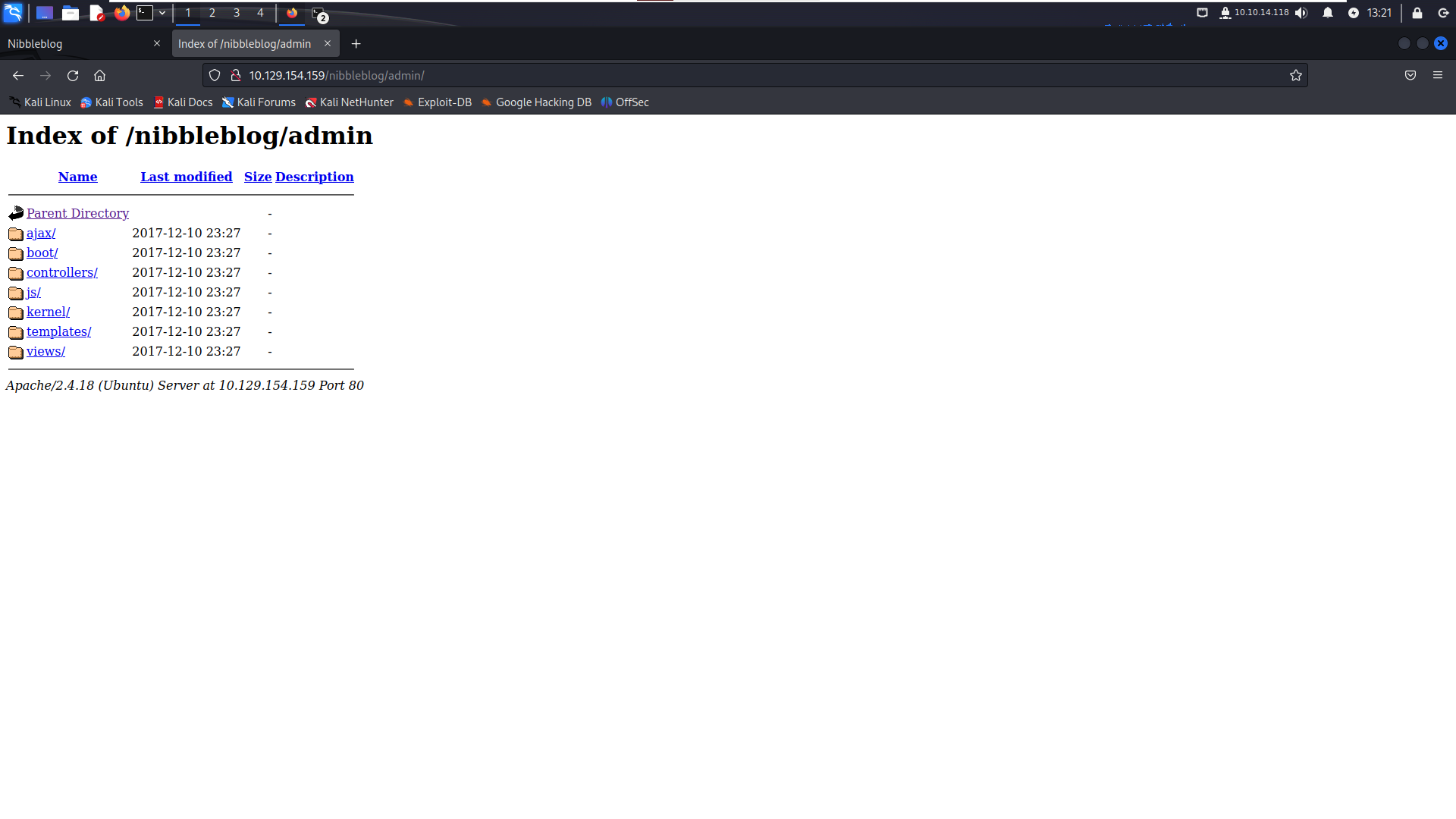


Figure 9: the admin directory

I found nothing really interesting other than the web configure, so I will try content next.

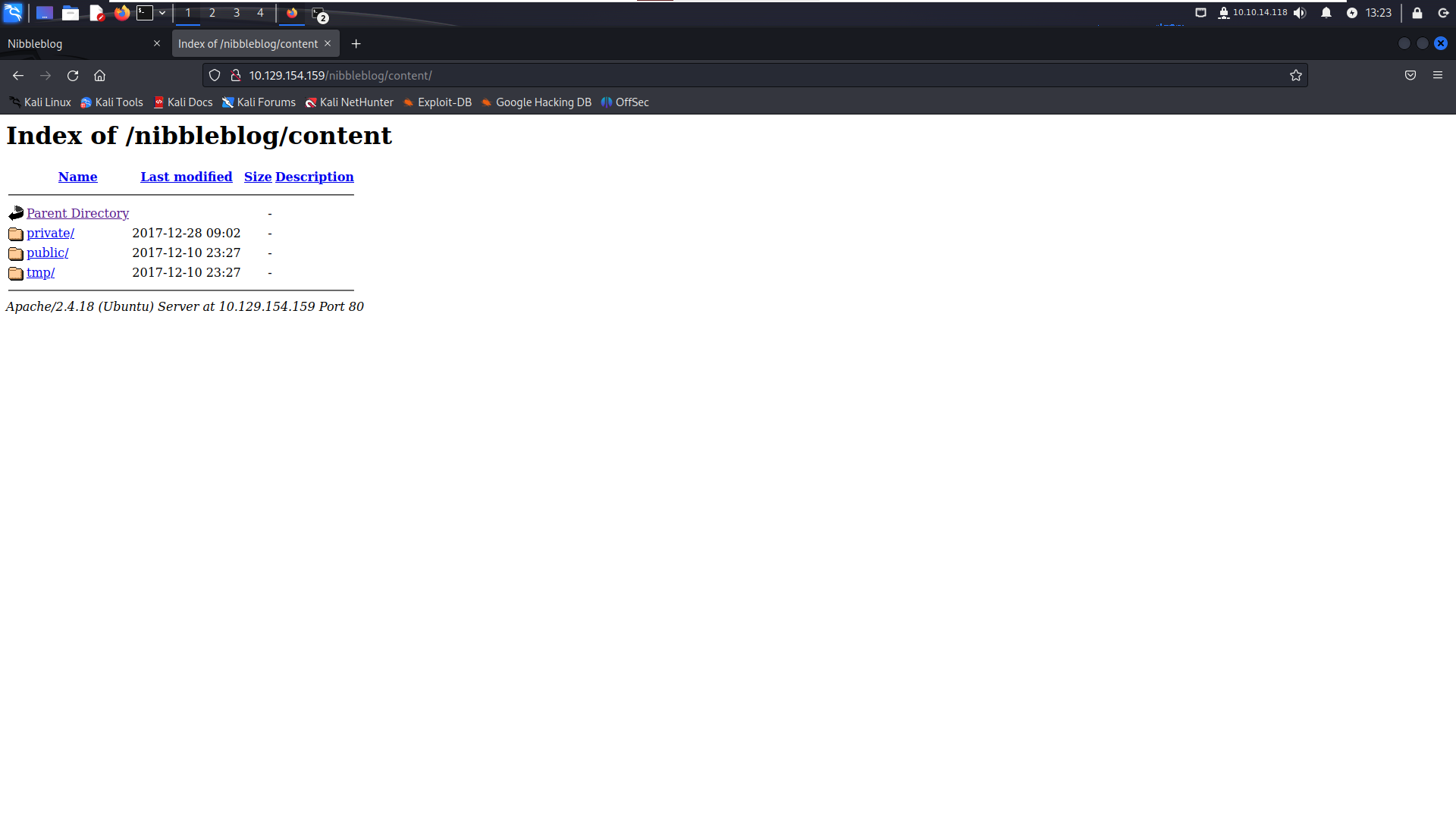
T

Figure 10: the content directory

The private directory seems very interesting, so I try to access it

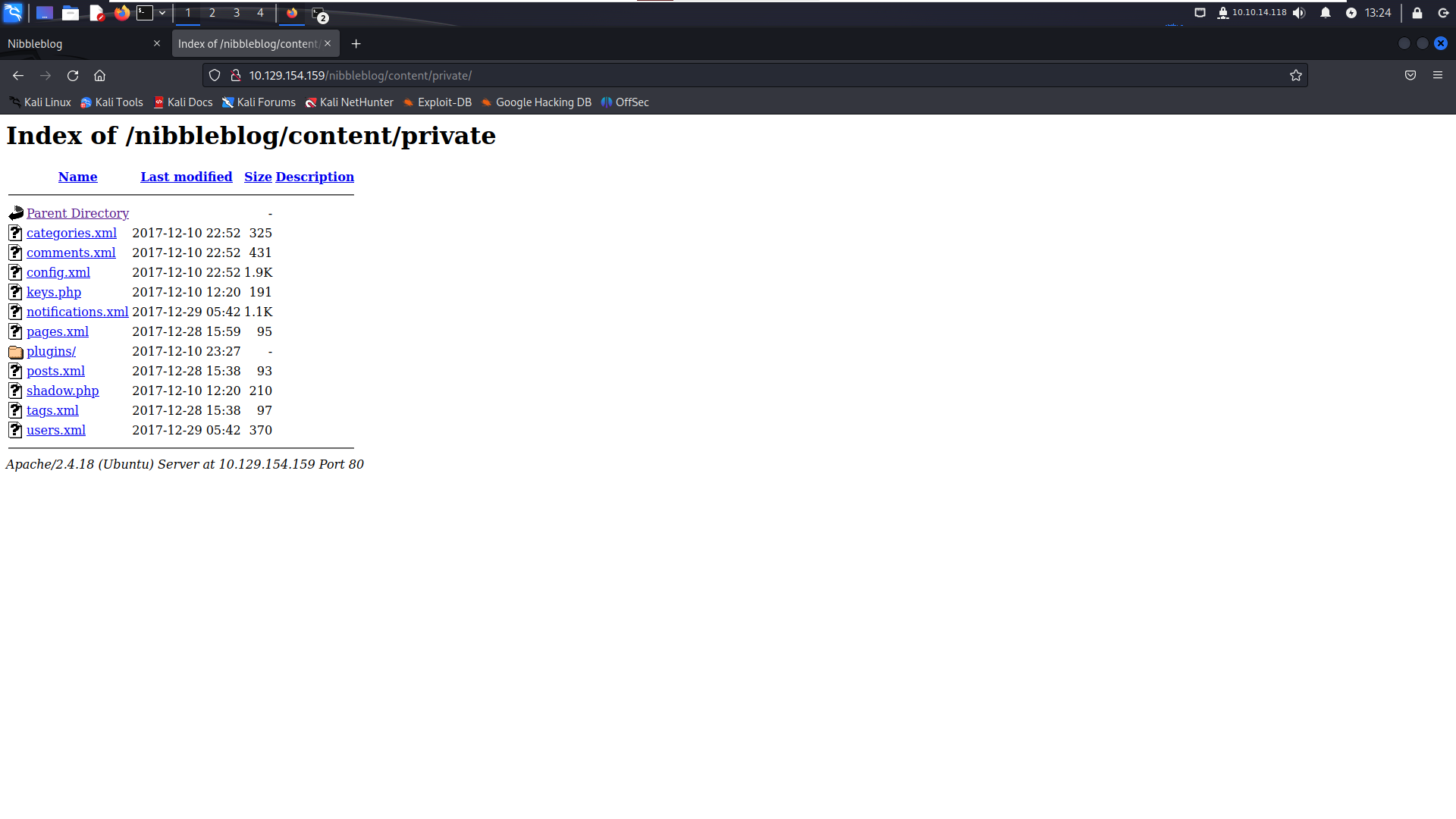


Figure 12: The private directory

The user directory is the one I was looking for and it did show me something interesting.

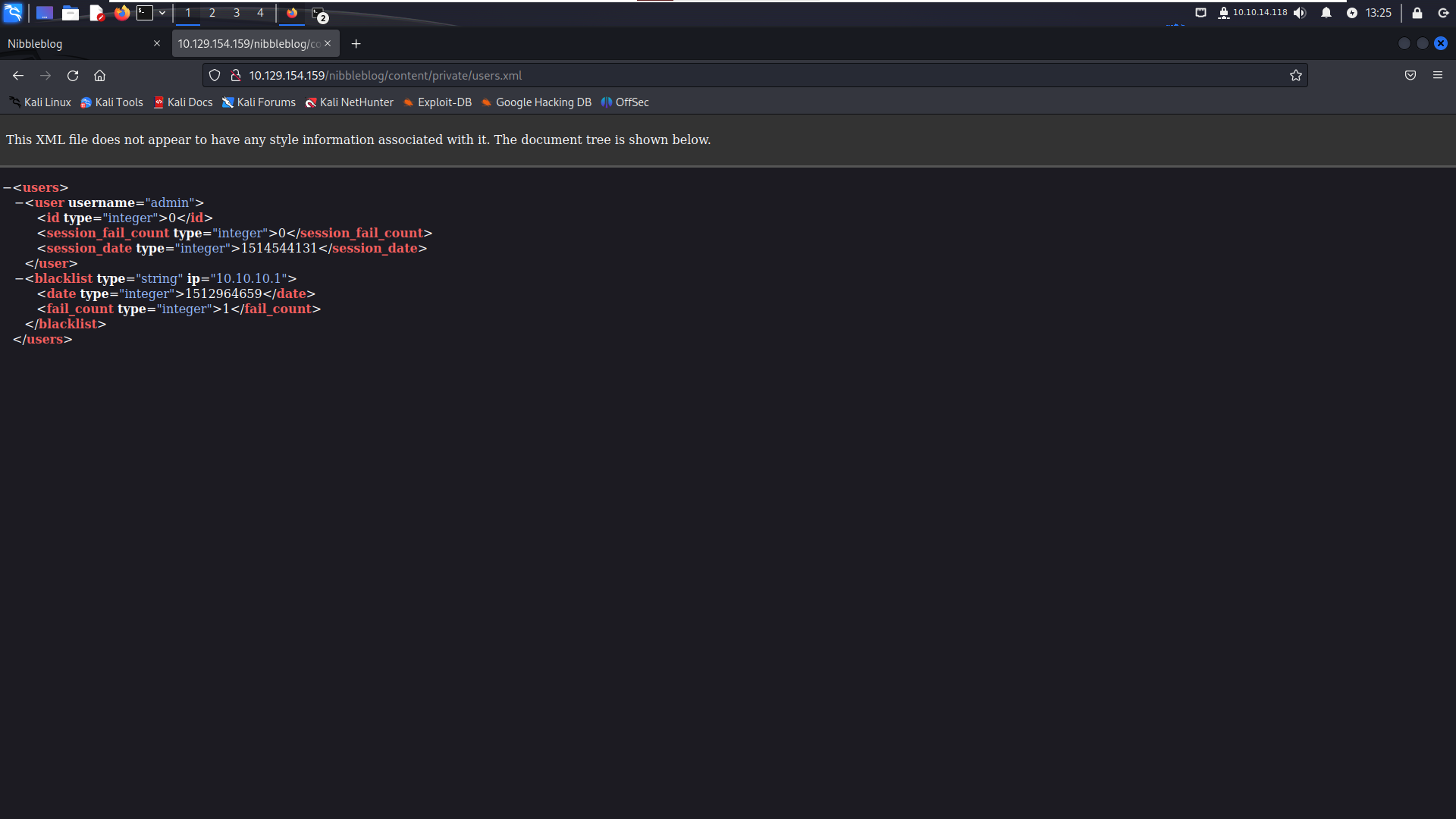


Figure 13: The user file

Now I know the username is admin and it seems like there is a blacklist which will block us from Bruce force. Looking around I find that Nibbles is mentioned twin in the config file and with the web also use nibble, now let begin to start the

“Gaining access” phase.

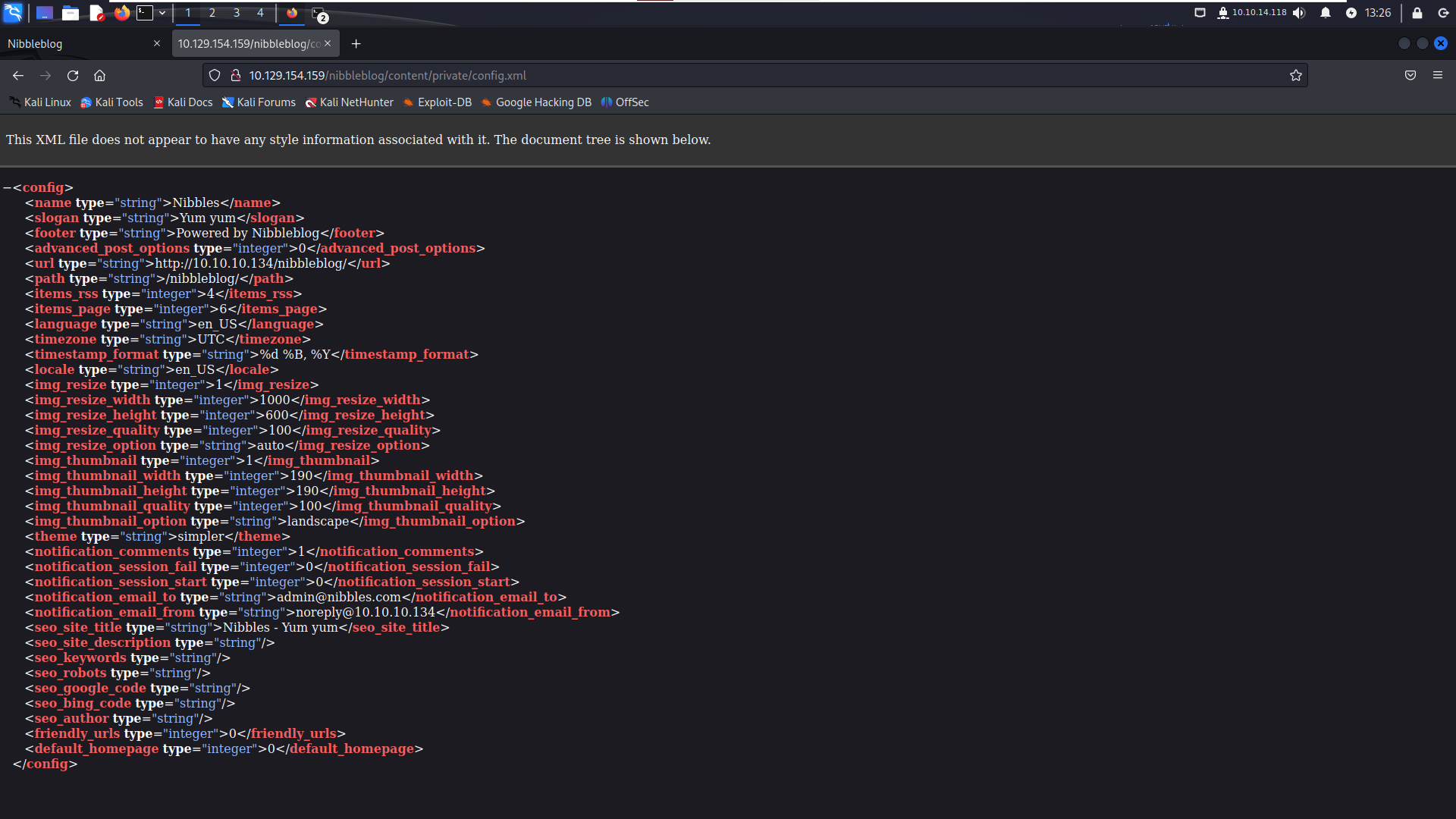


Figure 14: The config file

By entering the username admin and the password nibbles, I gain the admin access.

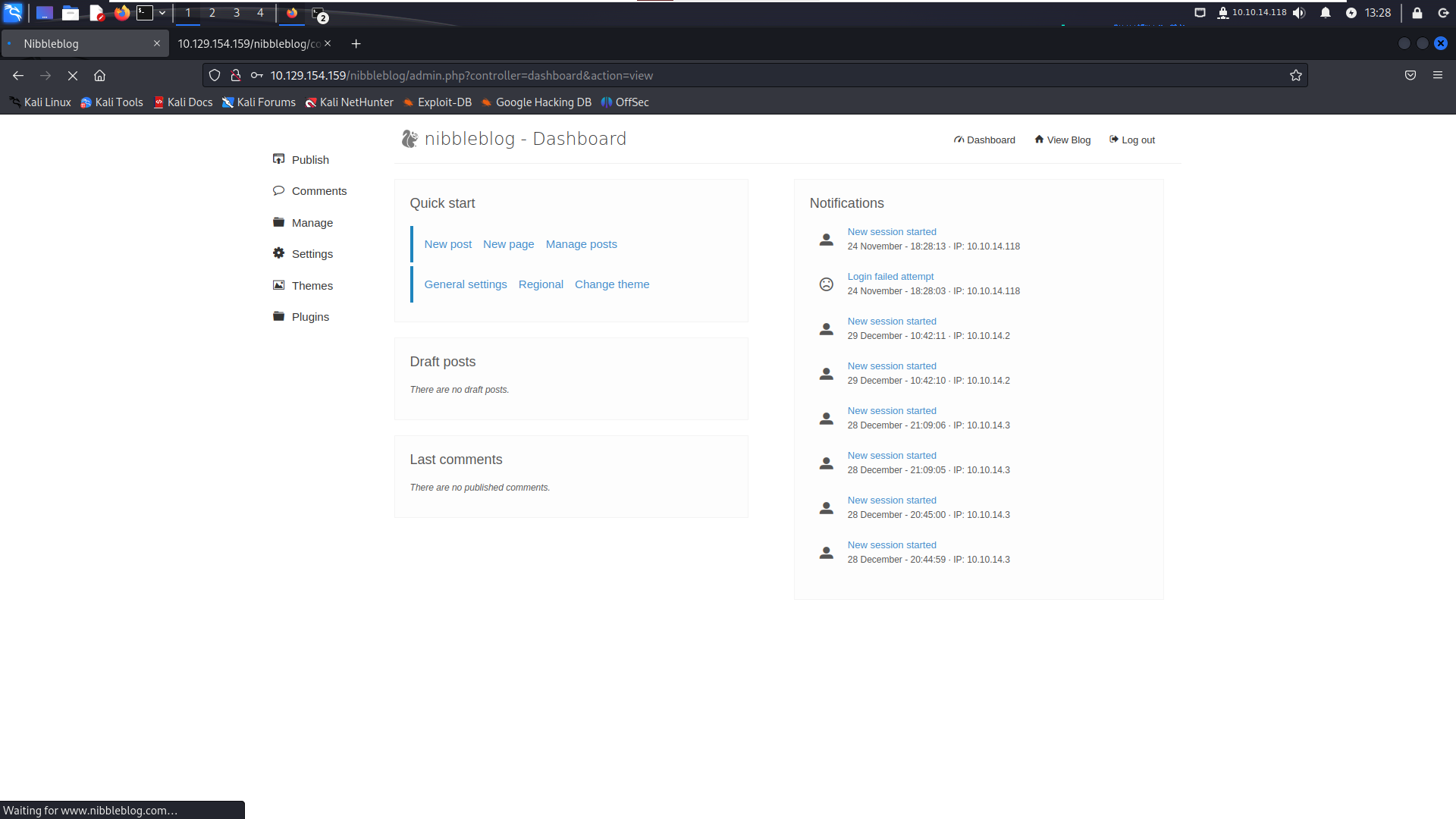


Figure 15: The main page after logging in

Looking around I see that we can upload an image in plugins my picture.

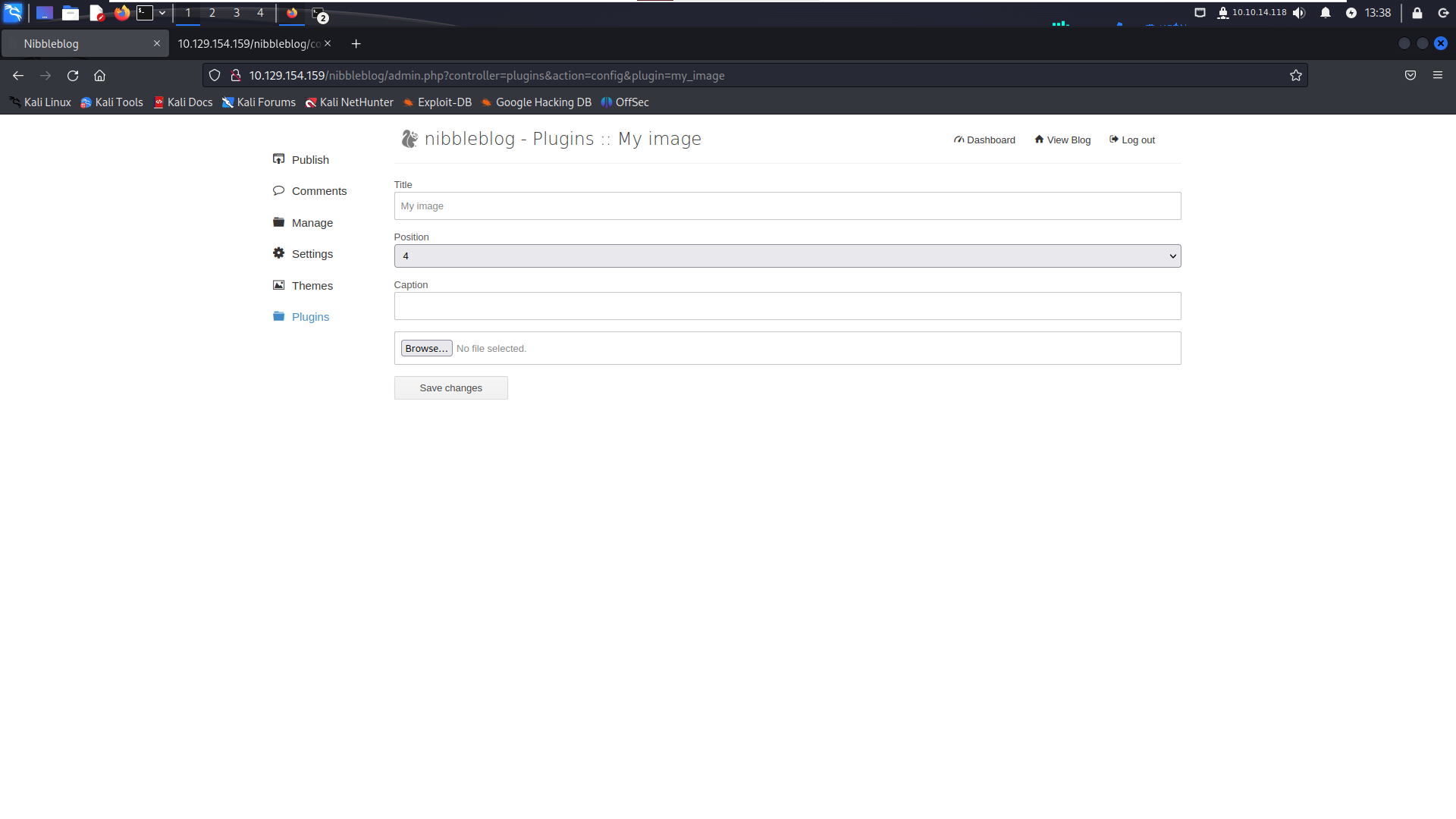


Figure 16: The Plugin page

We can try upload a shell in it, but I will use metasploit for this job.

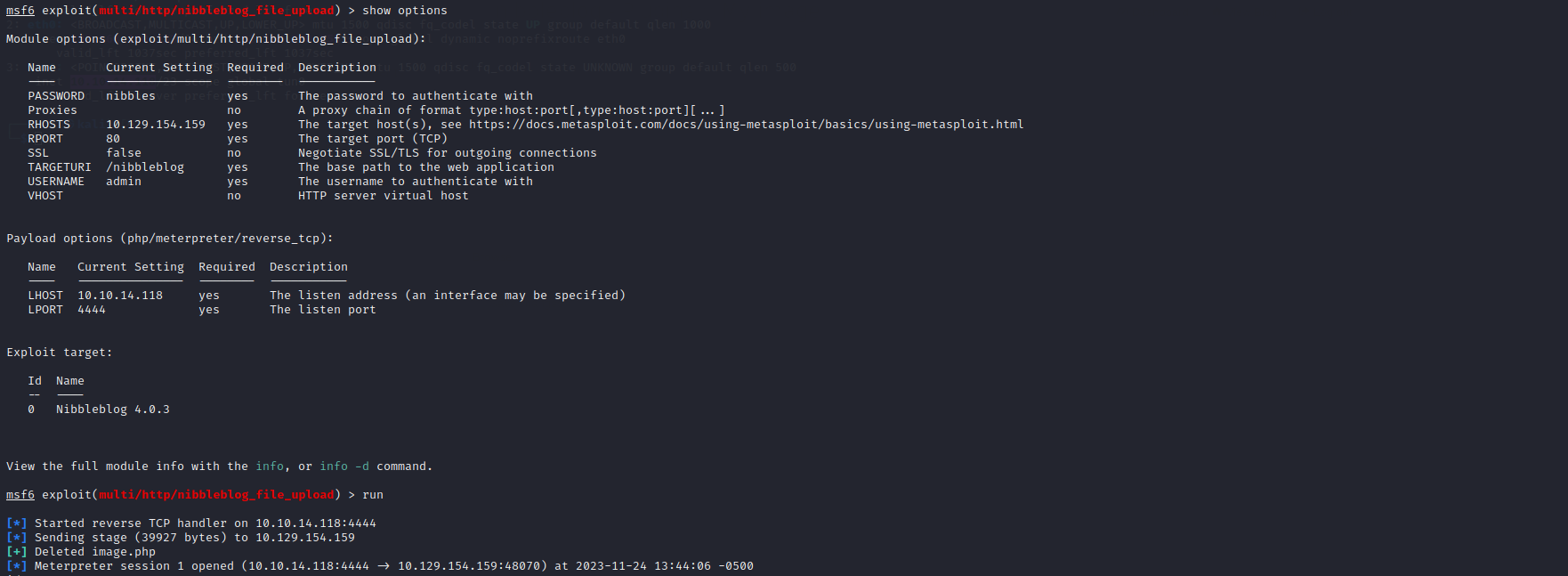


Figure 17: Metasploit options and gaining access

After getting in, searching around I saw monitor.sh has potential for further emulation as it doesn’t need password to execute in sudo -l, to maintain the access, I can install a back door or create an account, but I will not do this for now. Then I echo a shell to the scrip so I can netcat the system



Figure 18: injecting the netcat shell into monitor.sh

After netcat the port I insert, I get the control of the system and get the flag.

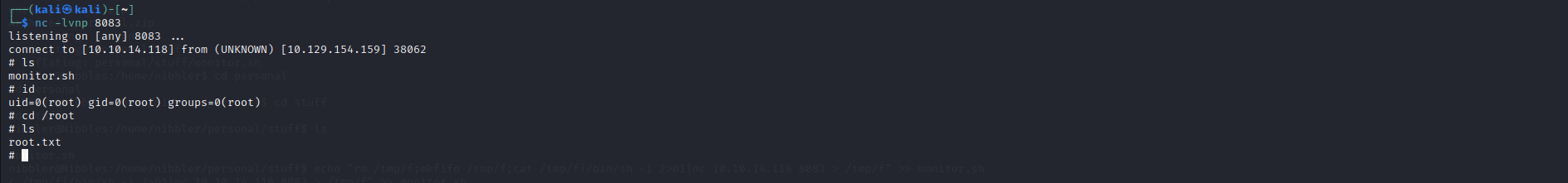


Figure 19: Gain root access and the root.txt location

Then to clear the track I delete the unzip personal file I unzip and clear in Metasploit.

Words Count: 1621

Referee:

GeeksforGeeks. (2022). *What are Scanning Attacks?* [online] Available at: <https://www.geeksforgeeks.org/what-are-scanning-attacks/>.

Tutorialspoint.com. (2019). *Ethical Hacking - Reconnaissance - Tutorialspoint*. [online] Available at: <https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_reconnaissance.htm>.

www.linkedin.com. (n.d.). *The Art of Reconnaissance in Ethical Hacking: Unveiling the Secrets of Information Gathering*. [online] Available at: <https://www.linkedin.com/pulse/art-reconnaissance-ethical-hacking-unveiling-secrets-information-u3ccf#:~:text=In%20the%20world%20of%20ethical>.

FireCompass (2020). *Top 10 Tools for Reconnaissance*. [online] FireCompass. Available at: <https://www.firecompass.com/blog/top-10-tools-for-reconnaissance/>.

GeeksforGeeks. (2019). *Phishing in Ethical Hacking*. [online] Available at: https://www.geeksforgeeks.org/phishing-in-ethical-hacking/ [Accessed 8 Dec. 2023].

IBM (2013). *Injection Attacks*. [online] www.ibm.com. Available at: <https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-injection-attacks>.

Praveen (2023). *Gaining Access: Unveiling the Techniques, Implications, and Safeguards*. [online] Cybersecurity Exchange. Available at: <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/gaining-access-techniques-implications-safeguards/>.

GeeksforGeeks. (2023). *Maintaining Access Tools in Kali Linux*. [online] Available at: <https://www.geeksforgeeks.org/maintaining-access-tools-in-kali-linux/>.

Meredith, D. (n.d.). *Ethics in hacking*. [online] www.pluralsight.com. Available at: <https://www.pluralsight.com/blog/software-development/ethic-in-hacking>.

‌