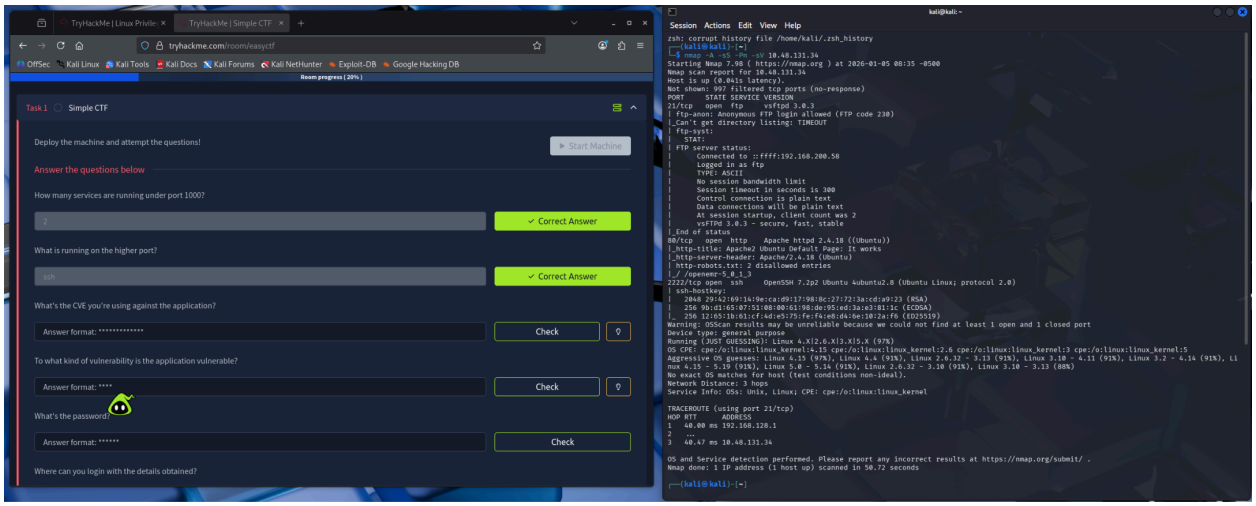
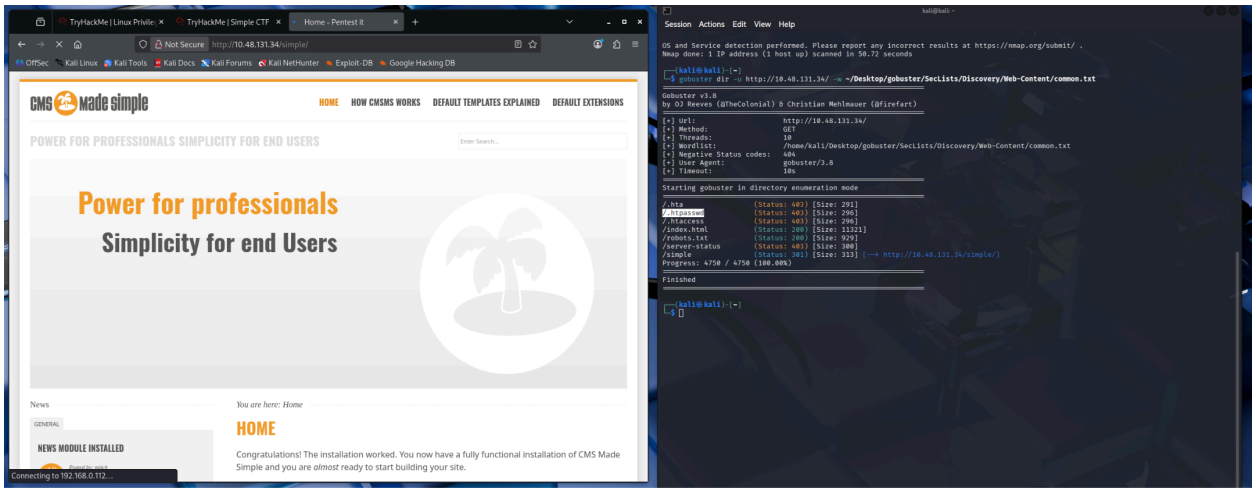
Simple CTF

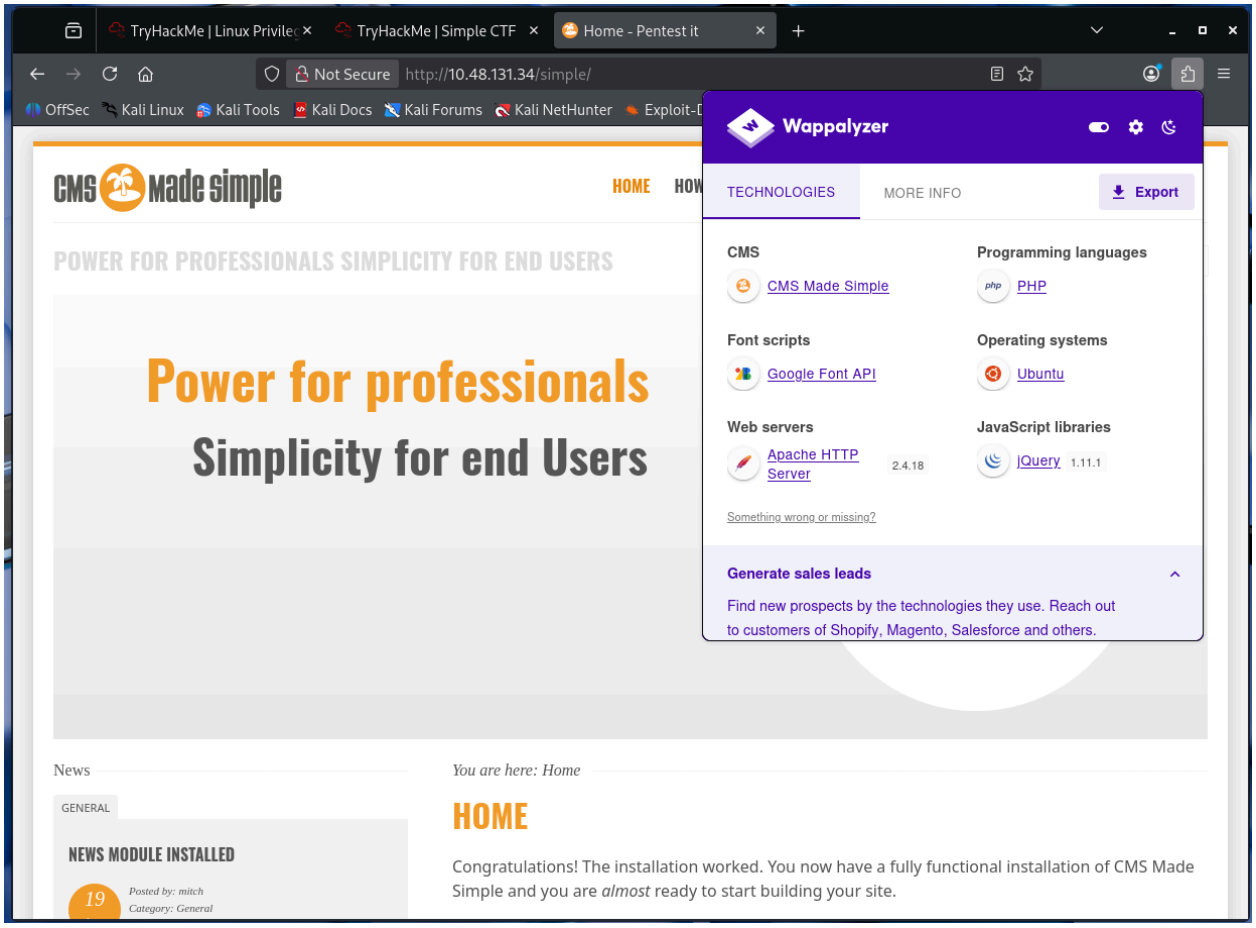
First, I ran an nmap scan on the target machine and that solved the first two questions.



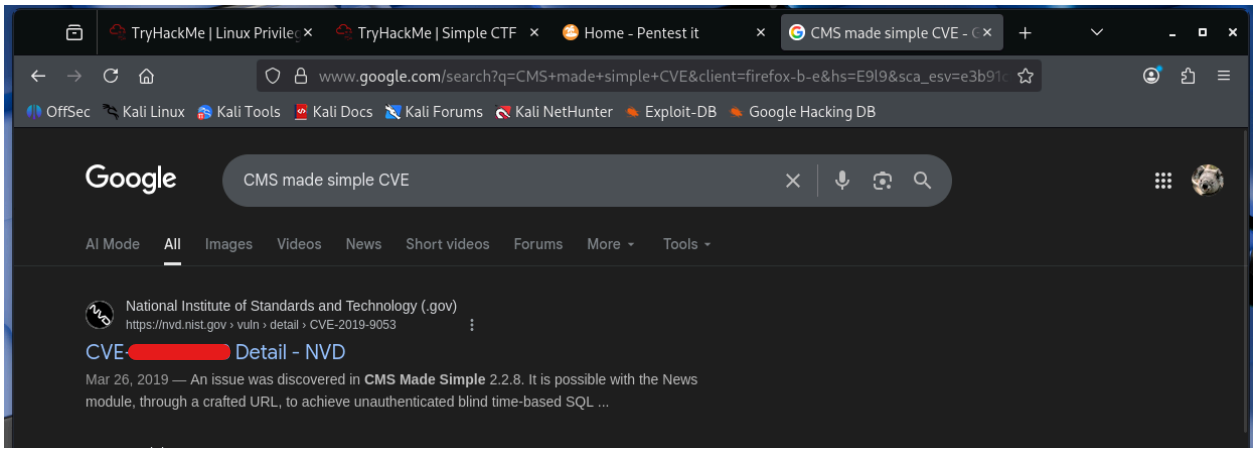
Total 3 open ports 80, 21 and 2222. Nothing suspicious till now on these ports. So i did directory Brute forcing as it is running a website on port 80



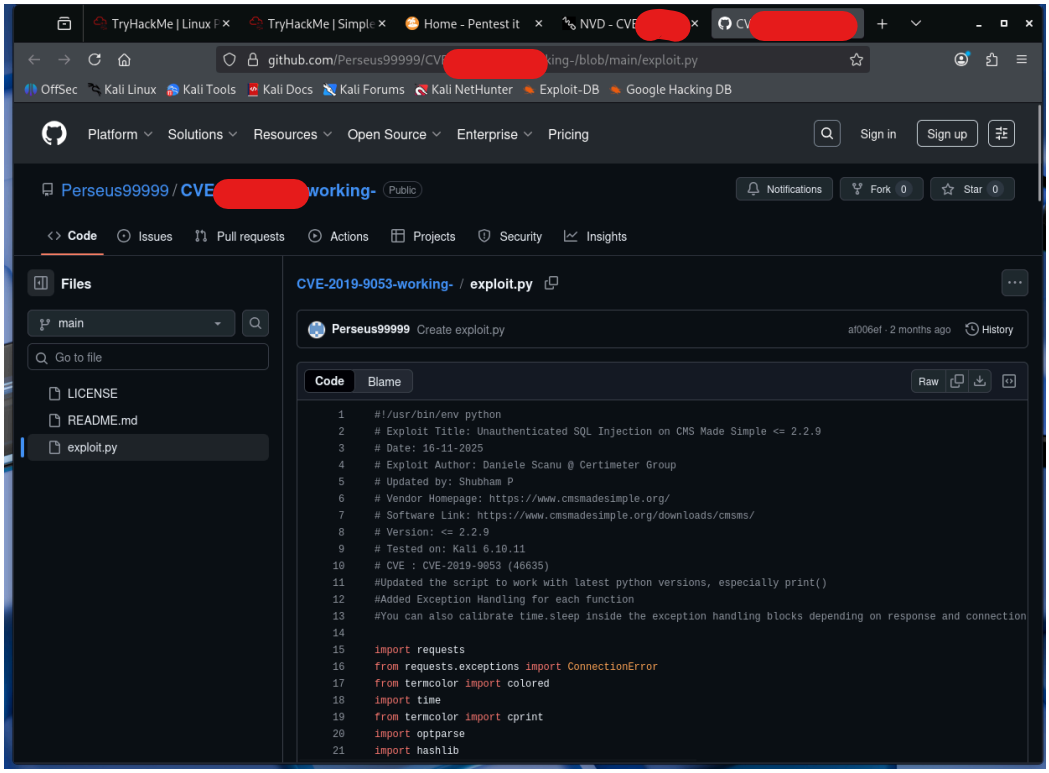
After brute forcing I found some directories and after searching them /simple showed something new and interesting. It is a free open-source Content Management System.



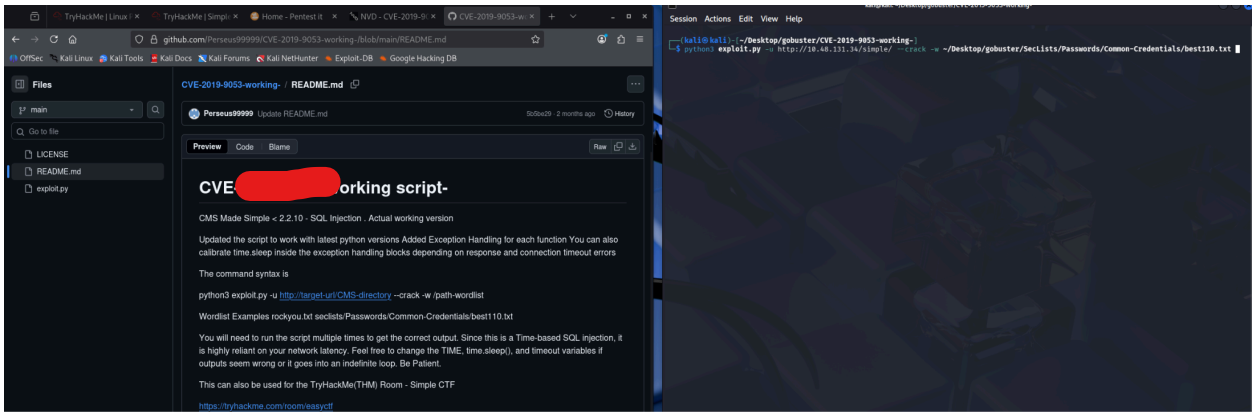
But wappalyzer didn't give me any version. So I searched CMS made simple CVE and found this version.



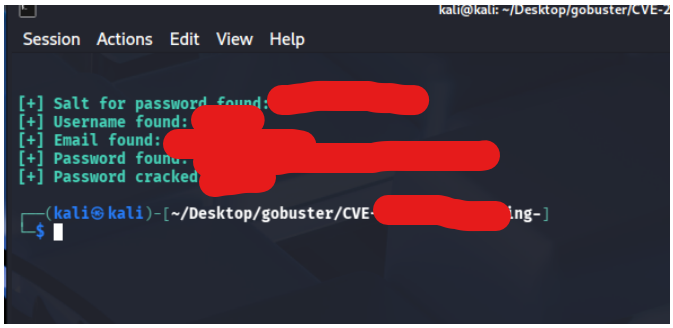
This was the third question answered and after reading the vulnerability I found the Fourth answer. Also I found a working exploit after reading the document.



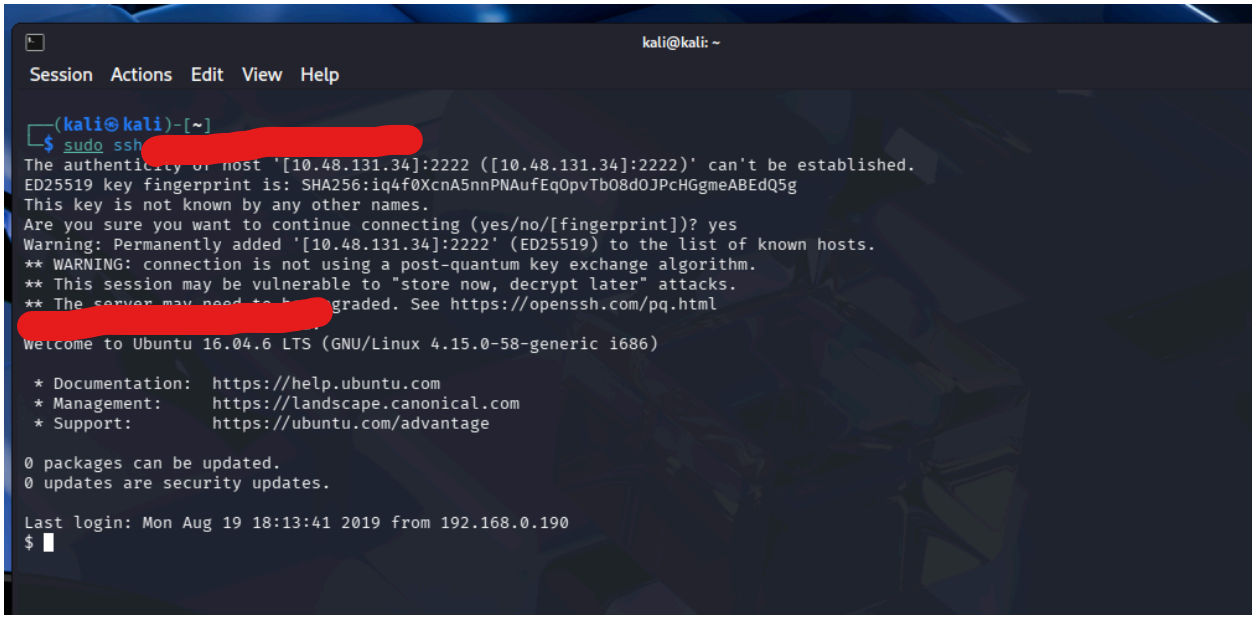
Then used the Exploit as explained in the README.md.



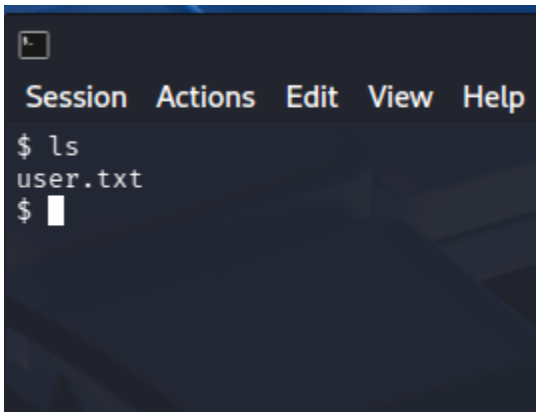
After Exploiting, I found these credentials.



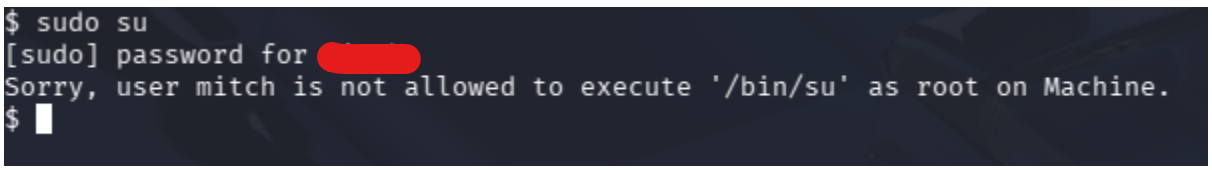
So, I found the credentials. That answers the password question. And we have a SSH port open on port 2222. So that is the next answer. Then I connected using SSH.

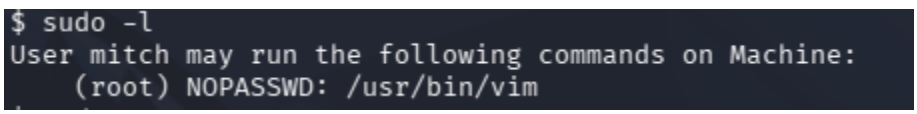


After using ls I found user.txt. That contains the next answer. And after using cd .. I found another answer.



Now, I have to escalate the privilege. So I used sudo -l command. That gives us info about what sudo commands can be run without password. As our user cannot access sudo.





So, we can run sudo vim without a password. That is the next answer.

From this repo we can find that we can use sudo vim -c ':!/bin/bash' command to escalate privilege.
[RoqueNight/Linux-Privilege-Escalation-Basics: Simple and accurate guide for linux privilege escalation tactics]

```
$ sudo vim -c ':!/bin/bash'

root@Machine:/home# ls
mitch  sunbath
root@Machine:/home# whoami
root
root@Machine:/home#
```

And Yo! I got root access. Now we have to find the flag in the root directory.

```
root@Machine:/home# cd ..
root@Machine:/# cd root
root@Machine:/root# ls
root.txt
root@Machine:/root#
```

And I found the last flag. That's all for now, thanks for reading :)

- Sk . Md. Rashid Assef Shibly