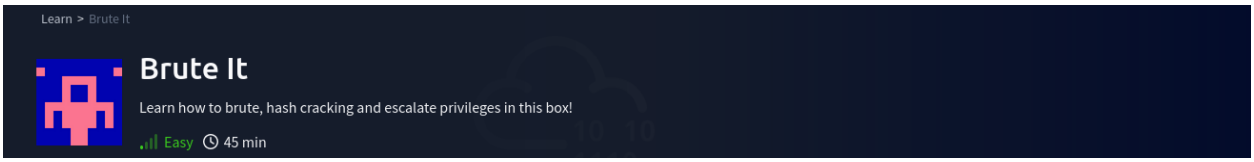
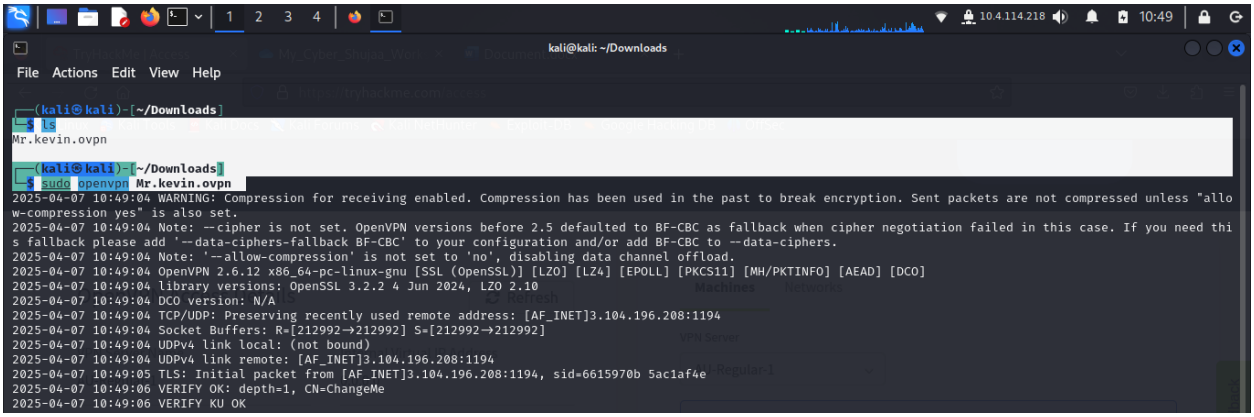
LinkedIn: Kelvin Kimotho



The first thing i always do is to connect to their network via the provided vpn using the OpenVPN tool. I download the vpn config file the connect to their network like this. This enables me to interact with the target machine.



“Initialization Sequence Completed” indicates a successful connection.

Recon

I becan by scaning the target for running services, open ports and service versions running on the target using NMAP tool.

“sudo nmap -sV 10[.]10[.]172[.]248”.

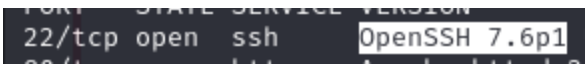
Questions

Question: Search for open ports using nmap.
How many ports are open?

Answer: 2

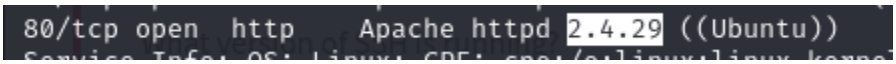
Question: What version of SSH is running?

Answer: OpenSSH 7.6p1



Question: What version of Apache is running?

Answer: 2.4.29



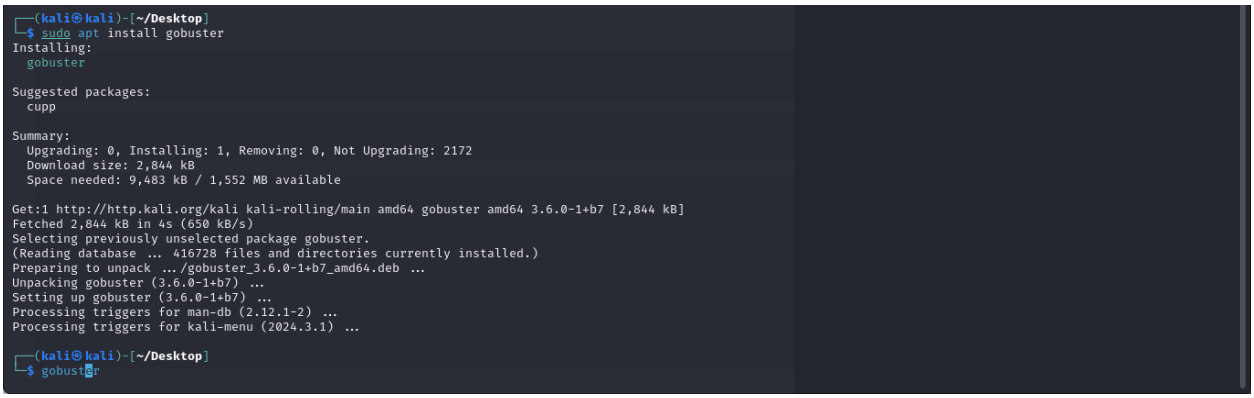
Question: Which Linux distribution is running?

Answer: Ubuntu

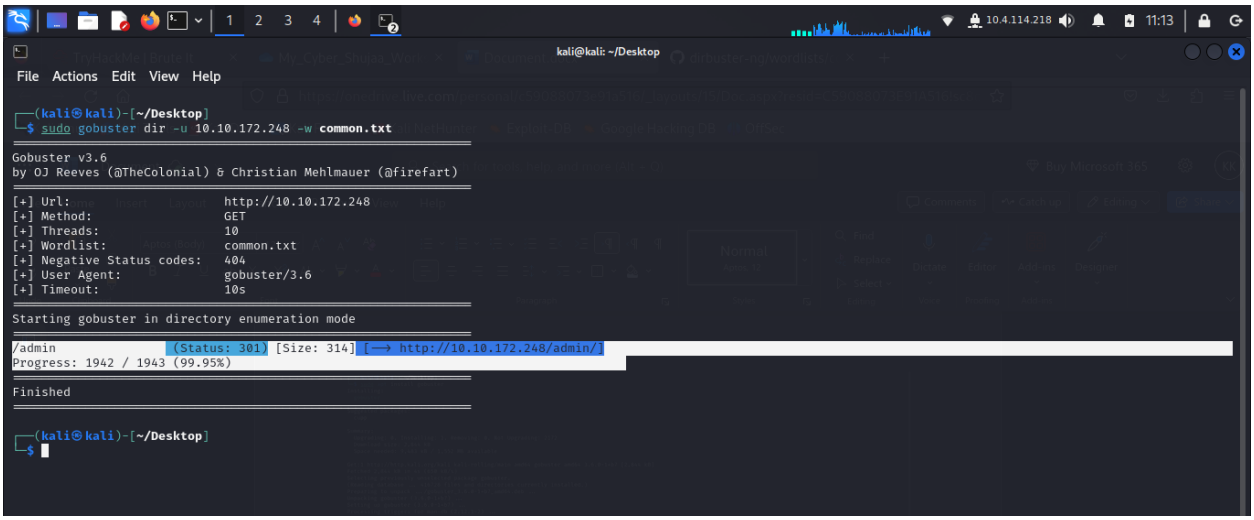
Question: Search for hidden directories on web server.

What is the hidden directory?

For directory enumeration, I used gorbuster. I first installed the tool into my vm.

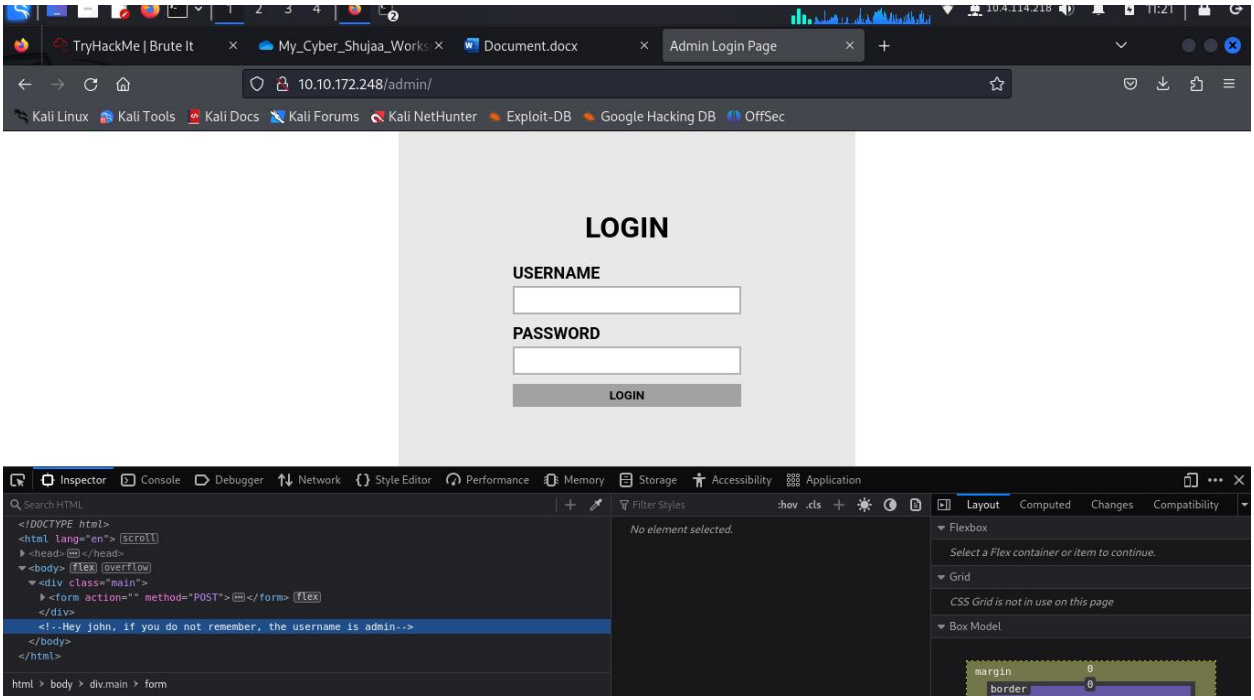


Then went ahead and performed the directory enumeration where i discovered admin directory.

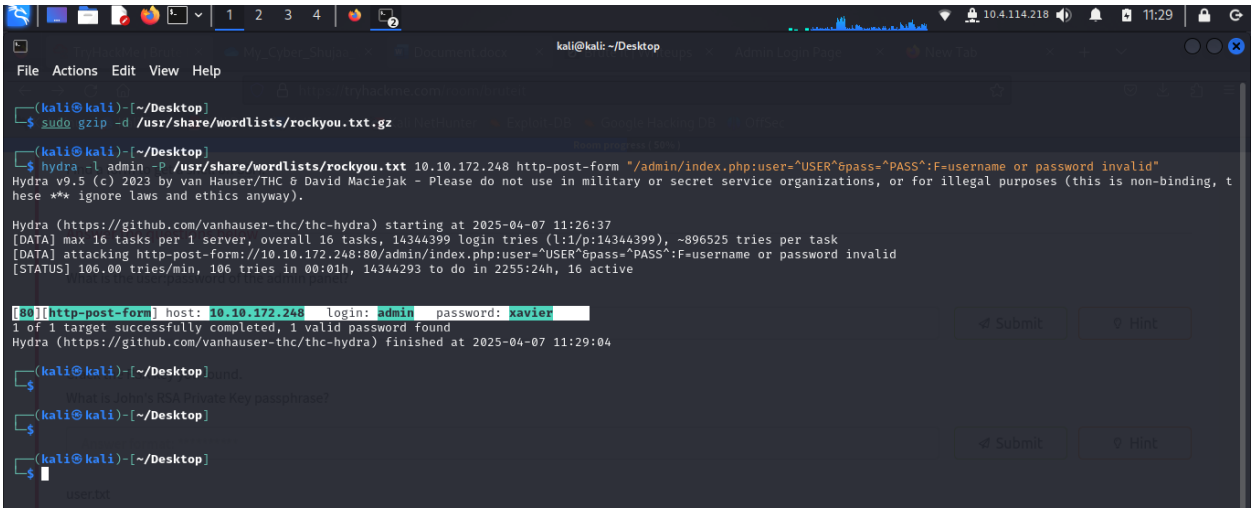


Getting a Shell

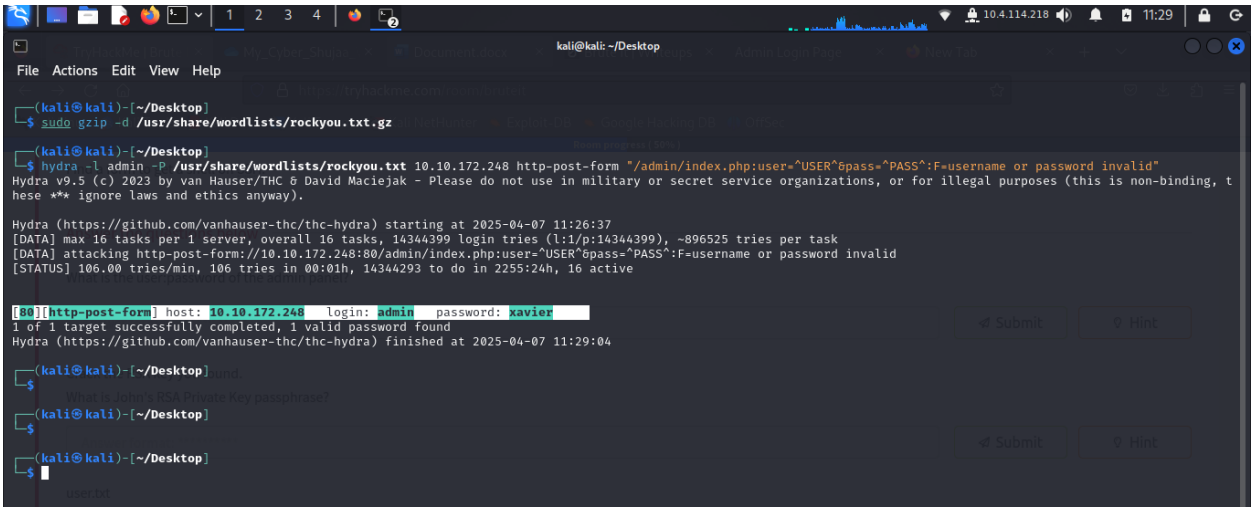
I first examined the admin login page including the html code where i found a comment that confirmed the username as ‘admin’. The only thing remaining was the admin password.



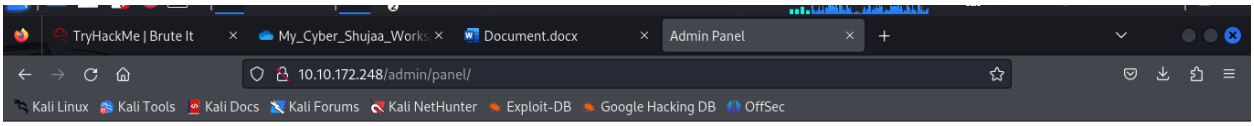
The hint suggested the use of hydra a tool to brute force the admin accounts password. I used the massive rockyou.txt wordlist for this operation.



Hydra managed to brute force the admin account password” xavier”.



I then logged in to the admins panel using username ’admin’ and password ’ xavier’.



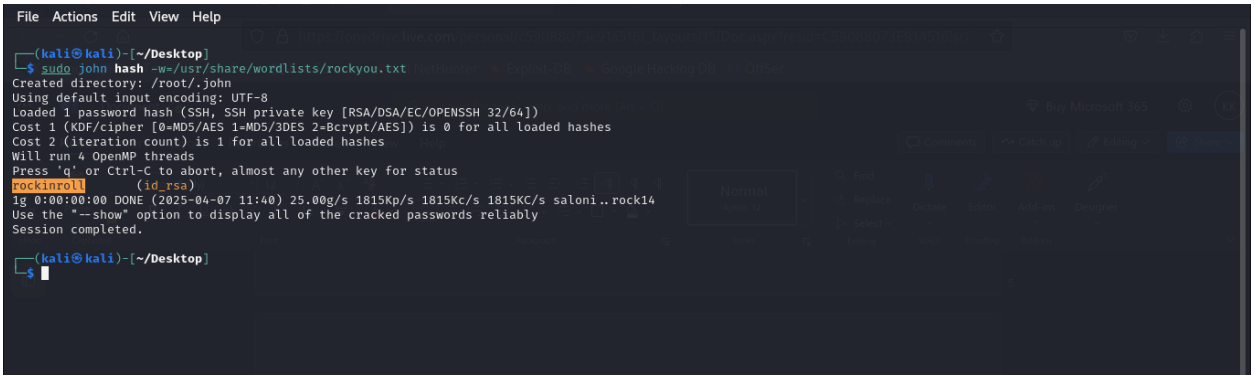
Hello john, finish the development of the site, here's your RSA private key.

THM{brut3_f0rce_is_e4sy}

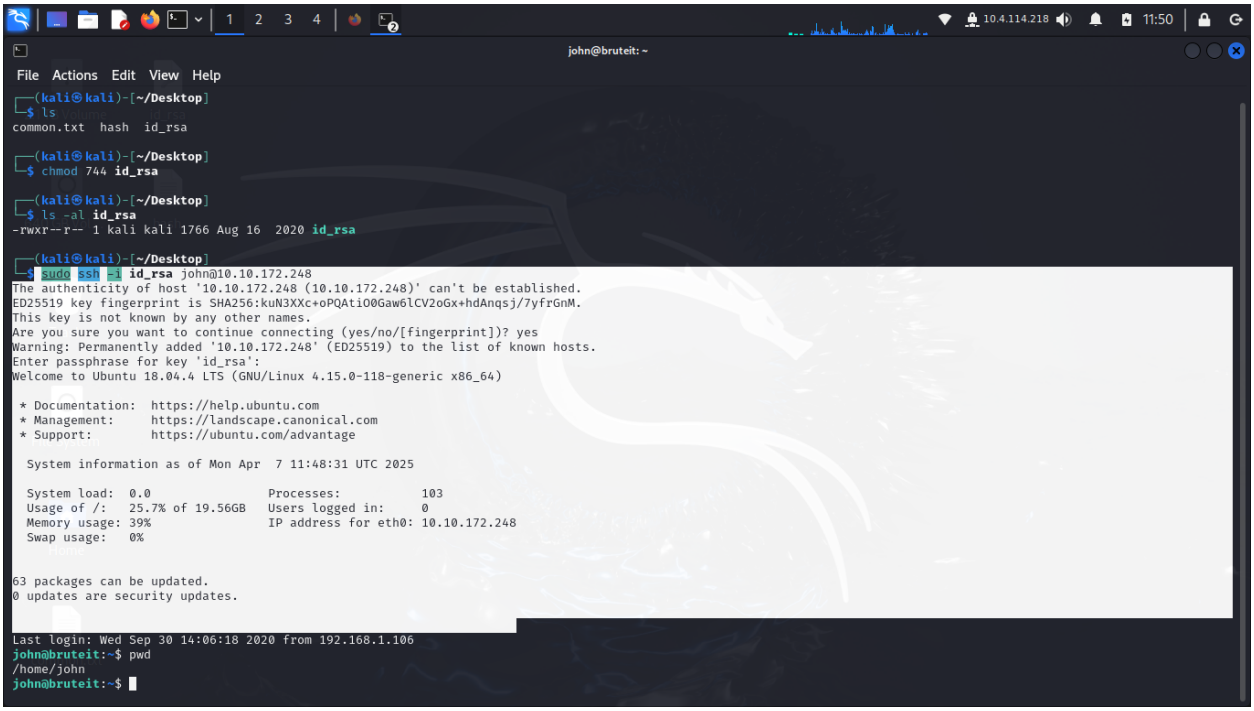
I then downloaded the RSA private key into my machine using wget tool.

I then used ssh2john tool to create a hash file from the private key file.

I then used john the ripper tool together with the rockyou wordlist to to crack the hash.

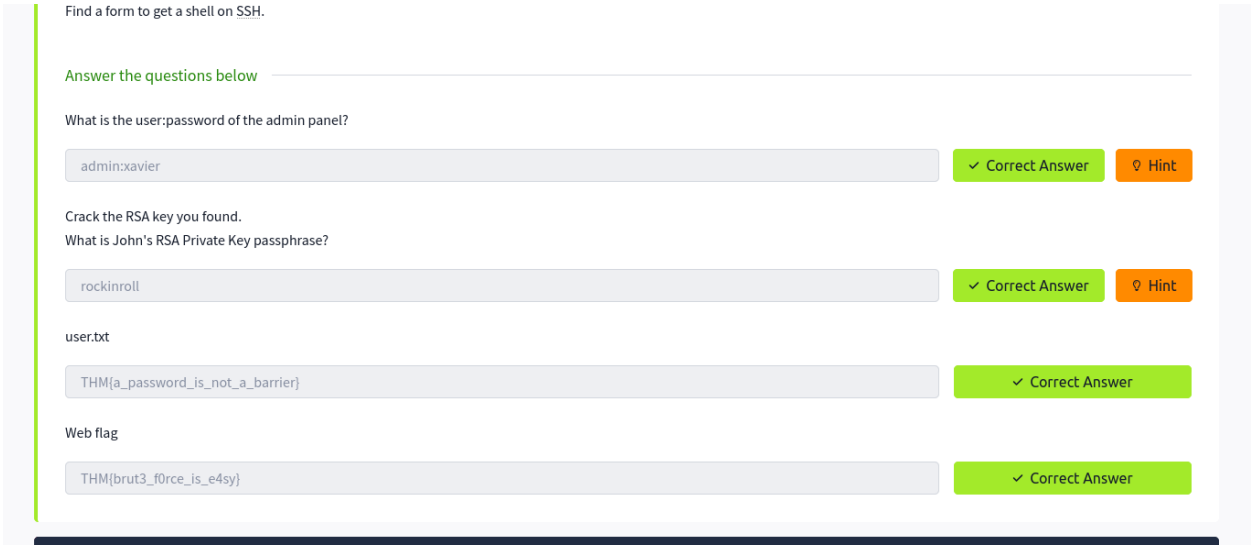


The RSA private key phrase was ” rockinroll” which was the password for john. I changed the permissions for the key file then went ahead to ssh into the target machine now, i entered the passphrase ” rockinroll” and i managed to login as user john.



I came across a user.txt file which held the flag.

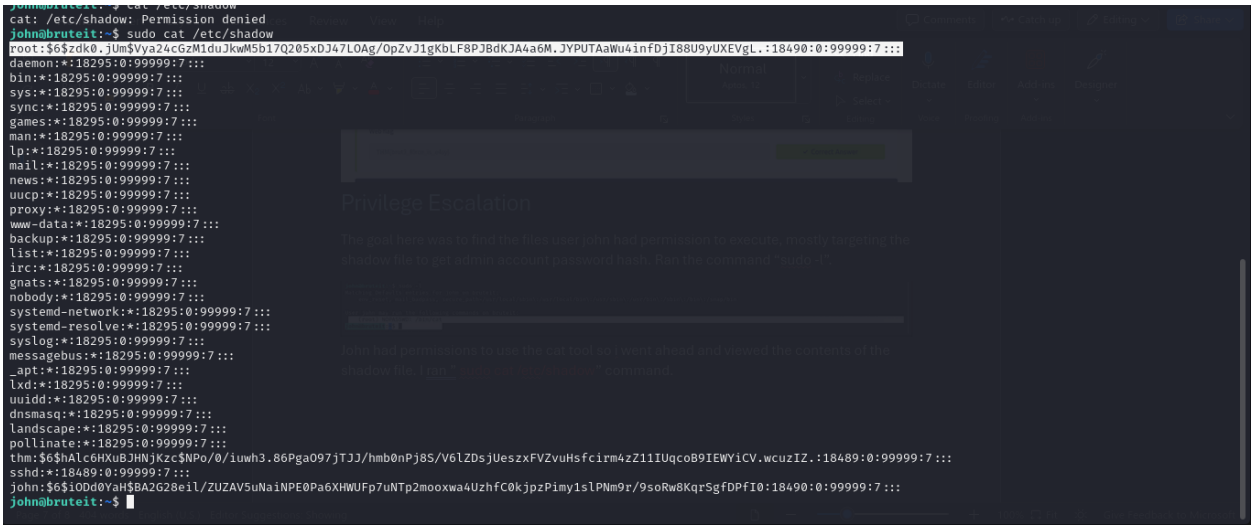
Questions



Privilege Escalation

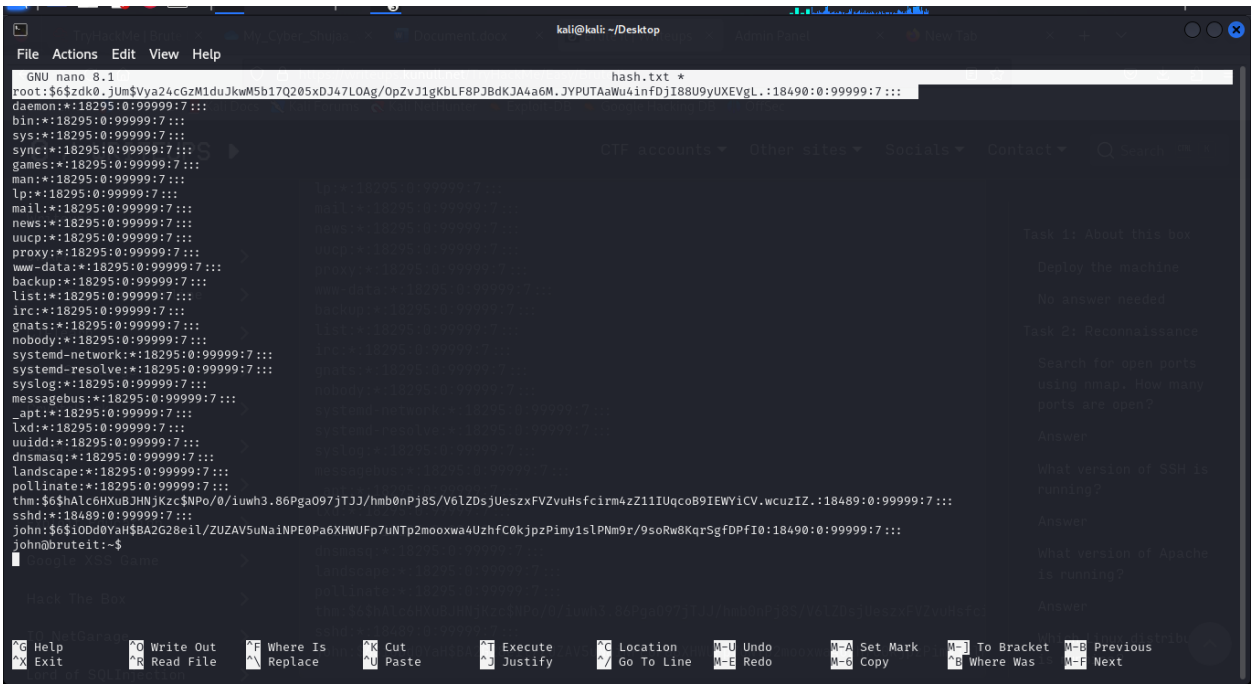
The goal here was to find the files user john had permission to execute, mostly targeting the shadow file to get admin account password hash. Ran the command “sudo -l”.

John had permissions to use the cat tool so i went ahead and viewed the contents of the shadow file. I ran ” sudo cat /etc/shadow” command.

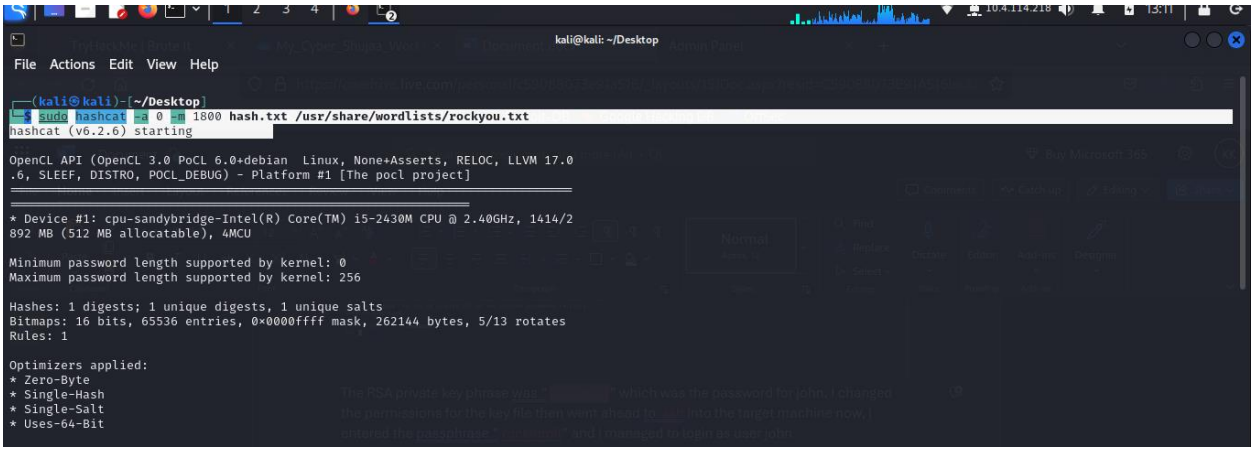


The root account has was ”
root:6zdk0.jUm$Vya24cGzM1duJkwM5b17Q205xDJ47LOAg/OpZvJ1gKbLF8PJBdKJA4a6M.JYPUTAaWu4infDjI88U9yUXEVgL”.

The hash appeared to be a sha-512 because of the 6 at the beginning of the hash. I went ahead and used Hashcat to crack the root user account password.



I then went ahead cracking the hash using hashcat. The root user password was ” football”.



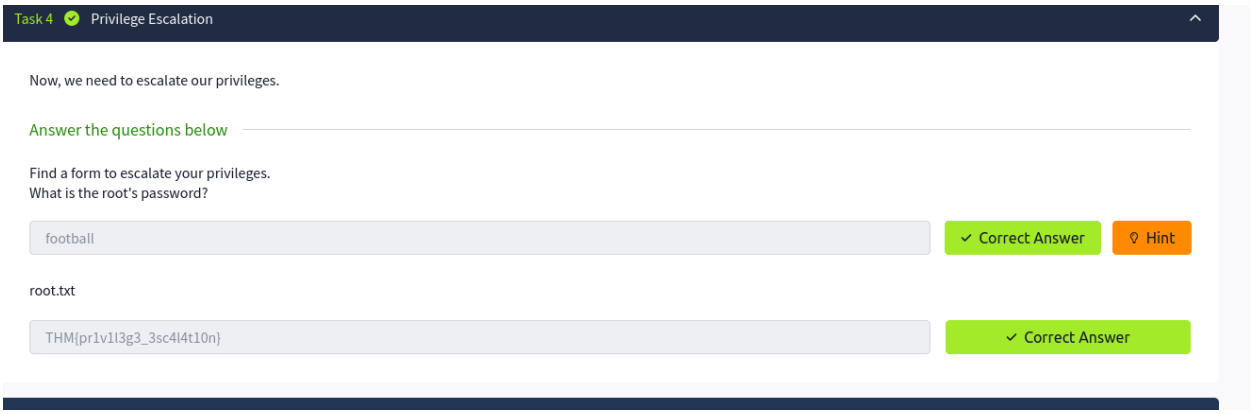
The next step now was to switch to the root user account and find the root user flag. But before that, I remembered that user john had permission to execute" cat". I tried cat on an imaginary root.txt in the root user directory. The root user flag was" THM{pr1v1l3g3_3sc4l4t10n}".

I tried to switch to the root user account from john's account. This was just a confirmation that the text file really existed. I used the password" football" and logged in to the root user account.

```
john@bruteit:~$ su
Password:
root@bruteit:/home/john# ls
user.txt
root@bruteit:/home/john# cd
root@bruteit:~# ls
root.txt
root@bruteit:~# cat root.txt
THM{pr1v1l3g3_3sc4l4t10n}
root@bruteit:~#
```

I tried to switch to the root user account from john's accou
that the text file really existed.

Questions



The badge!!!