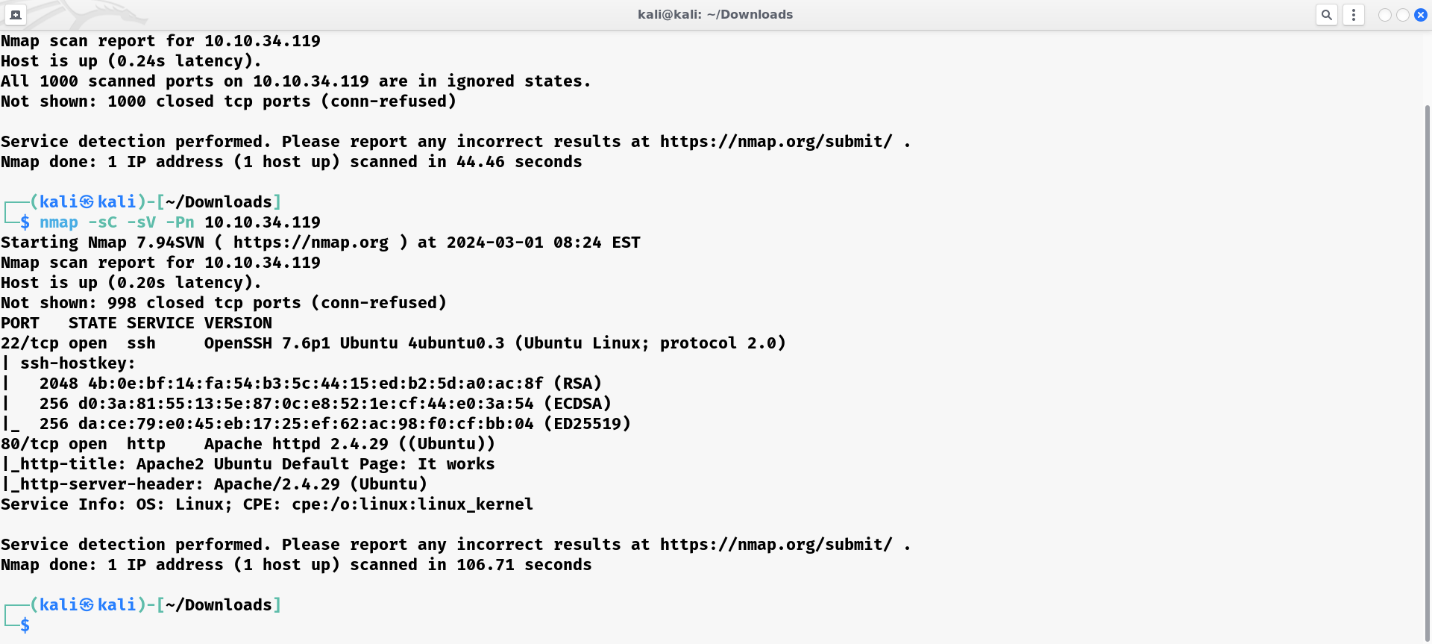
**Lab Practical #08:**

TryHackMe Room: - **Brute It**

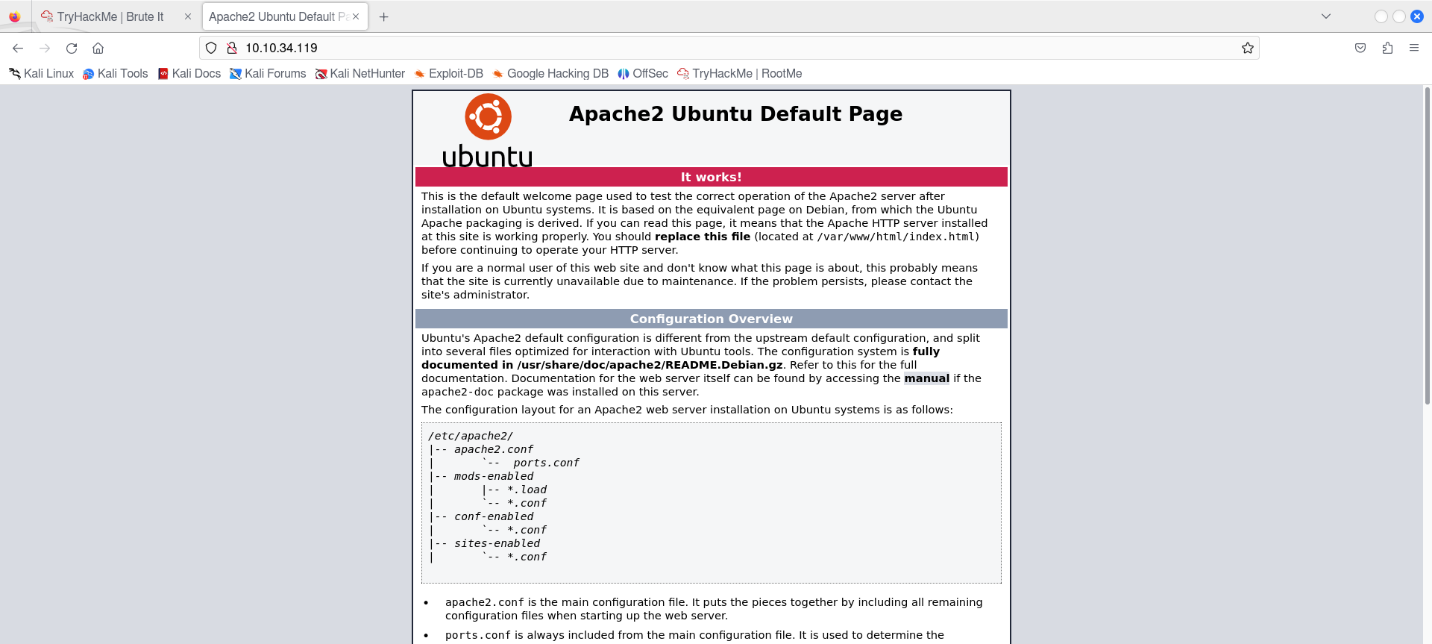
1. Initially, we will try with the reconnaissance, so let’s start with the nmap scan.



**nmap results**

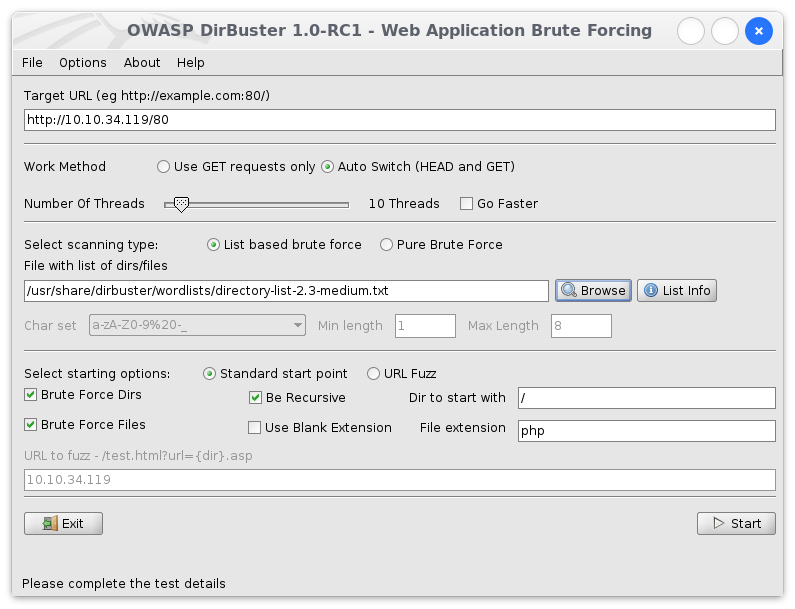
By looking at the above screenshot, we can see that we have found 3 ports open i.e. 21(FTP), 22(SSH) and 80(HTTP).

1. As port 80 is open, copy-paste the IP in the browser and check the page of it.

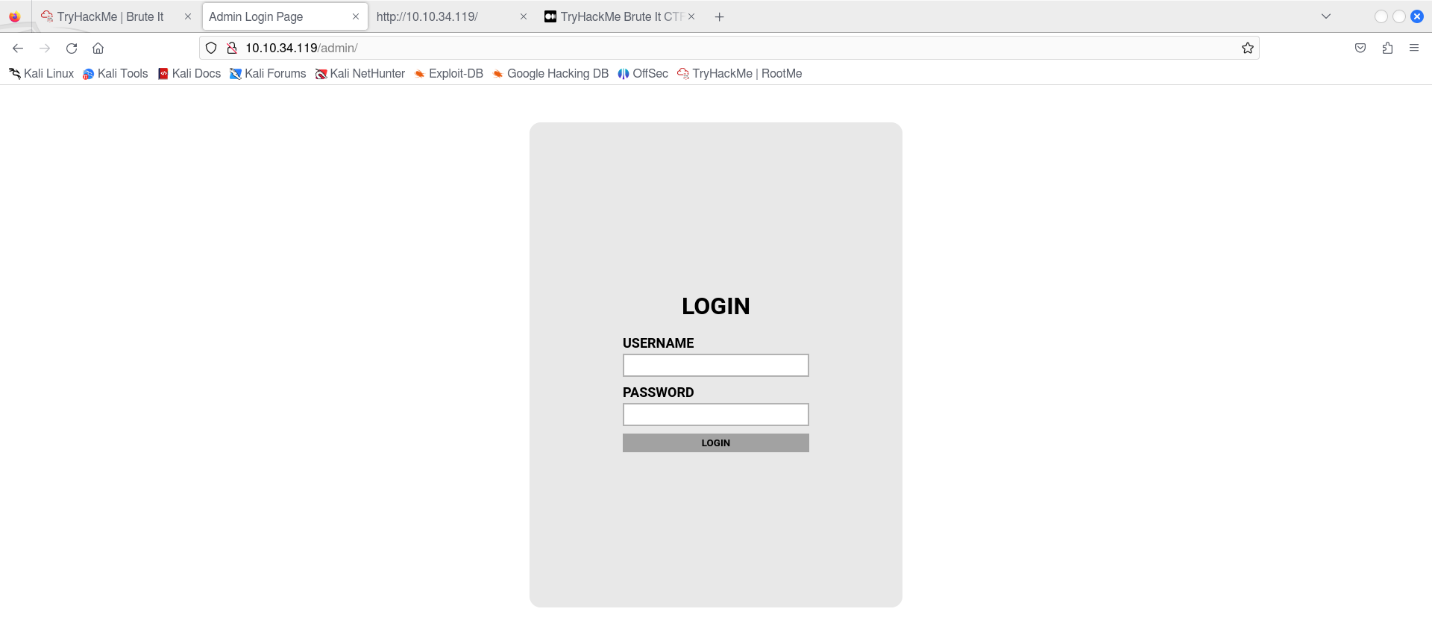


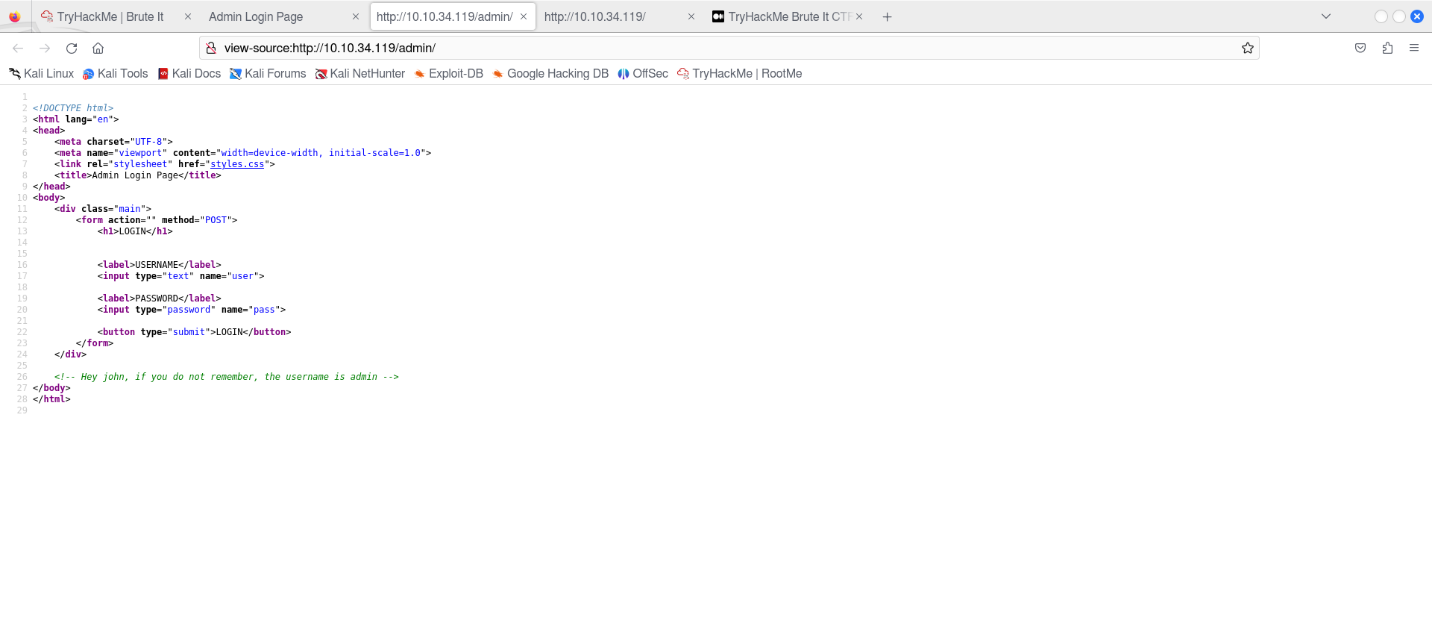
**page**

1. To perform directory search the tool called gobuster is used. I used he command: dirbuster.



From the results, We have discovered a hidden directory named /admin. Now navigate to http://10.10.204.93/admin and lets see what’s in there!!





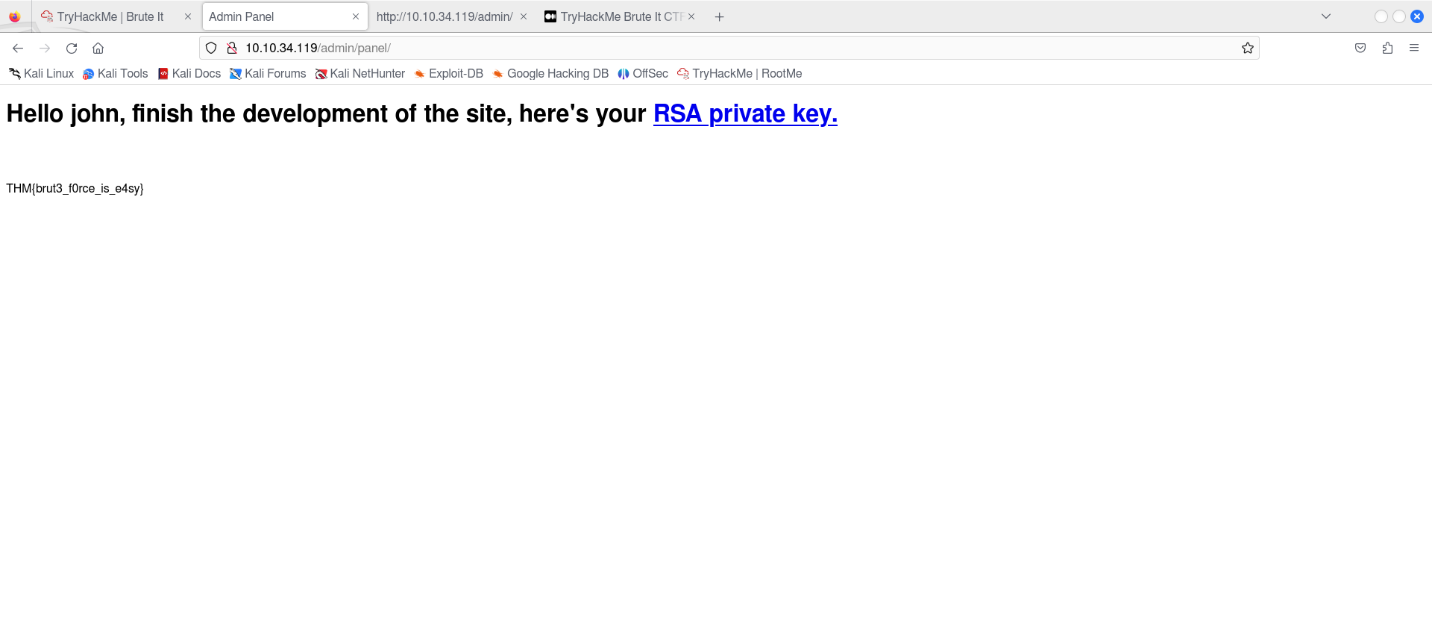
We can see an admin login page. It requires a username and Password. But we can try to bypass the Login through a Brute-Force attack using a tool called “Hydra”

From the Source code of the webpage, we get some information about the user . It says that there is a user named JOHN and his Username on the Web login is ADMIN .

Since we got a Username from the Source Code. Now we need to brute Force the password and bypass the Login.



Yep!! We cracked the Web Login Password! Now Login with admin username with password we cracked.



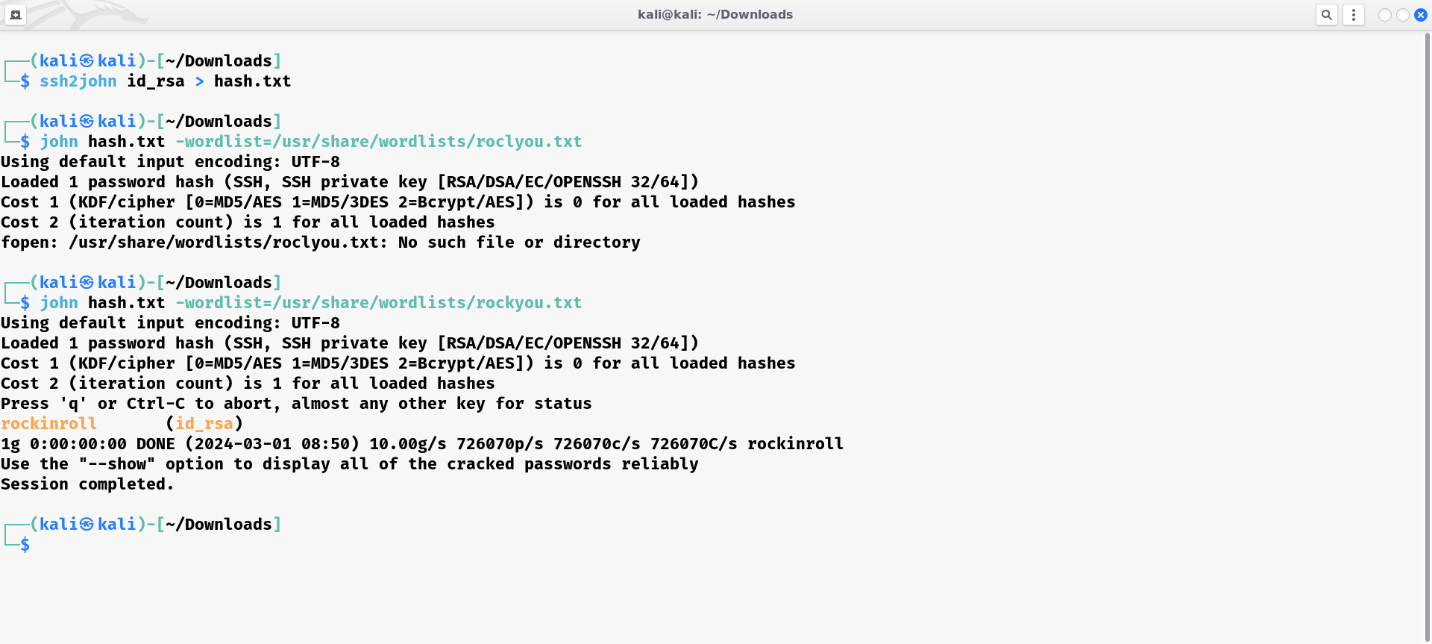
After successful Login, We get the Web Flag and an RSA Private key. Using this RSA key we can attempt to Login via SSH since Port 22 on the target is open.

When we attempt to login using this RSA key. It requires a Password!! Since we don’t have that password we need to crack it using a tool called “John The Ripper”

In order to crack a RSA private key we need to First convert the Key file into a text format. This can be done using a tool called “ssh2john”

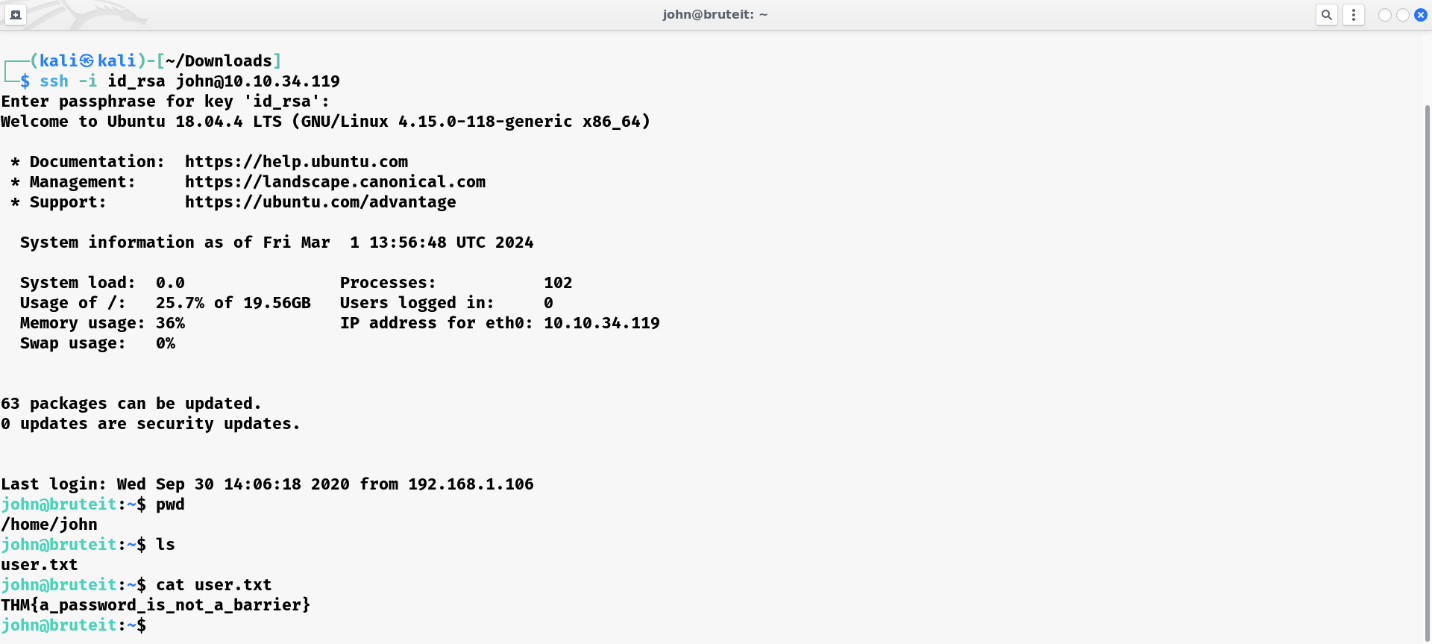
ssh2john is a utility to convert the key-file into a txt-format that would be suitable for John The Ripper to crack by comparing hashes.





Yep!! We cracked the password! Now since we have the Password of id\_rsa file. We can now login via SSH and pop the shell of user named JOHN.

Since id\_rsa is private RSA key file, in order to work the permissions to access it should be only given to the owner of the file.



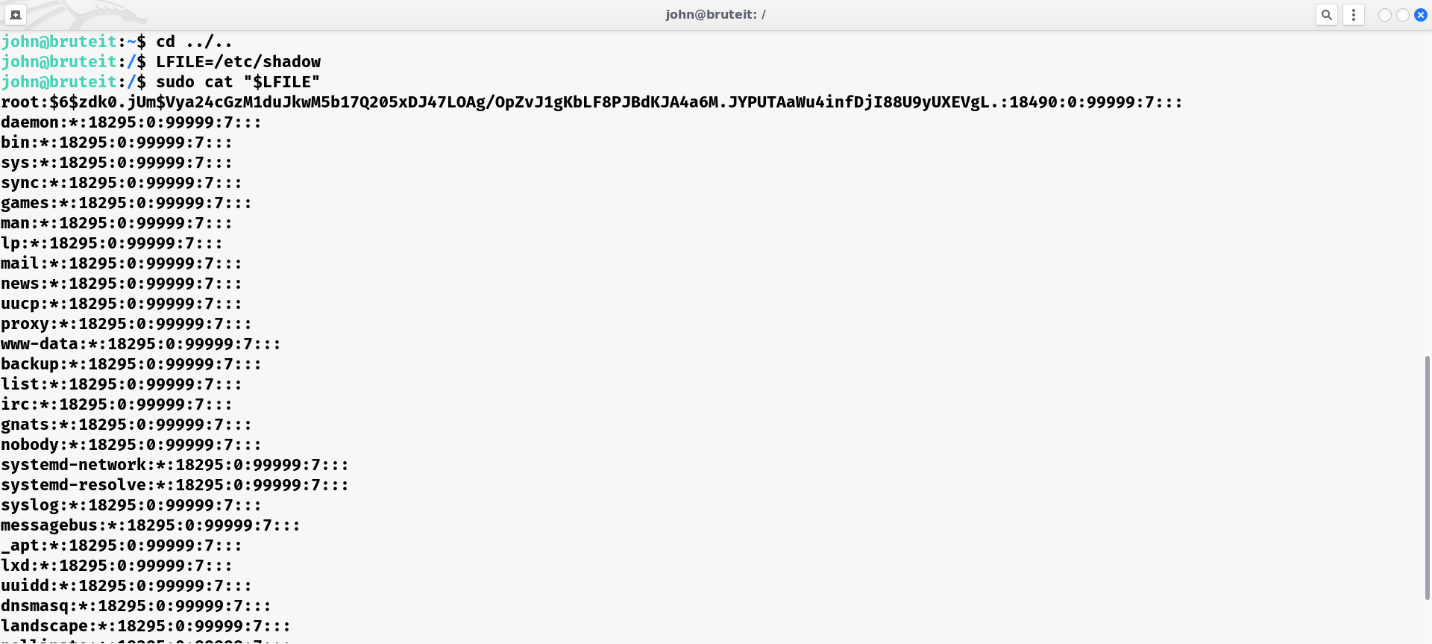
Now we successfully managed to pop a User Shell and the user flag under user.txt file.

From here we should escalate our privileges and become ROOT to get the Root Flag!

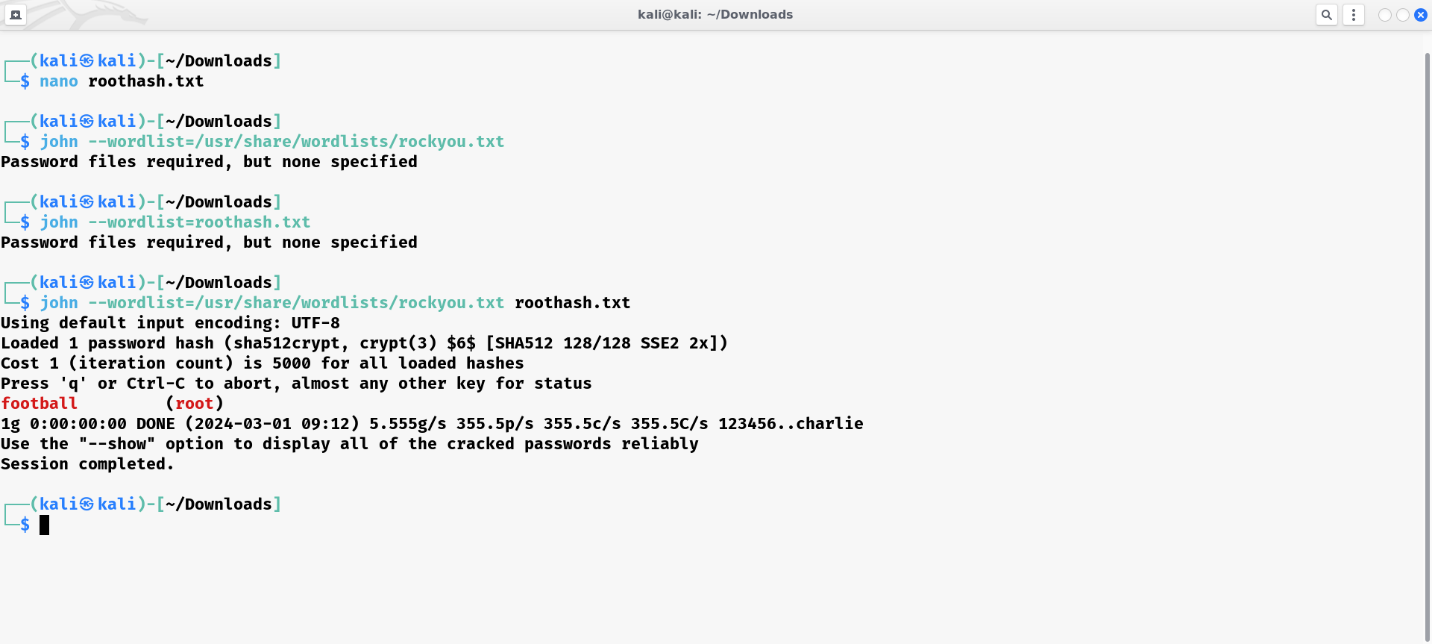
We can gain the ROOT shell on this box by abusing the SUDO rights of the user. SUDO rights gives the ability to a normal user to execute commands as ROOT!

Our user john have SUDO rights to run /bin/cat command as ROOT.

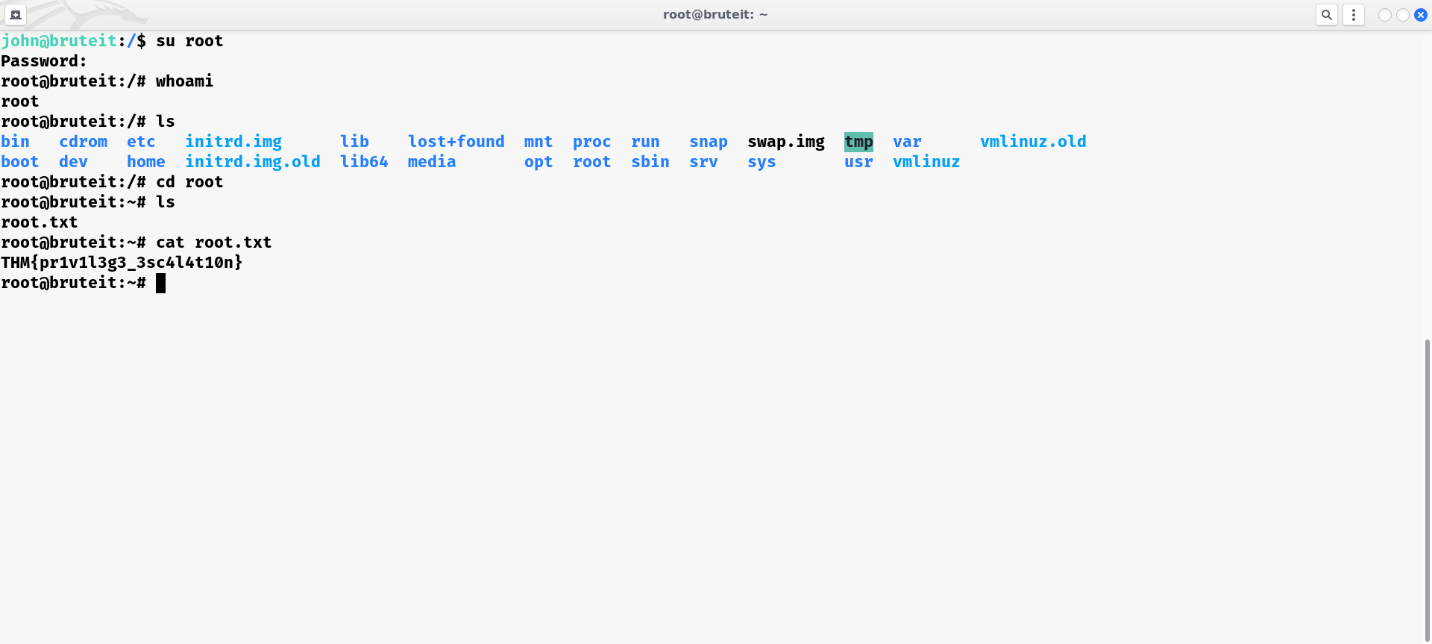
cat command in Linux is used to open and view the contents of a file. Since we have SUDO rights to cat command we can use that ROOT rights to open and access the contents of /etc/shadow file which contains the password hashes of all users including ROOT user!!



Once we get the password hash of ROOT user. We can store it in a txt-file and crack it using “John The Ripper”. A user’s password hash (if they have one) can be found between the first and second colons (:) of each line.



Now we can switch user to ROOT using su root command and grab the ROOT flag under /root directory.



That’s it!! We have successfully ROOTED the box and obtained the ROOT flag!!