**Task 1: About this box**

A screenshot of a computer

Description automatically generated

**Task 2: Reconnaissance**

Run a Nmap scan to get information about ports. I executed the order:

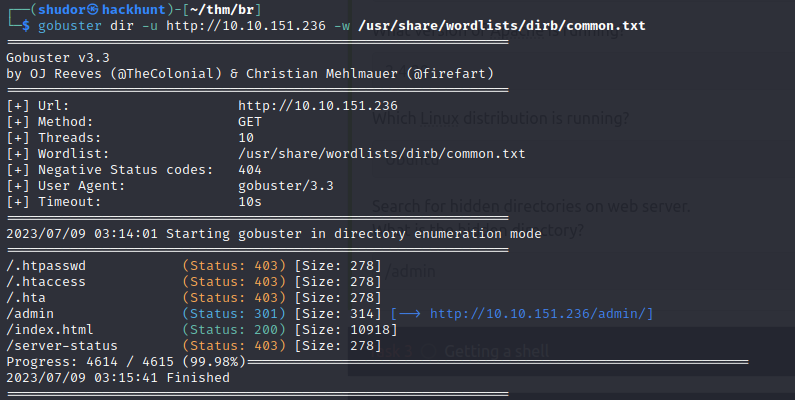
sudo nmap -sSV -Pn machine\_ip

A screenshot of a computer program

Description automatically generated

The gobuster tool is used to conduct directory searches. I executed this command:

gobuster dir -u http://MACHINE\_IP --wordlist /usr/share/wordlists/dirb/common.txt



With the help of above scanning result, we can answer the following questions:

A screenshot of a computer

Description automatically generated

**Task 3: Getting a Shell**

We will first start with /admin page.

It is a simple login page.

A screenshot of a computer

Description automatically generated

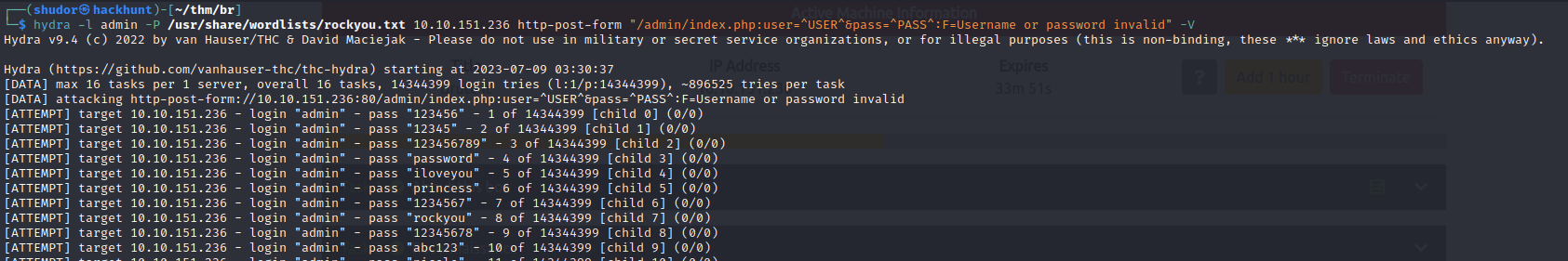
We will view the page source and try to find any clue from there.

A screenshot of a computer program

Description automatically generated

We found from the page view source the username is admin.

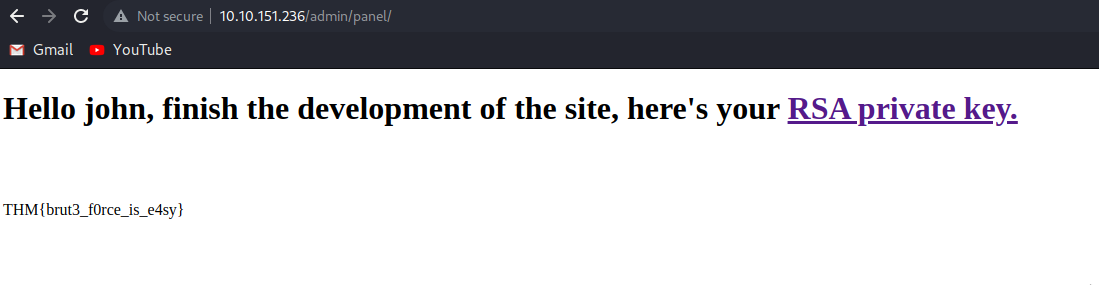
We will use password crack tool ‘Hydra’ to get the password with username admin.

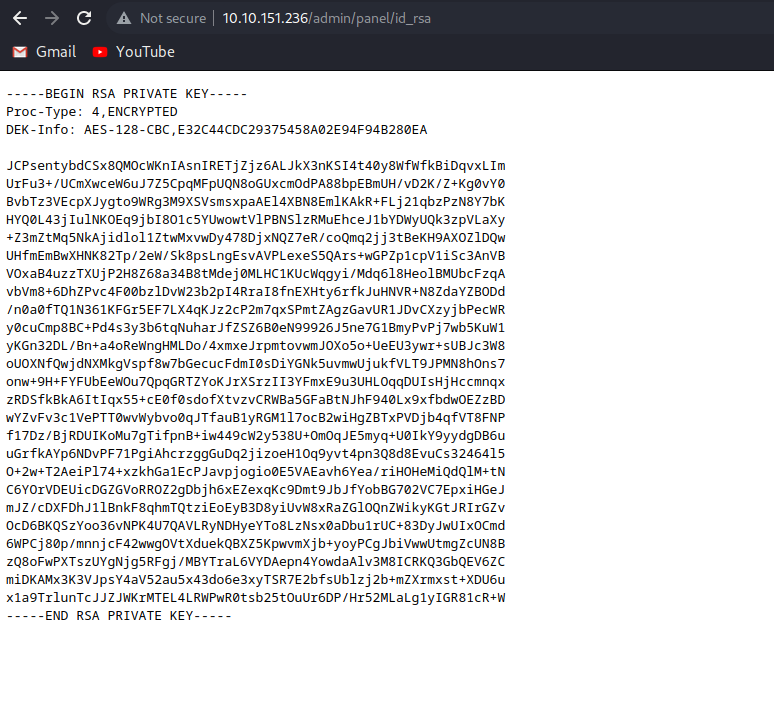


A screen shot of a computer

Description automatically generated

After successfully logging in we got a RSA key and web flag





we canget the RSA key in our local system. Usin the below command

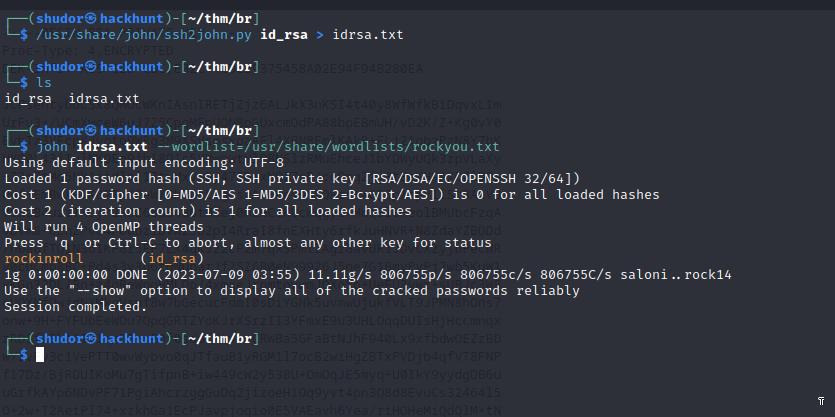
wget http://10.10.151.236/admin/panel/id\_rsa

using ssh2jhon we can convert rsa key into text format.

/usr/share/john/ssh2john.py > idrsa.txt

By Using the tool john the ripper, we can perform brute force to crack the RSA key.

john idrsa.txt --wordlist=/usr/share/wordlists/rockyou.txt

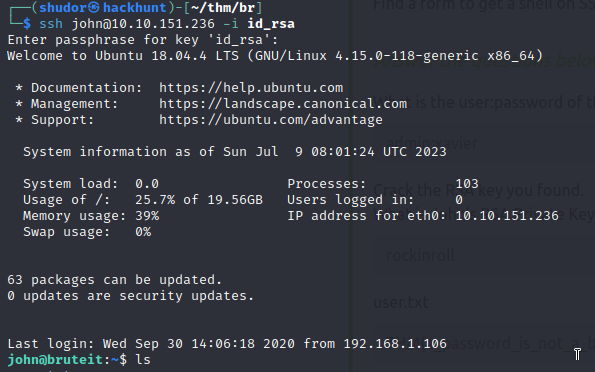


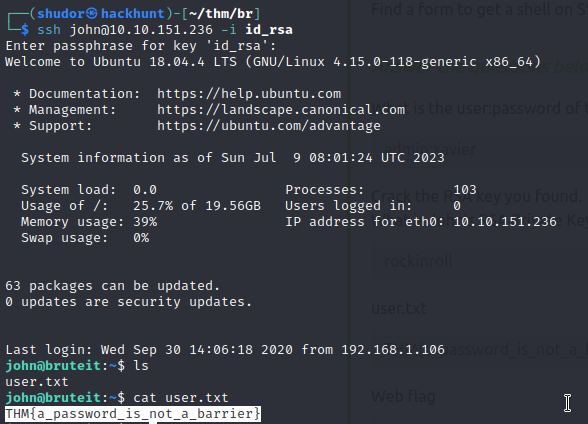
Now log into the ssh account: Don’t forget to change the permission of the id\_rsa file to:

Chmod 600 id\_rsa

Now logged in using below command:

ssh john@10.10.151.236 -i id\_rsa





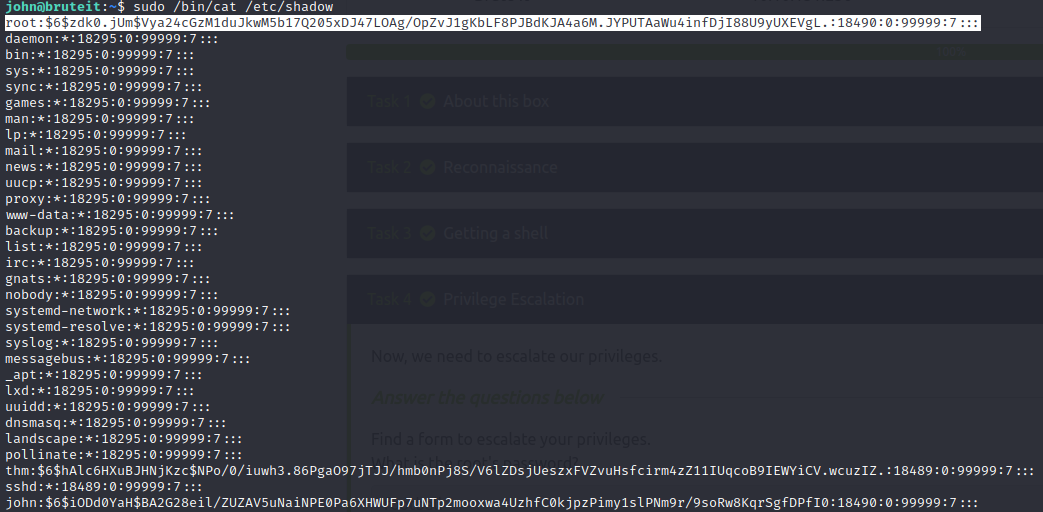
With the help of above we can answer the following questions:

A screenshot of a computer

Description automatically generated

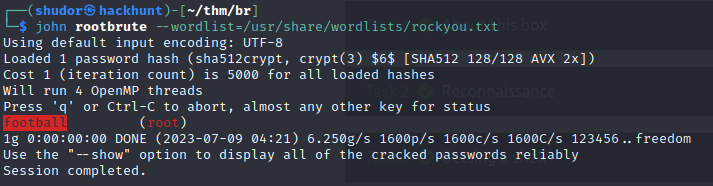
**Task4: Privilege Escalation**

By checking the user sudo permissions: sudo -l, we find that he can run cat with sudo. Let's read the /etc/shadow file, where it contains the users’ passwords.

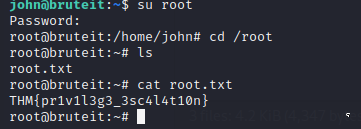


Copy the root hash key and paste in the rootbrute file.

With the help of john the ripper we can extract the password from the above file



Now we got the password we will login the root and get the root flag.



With the help of above we can answer the following questions:

A screenshot of a computer

Description automatically generated