CTF Writeups

Try Hack Me

Agent Sudo

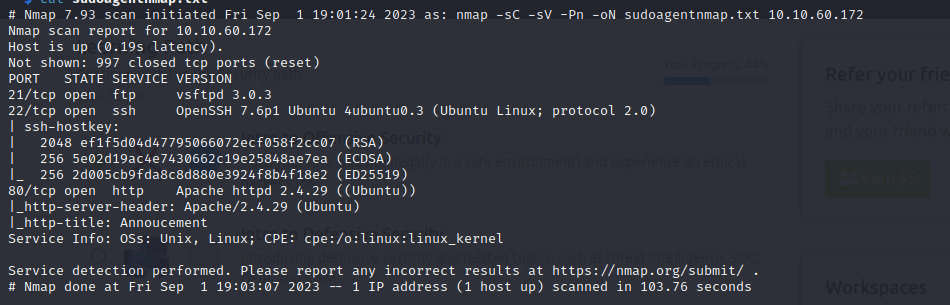
**Step 1:** Check Connectivity with the Target

Ping command

Ping is Success our Target is alive and Reachable

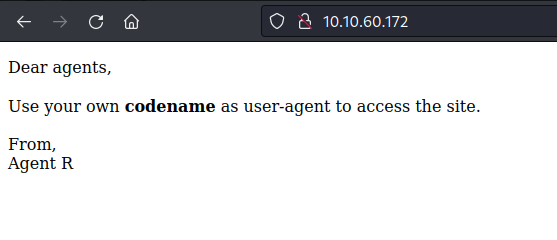
**Step 2: Information Gathering**

Use nmap command to check for Open Ports



We got Port 21,22,80 are open.

Lets check Port 80:



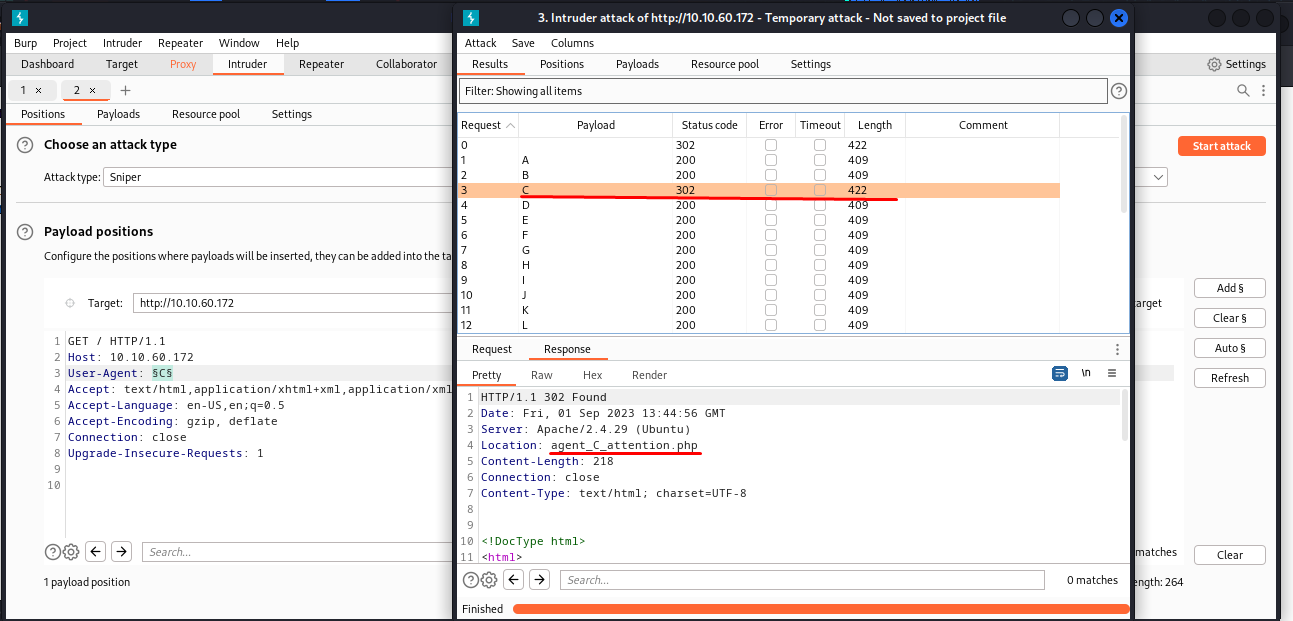
They have given a clue to use our own codename in the user-agent file in the HTTP request to access the file.

In the end the Agent is specified as R, so other agent likely be a Single Character from A-Z.

To Bruteforce the HTTP- Request we can use Burpsuite.

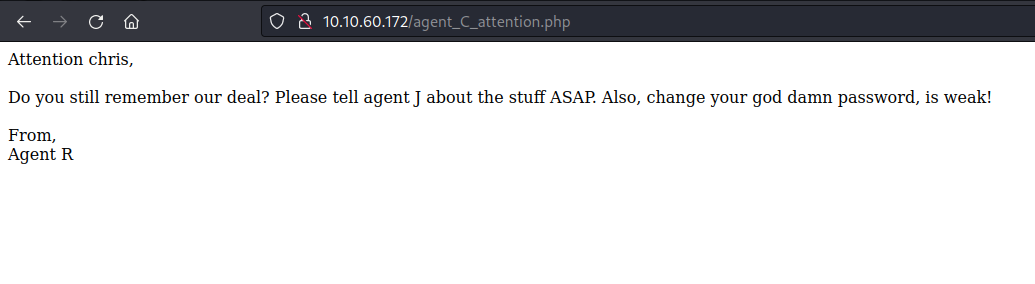
In BurpSuite:

Intercept ON => Send to Intruder => Add $$ in user agent from A-Z.



From the Burpsuite Intruder the Length of the file is changing for User-Agent: C and we got a file name **agent\_C\_attention.php**

Try Visiting that file name in the browser: 10.10.60.172/agent\_c\_attention.php

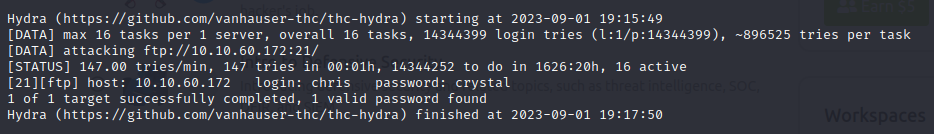


We got Agent C name Chris. And in the message they said that chris password is weak, so lets break it using Hydra.

**Step 3: Password Cracking**

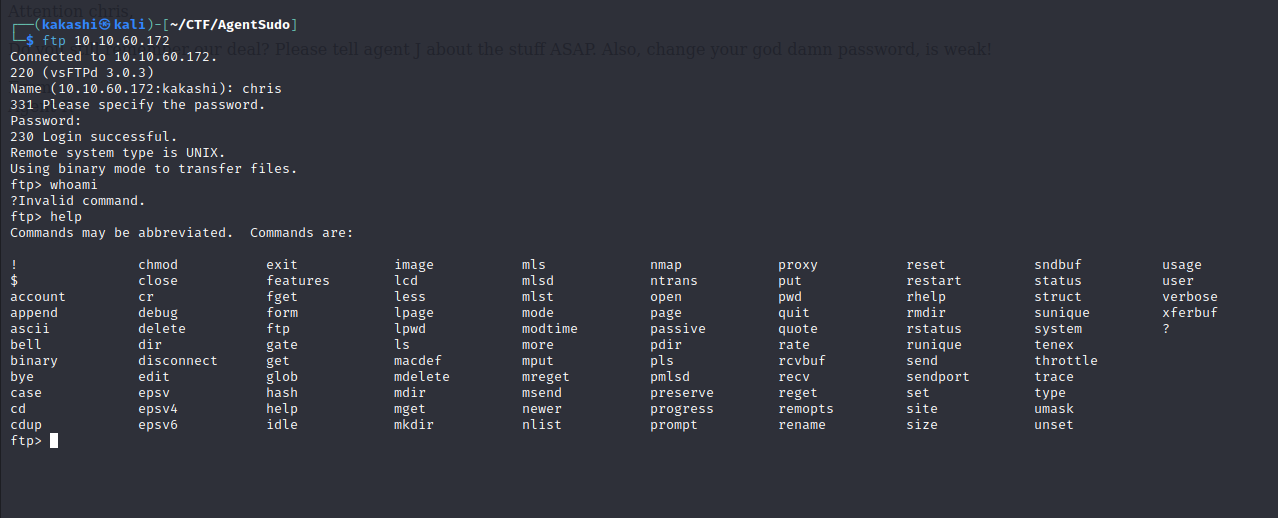
Using Hydra to Break the password for Chris.

Hydra -l chris -P /usr/share/wordlists/rockyou.txt ftp://10.10.60.172

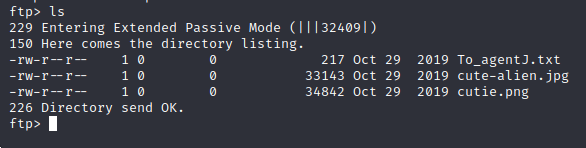


We Cracked the password **crystal** for username chris

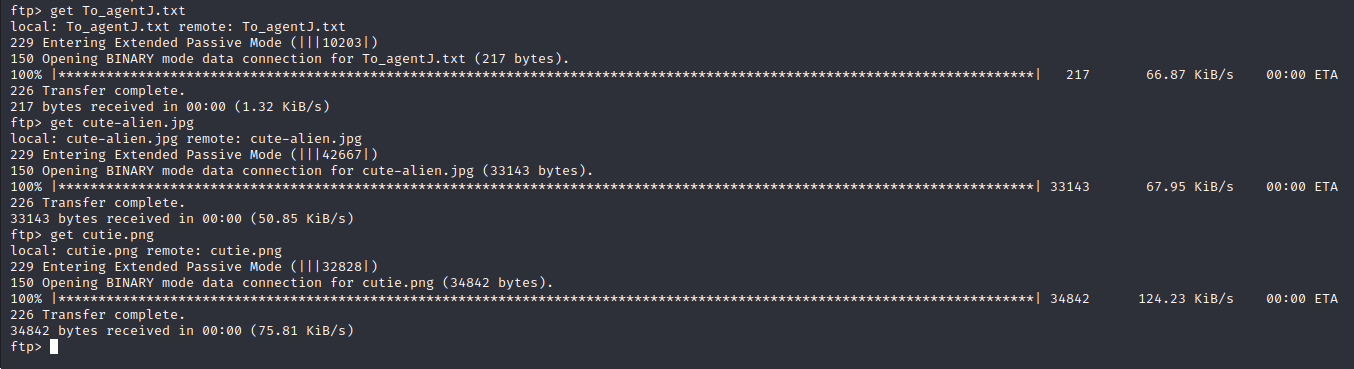
Lets try ftp login with the obtained Credentials.



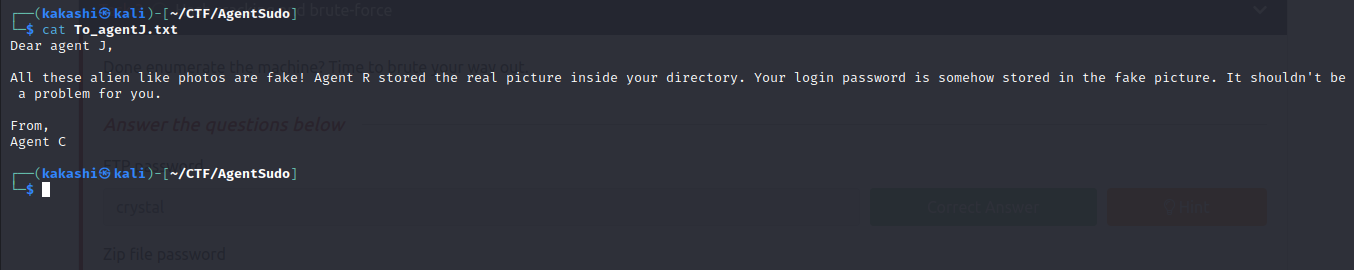
We have Logged in Successfully, there we find 3 files 2 images and a message file



We have Downloaded those 3 files to our machine using get command to examine it.

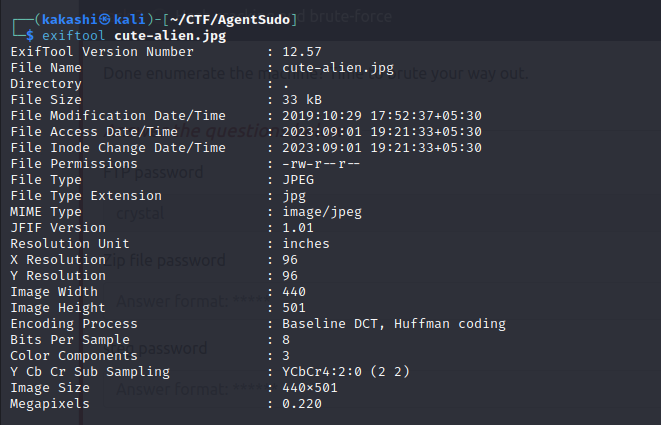


While Examining the text file they mentioned the Real image is stored in Agent J directory and the 2 images are fake and the login password for Agent J is stored in this images.

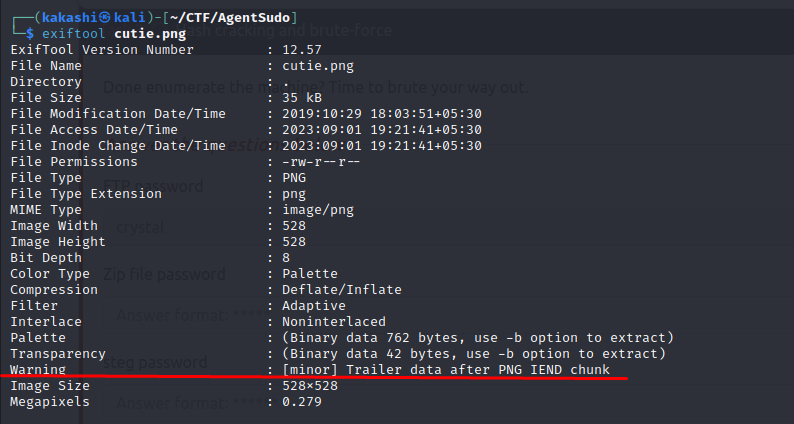


From the text file we got information about those images. Lets analyze the images separately for additional information and to extract the login password of Agent J.

Use exiftool to extract metadata from the images.



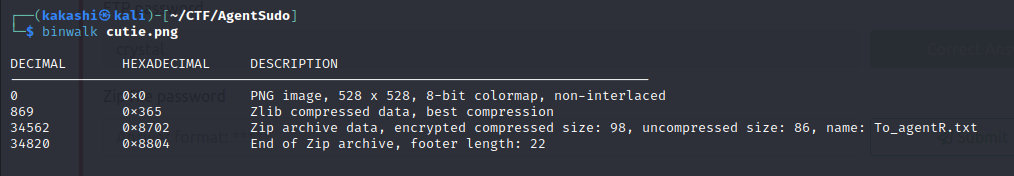
Cute-alien.jpg seems normal as of now.



While Analyzing the cutie.png we have found a warning states that there is a trailer data(file) embedded with the image.

To Extract the Embedded image from the image we can use binwalk tool.

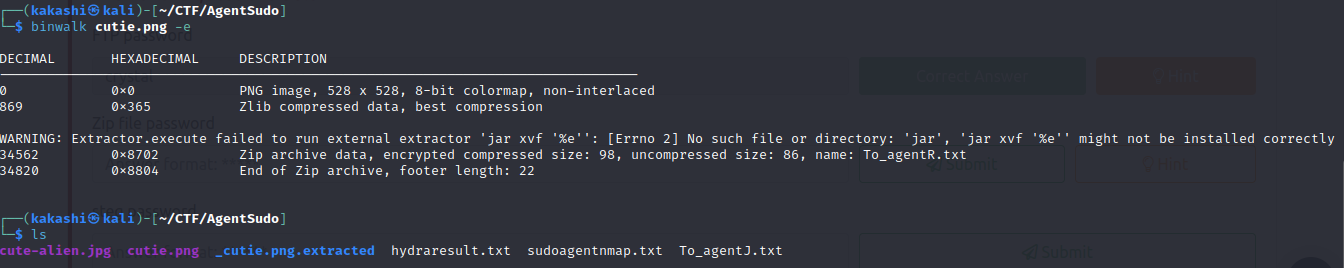
Binwalk cutie.png

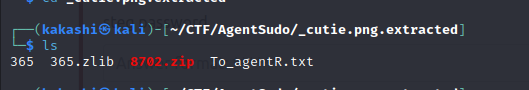


We found a zip file which is encrypted inside that we have text file.

To Extract the embedded file from the image we use -e flag to the binwalk command.

binwalk -e cutie.png

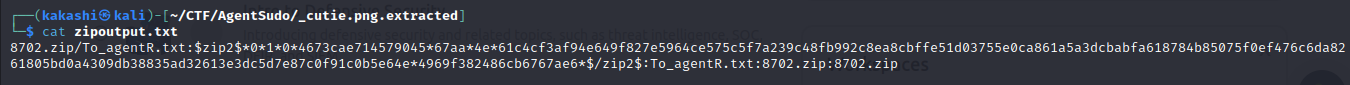




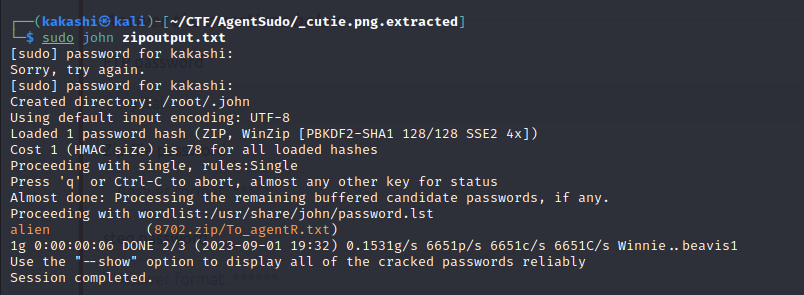
The Next Step is to crack the zip file password for that we use johntheripper tool

There is a extension for cracking the zip file password in the john the ripper that is zip2john we use that password to crack the zip file.

zip2john 8702.zip > zipoutput.txt



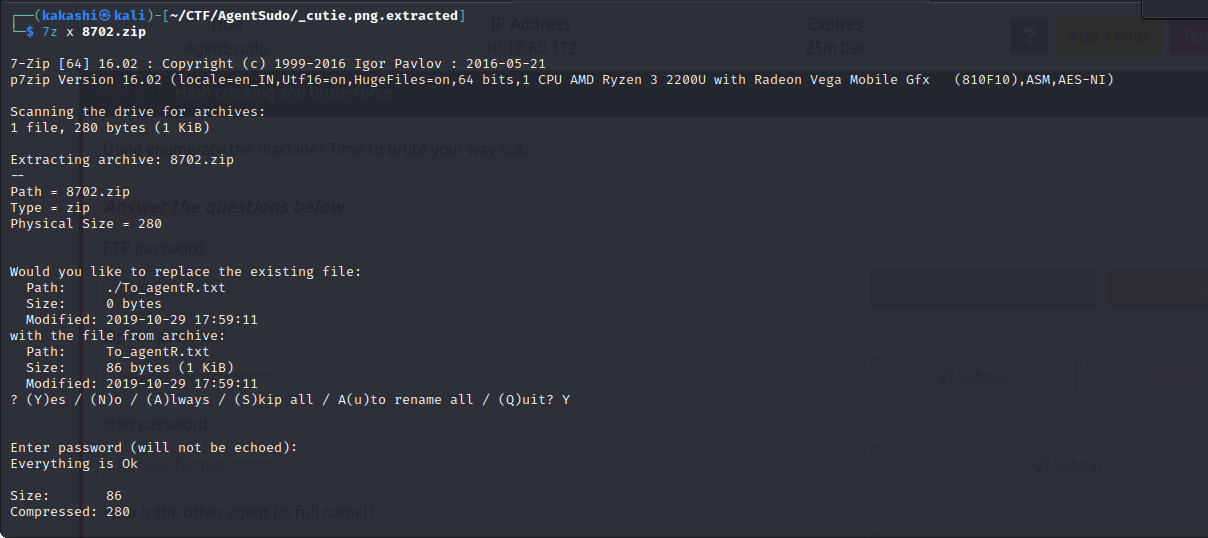
We got the hash for the password we use johntheripper tool to decrypt it

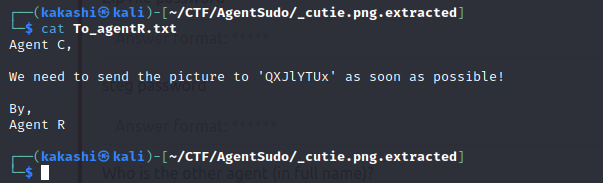


We found the password of the zip file **alien**

Next step is to unzip the files from the encrypted zip file using 7z

7z x 8702.zip

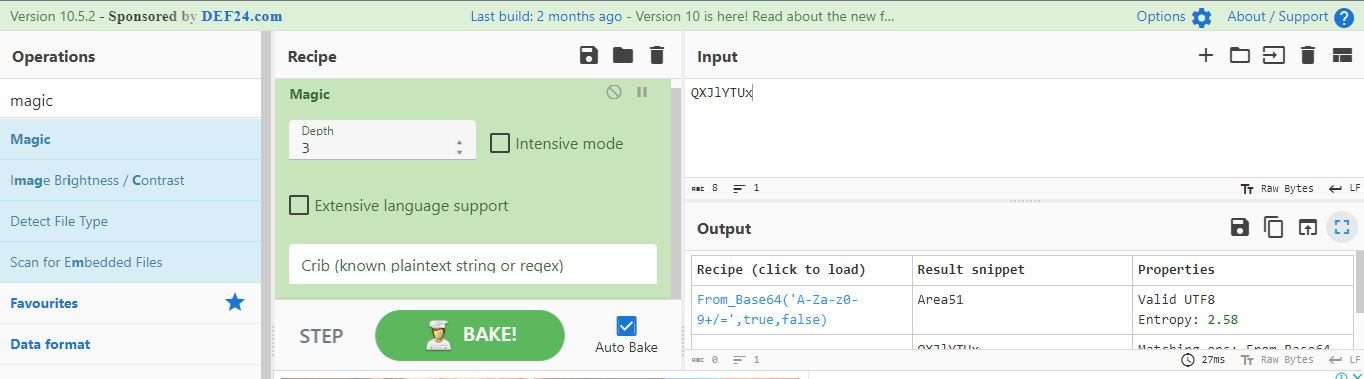




We got the hash of the password.

Go to cyberchef to decrypt it.

In cyberchef there is a option called **magic** which will automatically Decide which algorithm is used and gives us output.



We found the password Area51 which can be helpful.

The remaining is the other image cute-alien.jpg where the actual message is there.

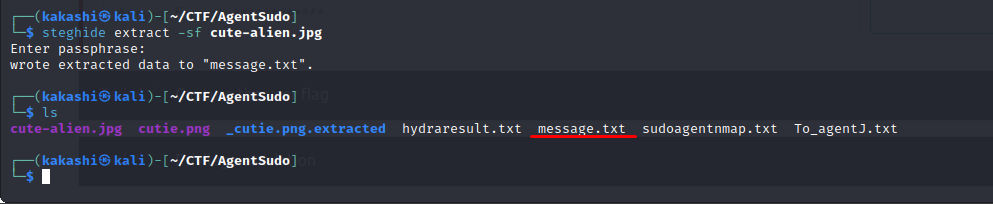
The method of hiding information in the image is called steganography, To Implement Steganography we can use steghide tool to hide data or extract data from images.

In our case we can use steghide in the cute-alien.jpg to extract information.

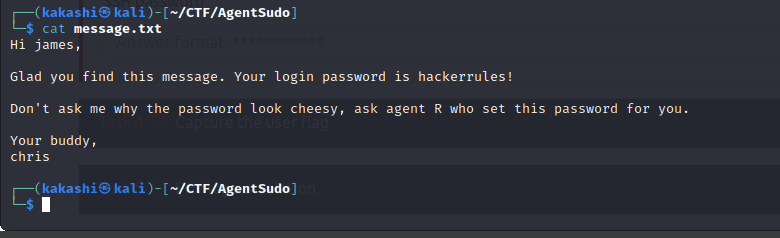
steghide extract -sf cute-alien.jpg

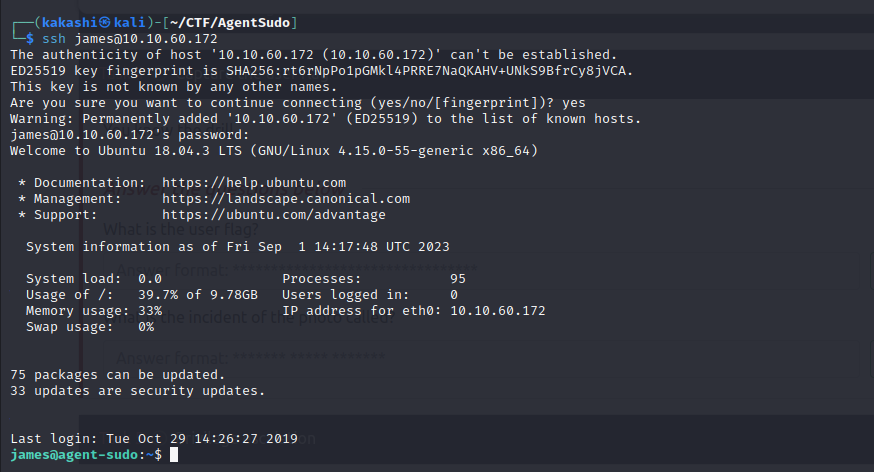
Enter password Area51

We got message.txt



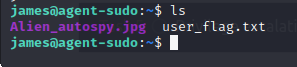
Analyzing the message.txt file we got username james and the password hackerrules! We can use this credential for ssh login to get the flags for this CTF.





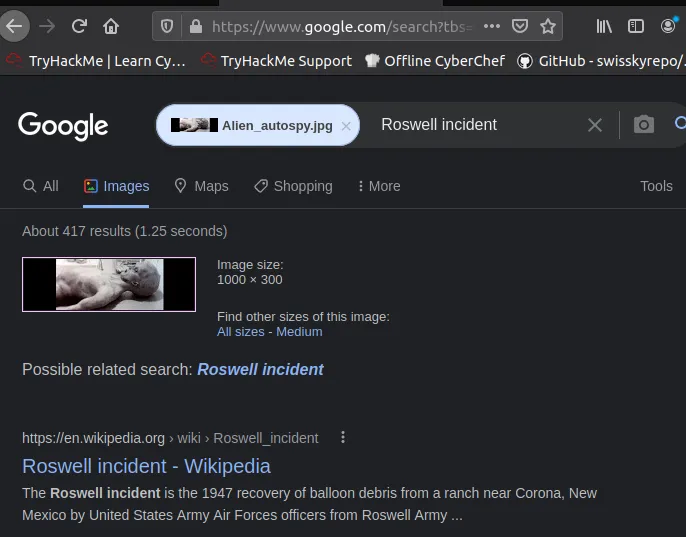
The SSH Login is successful, Analyze the files in the ssh system.

We got 2 files 1 flag and a image.



We got the user flag. And to answer the second question we need to copy the image to our kali machine and use google images to reverse search and read article related to it.

While reverse image search the Alien\_autospy.jpg we got



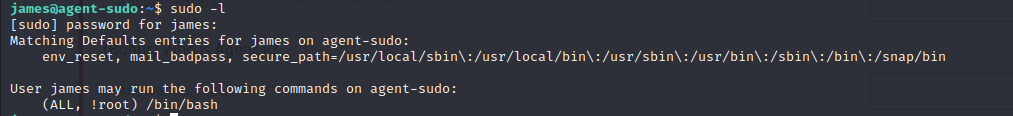


We got the answer Roswell alien autopsy.

**Step 5: Privilege Escalation**

To Elevate our Privilege to root we can able to find the root flag of the CTF.

The first step in the privilege Escalation is to check the current user permissions and privileges to check that type sudo -l



We found that /bin/bash can be run as root for all the user we can exploit that.

The CVE related to it is:

CVE-2019-14287

[Linux Privilege Escalation - Vulnerable Sudo Version - StefLan's Security Blog (steflan-security.com)](https://steflan-security.com/linux-privilege-escalation-vulnerable-sudo-version/#:~:text=The%20following%20command%20can%20be%20used%20in%20Unix-like,Sudo%20%3A%20sudo%20-V%20%7C%20grep%20%22Sudo%20ver%22)

Try the command mentioned in the blog to exploit the sudo vulnerability.

