Report PSP0201 T2130 Tutorial – Week 6

Group name: **Marceline**

|  |  |  |
| --- | --- | --- |
| ID | Name | Role |
| 1211100899 | Muhammad Shahril Aiman | Leader |
| 1211101533 | Muhammad Aniq Fahmi | Member |
| 1211101303 | Aiman Faris | Member |
| 1211102759 | Muhammad Zaquan | Member |

**Day 21 - Time for some ELForensics**

**Tools used: AttackBox, Remina, PowerShell**

Solution/Walkthrough:

**Question 1: Read the contents of the text file within the Documents folder. What is the file hash for db.exe?**

=596690FFC54AB6101932856E6A78E3A1



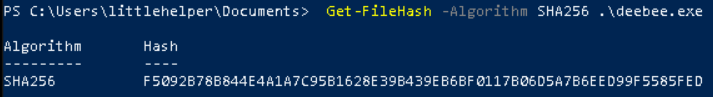
**Question 2: What is the MD5 file hash of the mysterious executable within the Documents folder?**

=5F037501FB542AD2D9B06EB12AED09F0



**Question 3: What is the SHA256 file hash of the mysterious executable within the Documents folder**?

=F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED



**Question 4: Using Strings find the hidden flag within the executable?**

= THM{f6187e6cbeb1214139ef313e108cbf9}



**Question 5: What is the powershell command used to view ADS?**

= Get-Item -Path file.exe -Stream \*



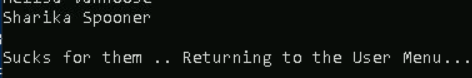
**Question6: What is the flag that is displayed when you run the database connector file?**

= THM{088731ddc7b9fdeccaed982b07c297c}



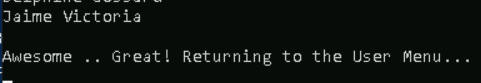
**Question 7: Which list is Sharika Spooner on?**

= Naughty list



**Question 8:Which list is Jaime Victoria on?**

= Nice list



**METHODOLOGY:**

We deploy the AttackBox, waiting for Ip address appear and use Remina to connect to the remote machine. For Server provide (10.10.198.97) we use it to create new profile in the remote desktop preference with (User name: littlehelper) and (User password: iLove5now!). After we save and connect the server and logged into the remote system, we open the PowerShell to solve the today task. First, we use (cd. \Documents\) and dir. to get the length name of the file (deebee.exe). Then, we continue running the following command: (Get-FileHash ‘.\db file hash.txt’) to solve question1. Next, we run the command (Get-FileHash -Algorithm MD5 deebee.exe) for the question2. To solve the question3 we replace the command MD5 to SHA256. Furthermore, we run the command (C:\Tools\strings64.exe -accepteula deebee.exe) to scan the mysterious hidden flag within the executable. We view the ADS using Powershell: (Get-Item -Path file.exe -Stream \*) and pay attention to the Stream and Length which is hidedb. We lastly use command to run to launch the hidden executable hiding within ADS: (wmic process call create $(Resolve-Path .\deebee.exe: hidedb) and it shows us the flag and the naughty and nice list to directly finished the today task.

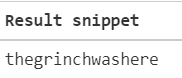
**Day 22 - Elf McEager becomes CyberElf**

**Tools used: AttackBox, Remina, KeePass, CyberChef**

Solution/Walkthrough:

**Question 1: What is the password to the KeePass database?**

= thegrinchwashere



**Question 2: What is the encoding method listed as the 'Matching ops'?**

= base64



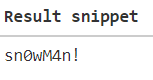
**Question 3: What is the note on the hiya key?**

= Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P



**Question 4: What is the decoded password value of the Elf Server?**

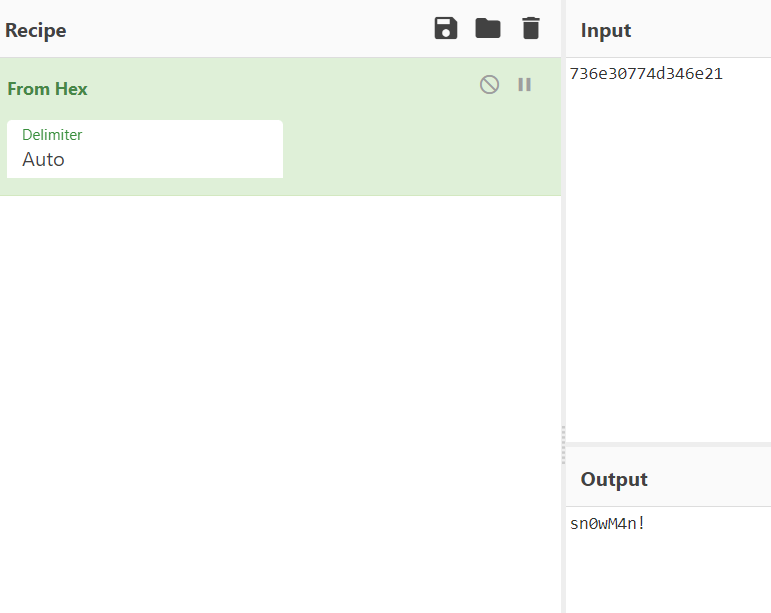
= sn0wM4n!



**Question 5: What was the encoding used on the Elf Server password?**

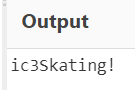
= hex





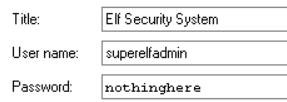
**Question 6: What is the decoded password value for ElfMail?**

= ic3Skating!



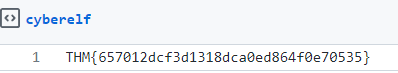
**Question 7: What is the username:password pair of Elf Security System?**

= superelfadmin:nothinghere



**Question 8: Decode the last encoded value. What is the flag?**

= THM{657012dcf3d1318dca0ed864f0e70535}



**METHODOLOGY:**

For this task we use same method as the previous day task which day 21 by using the AttackBox, Remina but in addition KeePass and CyberChef. We have to create new profile using the Ip address given, (User name: Administrator) and (User password: sn0wF!akes!!!) After we save and connect the server and logged into the remote system, we saw the strange-looking folder name on the desktop and click it. We open the KeePass and prompted to enter the master password (mceagerrockstar) and will get a message stating that the key is invalid meaning we have to decode the encrypted. First, we visit the CyberChef website and use the Magic recipe to decode the strange-looking folder name (dGhlZ3JpbmNod2FzaGVyZQ== folder) by simply drag and drop it into the Recipe window to receive the output which is the password for the KeePass. Now that we have unlocked the KeePass there are more encodings within the KeePass database file, we can easily solve the rest of the question. To decoded password value of the Elf Server we use Hex recipe and to decoded password value for ElfMail we use HTML Entity. Finally, for the flag we decoded the value from the Elf Security System by using From Charcode recipe twice, comma as the delimiter and base of 10 and obtained a link from the output. We open the link (. <https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8>) and it brought us to GitHub Gist website where there is the flag shown.

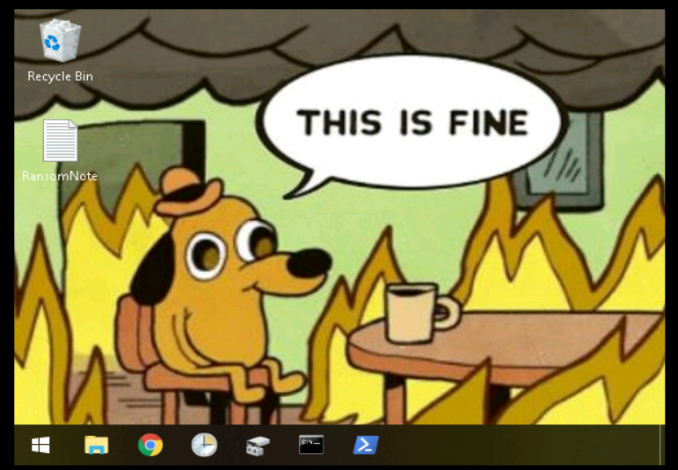
**Day 23 - The Grinch strikes again!**

**Tools used: AttackBox, Remina, CyberChef, Disk Management**

Solution/Walkthrough:

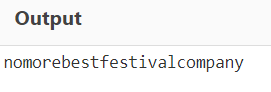
**Question 1: What does the wallpaper say?**

= THIS IS FINE



**Question 2: Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?**

= nomorebestfestivalcompany



**Question 3: At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?**

= .grinch



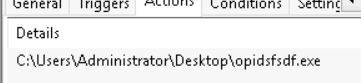
**Question 4: What is the name of the suspicious scheduled task?**

= opidsfsdf



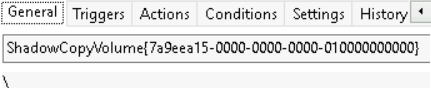
**Question 5: Inspect the properties of the scheduled task. What is the location of the executable that is run at login?**

= C:\Users\Administrator\Desktop\opidsfsdf.exe



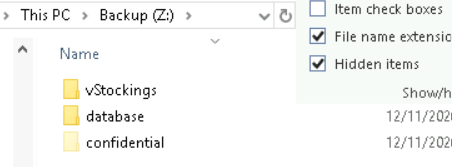
**Question 6: There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID**?

= 7a9eea15-0000-0000-0000-010000000000



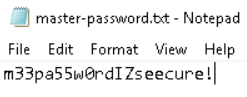
**Question 7: Assign the hidden partition a letter. What is the name of the hidden folder?**

= confidential



**Question 8:** **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?**

**Answer:** m33pa55w0rdIZseecure!



**METHODOLOGY:**

We deploy the AttackBox and use Remina and CyberChef for this task. First of all we have to create a new profie to connect to the remote machine same as recent task (day 21 & 22) but this time we have set a few things in the preferences remina remoted desktop adding the wallpaper. Next, we decrypt the fake 'bitcoin address' within the ransom note using CyberChef and put the base64 recipe to receive the value. After that, we went to disk management to change drive letter and paths in the Backup file then we click add in the dropdown a letter such as Z, and click OK. At the top, in the Volume column, we can now see that the partition has a letter assigned to it. We open Windows Explorer to navigate to the partition and solve the question 3,4 and 7. Then, we inspect the properties of the scheduled task to solve the question 5 and 6. Lastly, we went back to the confidential folder and followed the instruction in the question 8 to restore pervious version of the folder to gain the password.

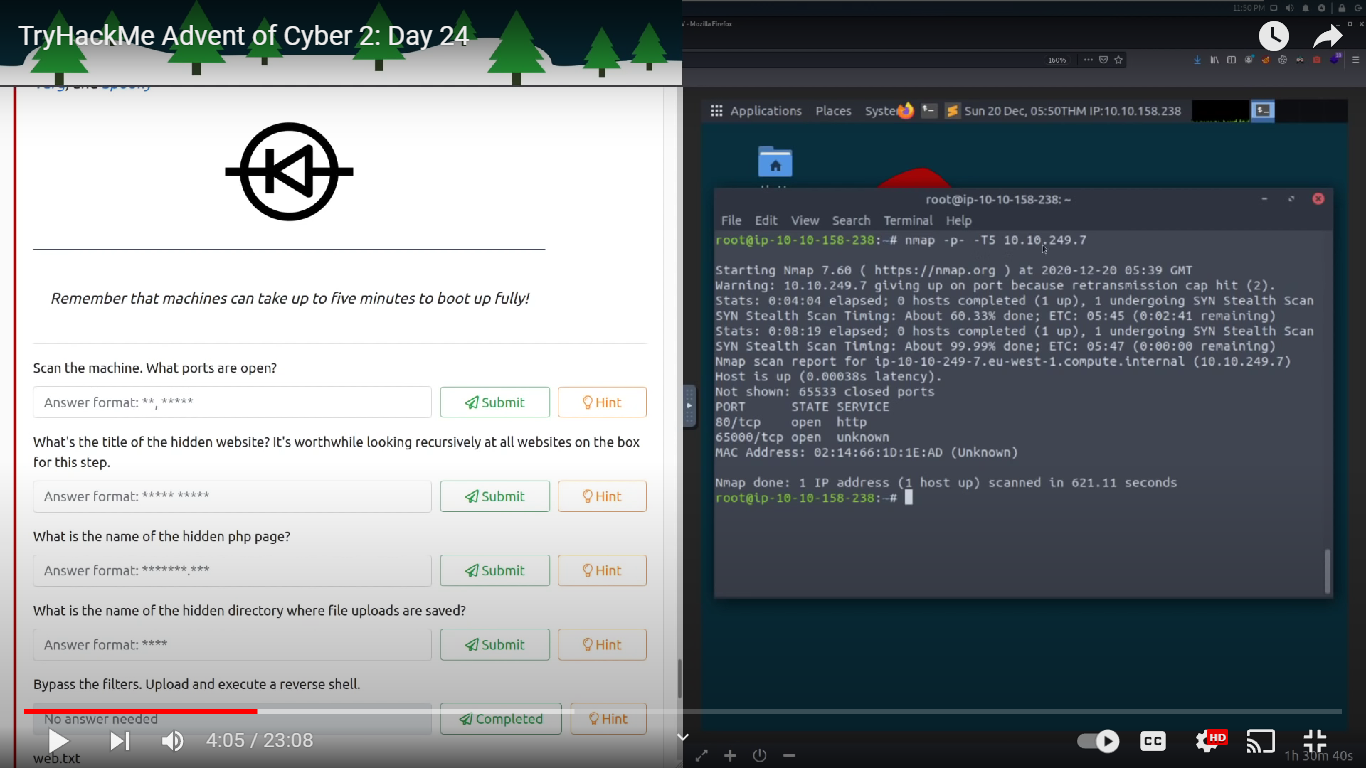
**Day 24- Final Challenge The Trial Before Christmas**

**Tools used: KALI LINUX,BURPSUITE,FIREFOX,MYSQL,ATTACKBOX**

Solution/Walkthrough:

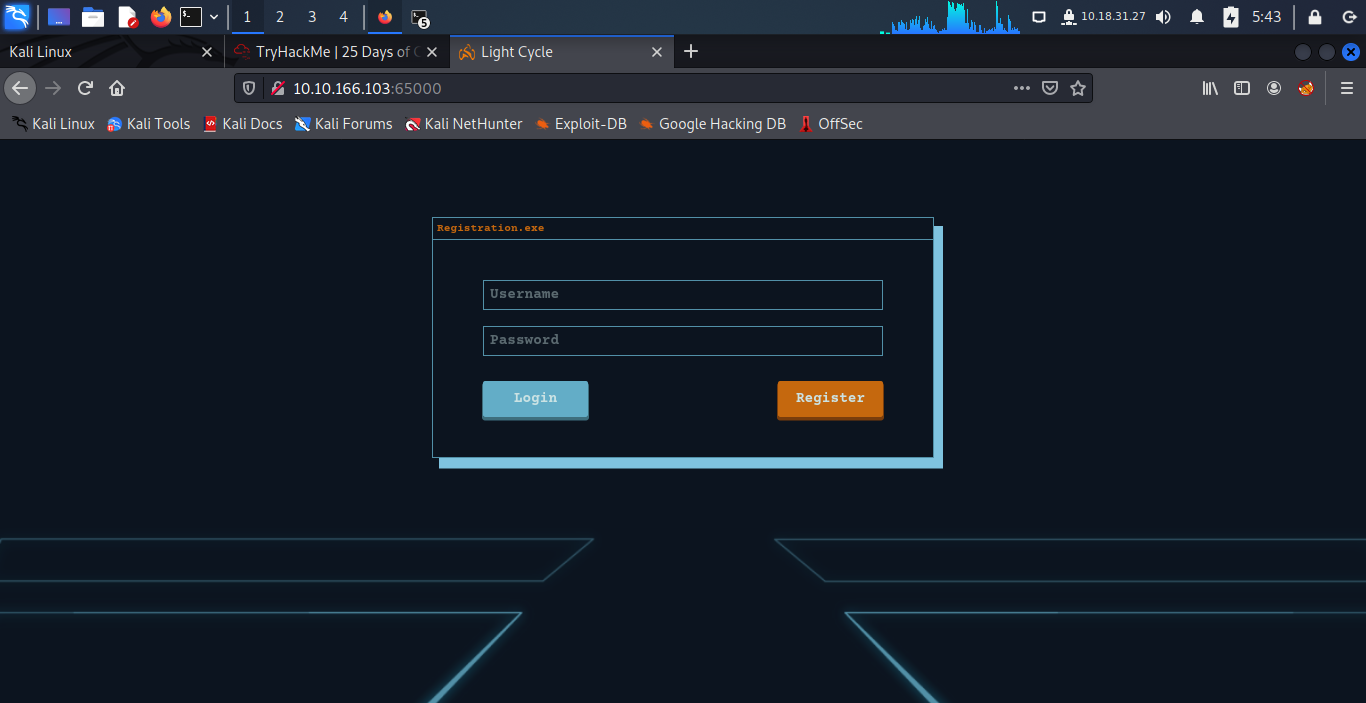
**Question 1: Scan the machine. What ports are open?**

**Answer** :80, 6500



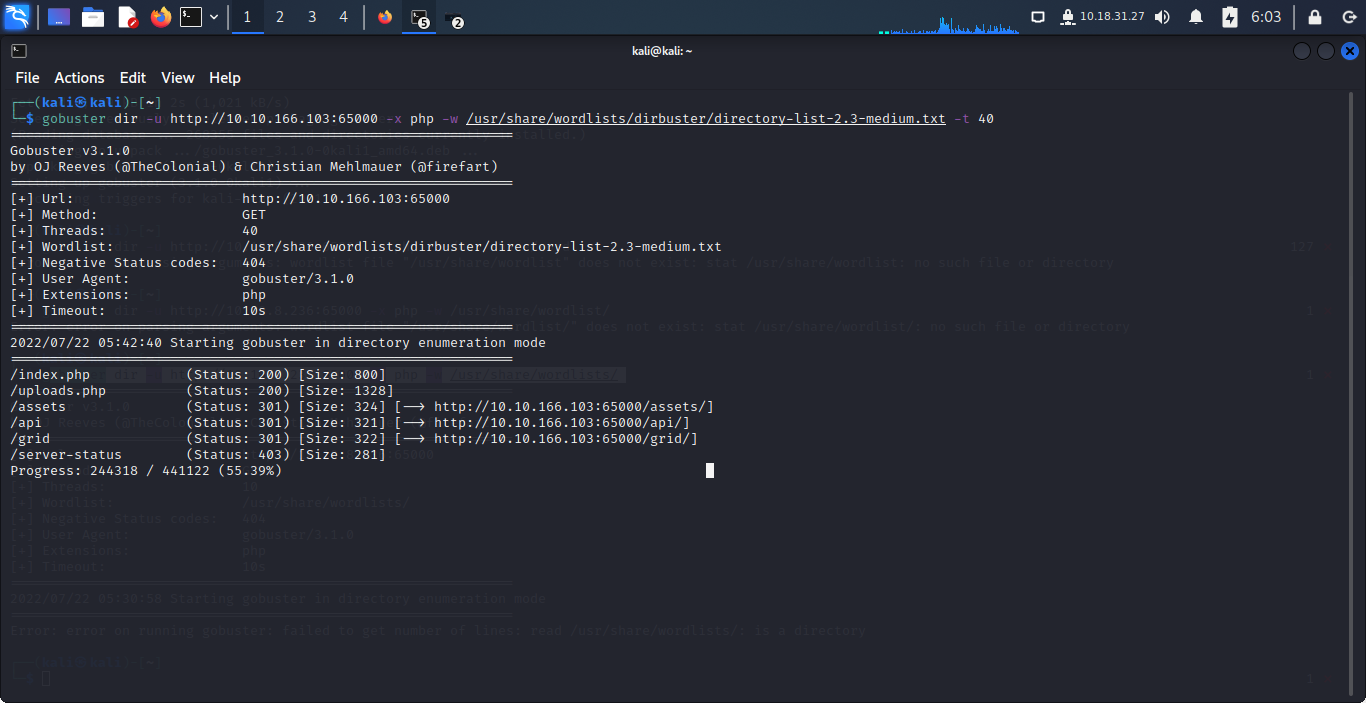
**Question 2: What's the title of the hidden website?**

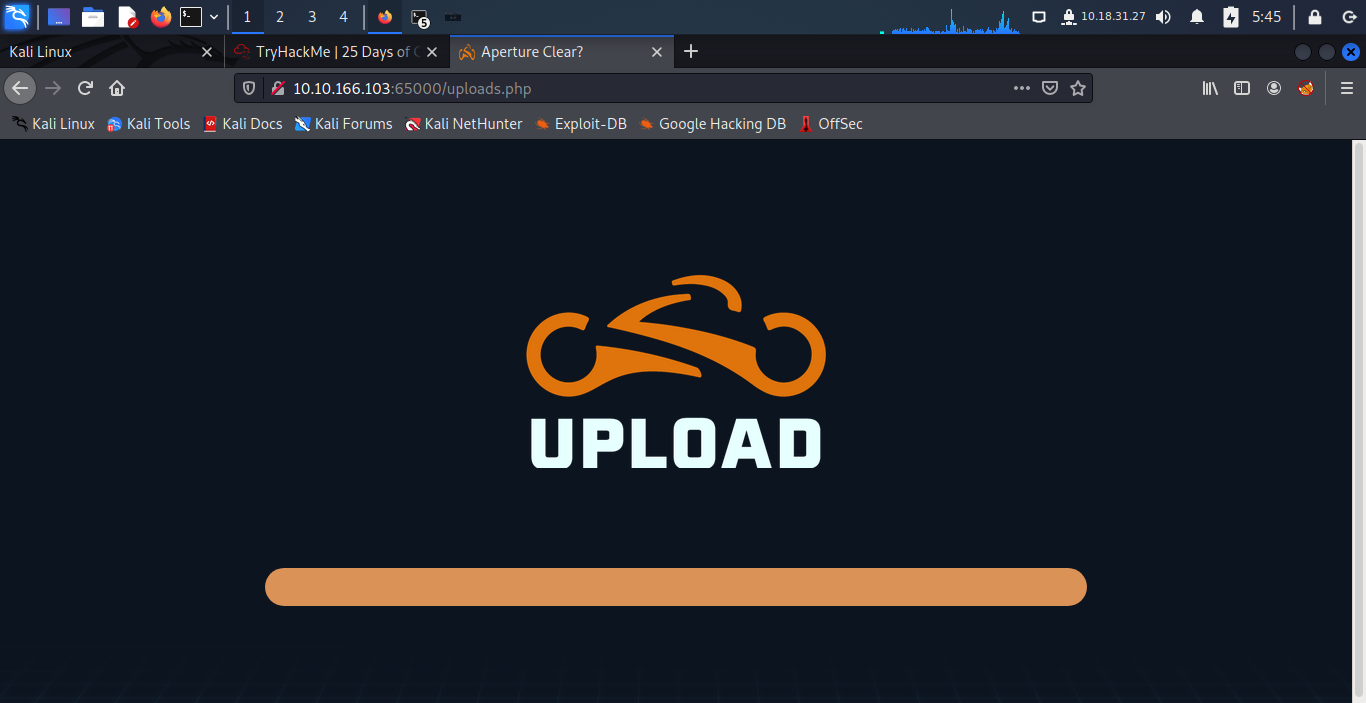
**Answer :** Light Cycle



**Question 3 :What is the name of the hidden php page?**

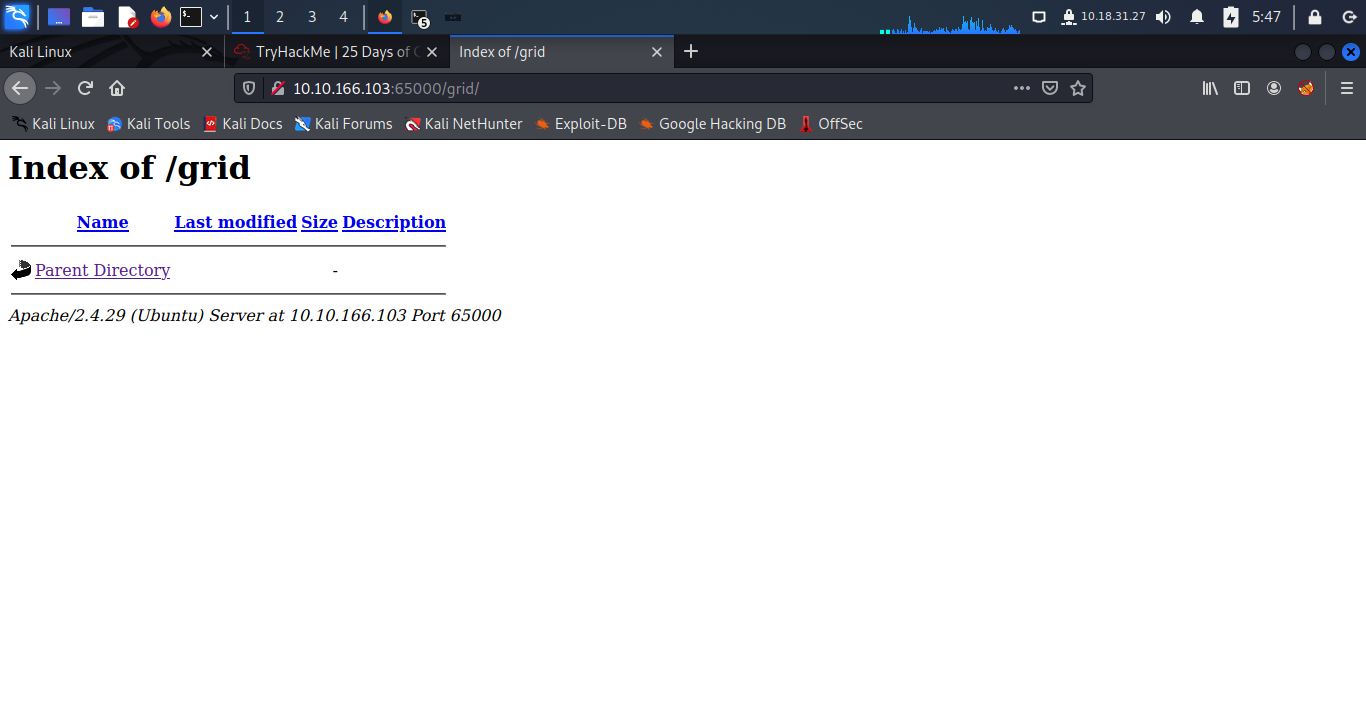
**Answer**: /uploads.php





**Question 4: What is the name of the hidden directory where file uploads are saved?**

**Answer**: /grid

**Question 5: What is the value of the web.txt flag?**

**Answer**:THM{ENTER\_THE\_GRID}

**Graphical user interface, application

Description automatically generated**

**Graphical user interface, text, application, email

Description automatically generated**

**A picture containing table

Description automatically generated**

**Graphical user interface

Description automatically generated with medium confidence**

**A picture containing graphical user interface

Description automatically generated**

**A screenshot of a computer

Description automatically generated with medium confidence**

**Text

Description automatically generated**

**Text

Description automatically generated**

**A screenshot of a computer

Description automatically generated with medium confidence**

**Shape

Description automatically generated**

**Text

Description automatically generated**

**Question 6: What lines are used to upgrade and stabilize your shell?**

**Answer:** export TERM=xterm

stty raw -echo; fg

python3 -c 'import pty;pty.spawn("/bin/bash")'

Text

Description automatically generated

**Question 7: Review the configuration files for the webserver to find some useful loot in the form of credentials. What credentials do you find?**

**Answer:** tron:ifightfortheusers

A screenshot of a computer

Description automatically generated with medium confidence

**Question 8: Access the database and discover the encrypted credentials. What is the name of the database you find these in?**

**Answer**: tron

Text

Description automatically generated

Graphical user interface

Description automatically generated

Text

Description automatically generated

**Question 9: Crack the password. What is it?**

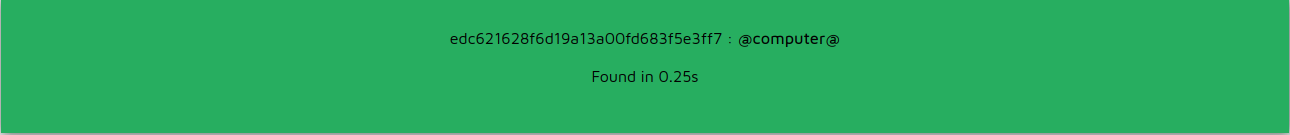
**Answer:** @computer@

Graphical user interface

Description automatically generated

Graphical user interface, text

Description automatically generated with medium confidence



**Question 10: Use su to login to the newly discovered user by exploiting password reuse. What is the user you are switching to?**

**Answer:** flynn

Shape

Description automatically generated with low confidence

**Question 11: What is the value of the user.txt flag**

**Answer:** THM{IDENTITY\_DISC\_RECOGNISED}

Text

Description automatically generated

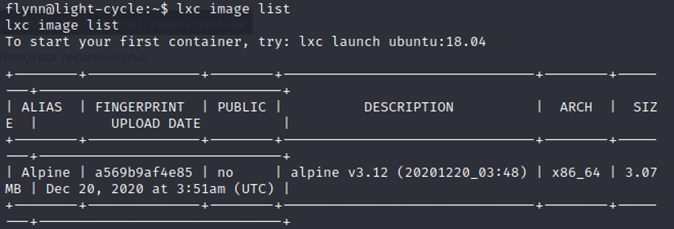
**Question 12: Check the user's groups. Which group can be leveraged to escalate privileges?**

**Answer**: lxd

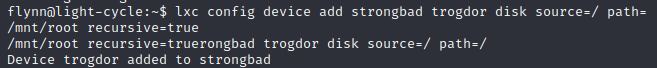


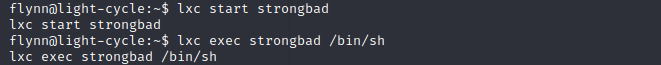
**Question 13: What is the value of the root.txt flag?**

**Answer:**THM{FLYNN\_LIVES}









A picture containing text

Description automatically generated



**METHODOLOGY**:

After gaining access to the IP address of the targeted machine, we used Nmap to do a service and version fingerprinting on the address. We discovered the web server's port number from the scan. After that, we visit the website where we could view its title. We then used Gobuster to search the website, which allowed us to locate the "/uploads.php" page and the "/grid" directory. We opened Burpsuite and went to the proxy's option to change the Intercept Client Requests before attempting to open "uploads.php." We removed the "|js$" from the intercepting rule details and saved the configuration.Once FoxyProxy was activated, we went to the "/uploads.php" page. We forwarded the GET request but discarded the one that received a response from filter.js. We disabled the intercept once we reached the "/uploads.php" page and looked at the kinds of files that the website supported. We guessed that the website would only take photos, so we made a reverse shell file, changed the IP address to our own, and gave it the name "day-24-shell.jpg.php". We configured a netcall listener and uploaded the reverse shell. After navigating to the "/grid" directory, we turned on the reverse shell. To obtain a flag, we went to the /var/www directory and examined the web.txt file. After that, the reverse shell was improved and stabilised.When we went to the included files in /var/www/TheGrid and accessed the dbauth.php file to study the configuration file, we were given the credentials. With the login information we discovered in dbauth.php, we can access the database using MySQL Client. After that, we looked through the databases that were offered and found the "tron" database. After logging in, we listed all of the tables in the "tron" database. The "users" table, where we received the username and password, was deleted. We made advantage of a website that cracks passwords online. Once we had the password broken, we took advantage of password reuse by using su to log into "flynn."After that, we went to Flynn's home directory and opened the user.txt file to get another flag. After that, we looked up the user's group and took advantage of it to increase our privilege After that, we looked over the photographs the machine had. We were aware that Alpine was the image's alias. We started the container and configured the discs using a series of commands using the image. We mounted the storage and checked that we had reached the root level. Finally, we used the root.txt to retrieve the final flag.