PSP0201 Week 6 Writeup

Group Name: Hacktocrats

Members

ID	Name	Role
1211103194	NUR FARAHIYA AIDA BINTI ABD RAZAK	Leader
1211103602	NUR ALIA AMELISA SYAZREEN BINTI MOHD SULEI	Member
1211103430	AINA SOFEA BINTI AMIER HAMZAH	Member
1211103237	NURUL AIN BINTI KAMARUDIN	Member

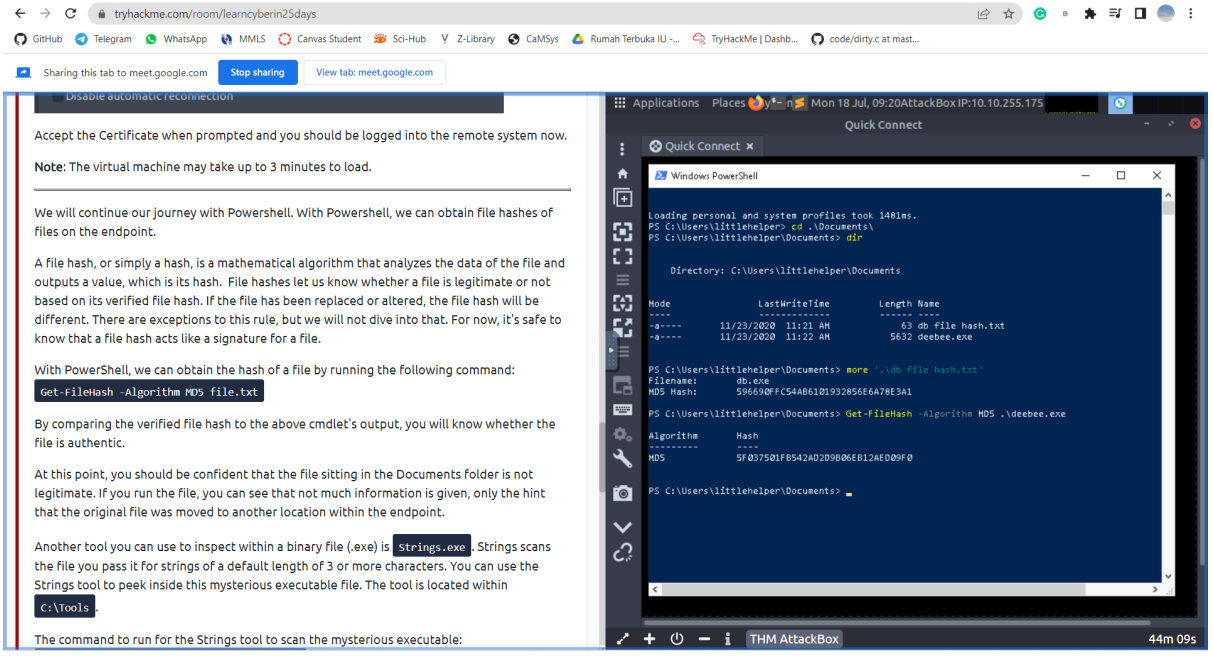
Day 21: Time for some ELForensics

Tools used: Remmina, Windows Powershell

Solution / walkthrough:

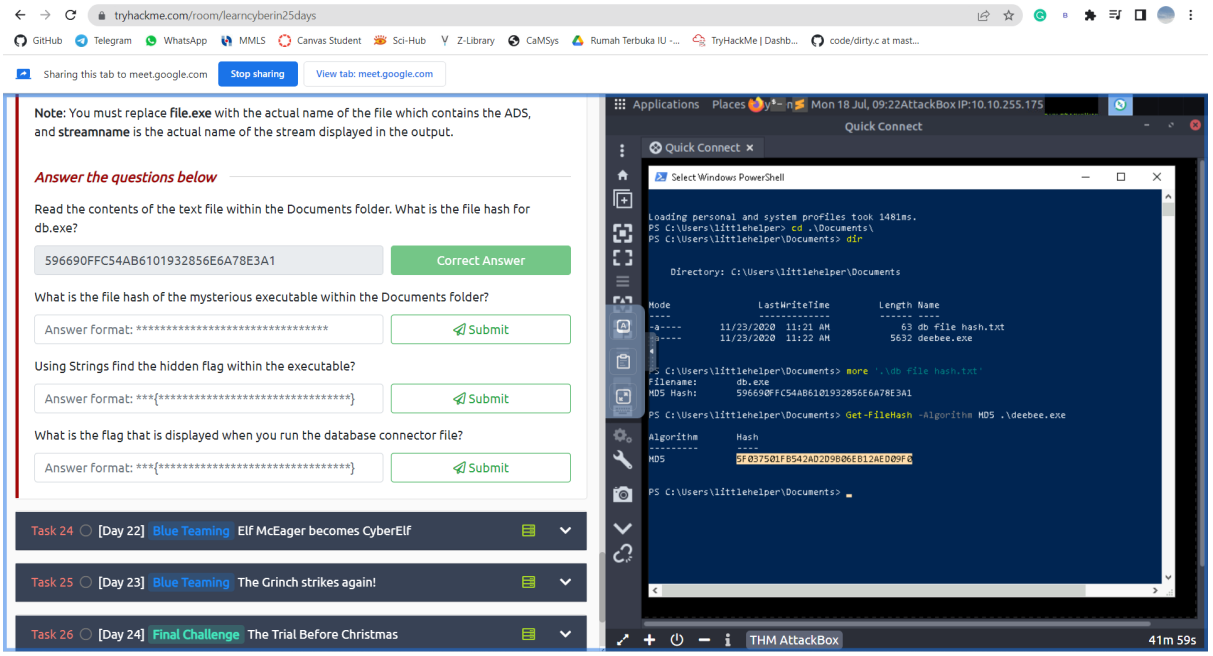
Question 1:

View the contents of the text file within the Documents folder using command *more* in powershell to display the first screen of information from db file hash.txt and successfully retrieve the MD5 Hash for db.exe.



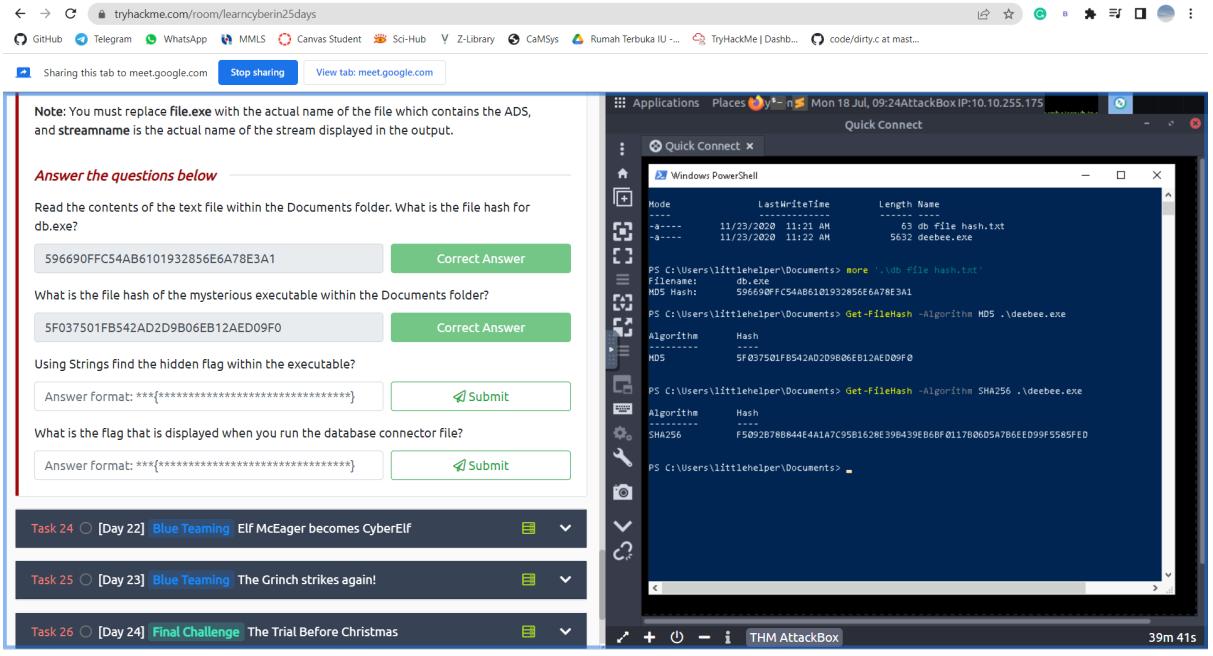
Question 2:

Type in command *Get-FileHash -Algorithm MD5 .\deebee.exe* to compute the hash value for mysterious executable within the Documents folder. This command uses MD5 algorithm and not the default SHA256 algorithm.



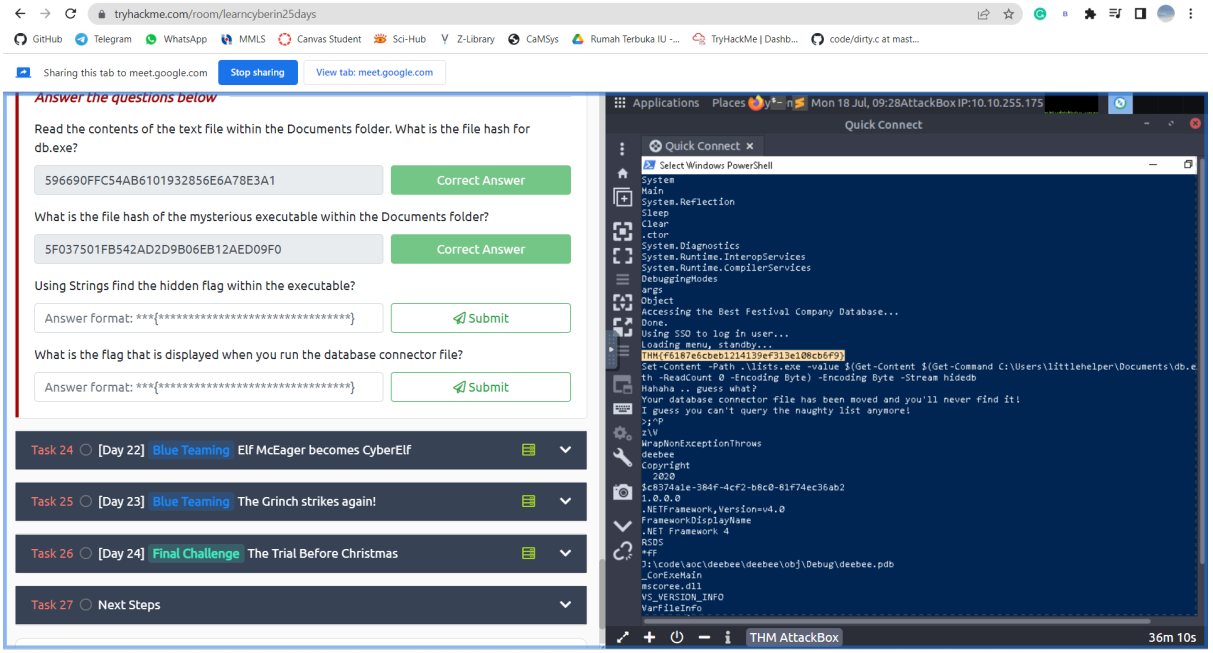
Question 3:

Change MD5 inside *Get-FileHash -Algorithm MD5 .\deebee.exe* to SHA256 to obtain the hash value of the executable file using SHA256 algorithm



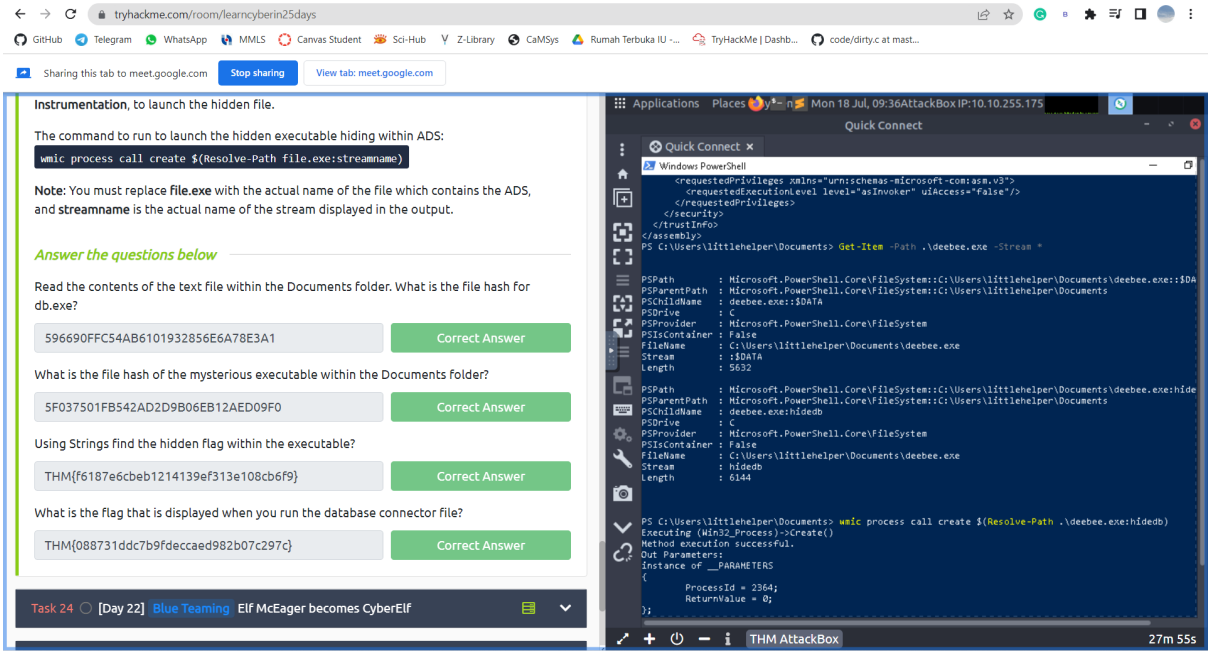
Question 4:

Use String.exe to displays strings of printable characters found in the deebee.exe file and find the flag hidden within the executable file



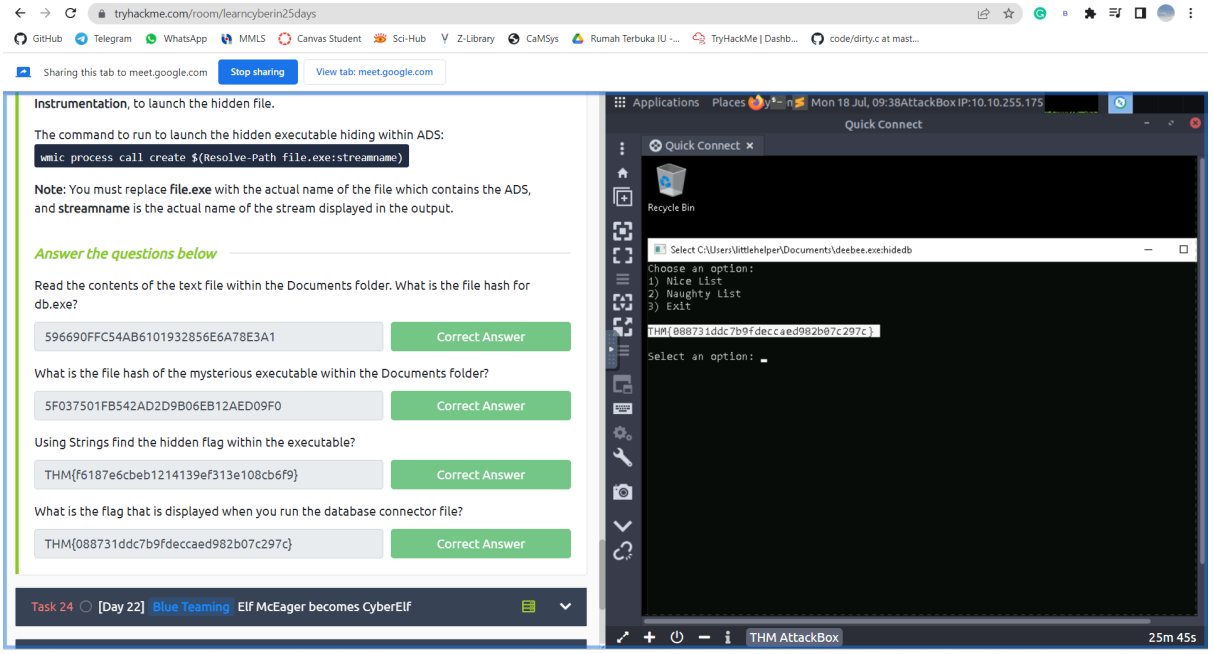
Question 5:

To view ADS of deebee.exe file in powershell, we used *Get-Item -Path .\deebee.exe -Stream ** command. *Get-Item* will get the item at specified location. *-Path* is used to specify the path to an item. Dot(.) is used to specify the current location and *-Stream ** gets all alternative data stream from the file.



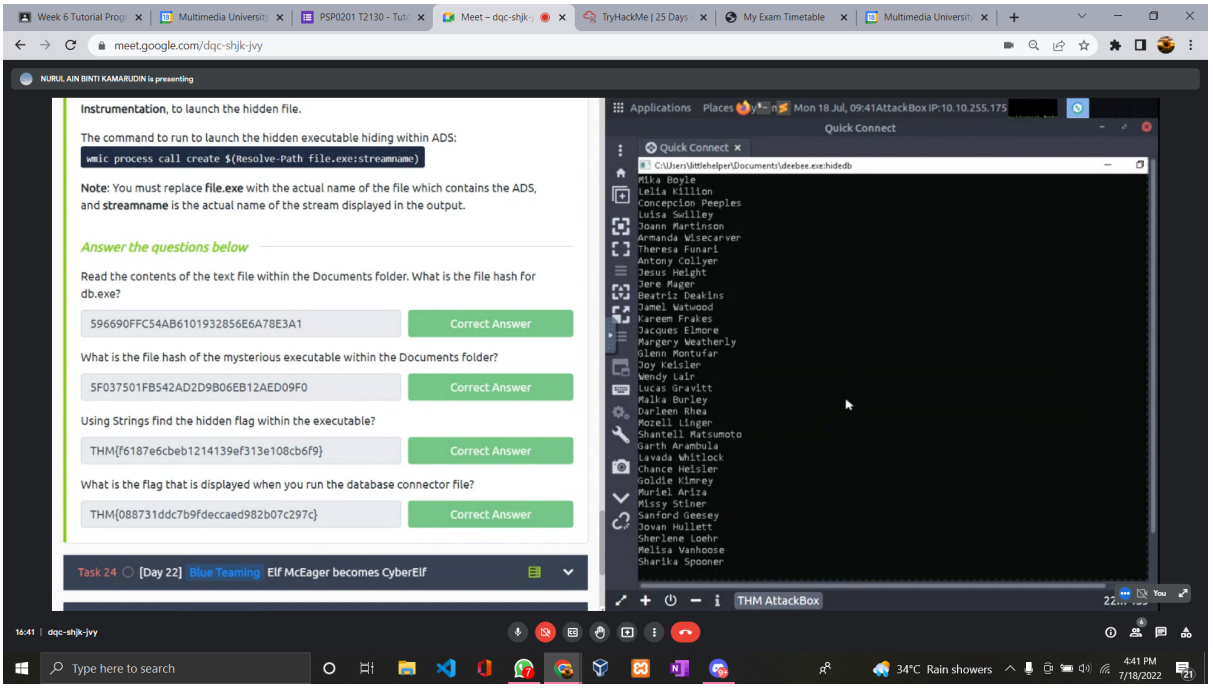
Question 6:

Run *wmic process call create $(Resolve-Path .\deebee.exe:hidedb)* command to execute database connector file hidden inside ADS. Once the file executed, we were presented with the flag Nice&Naughty List option



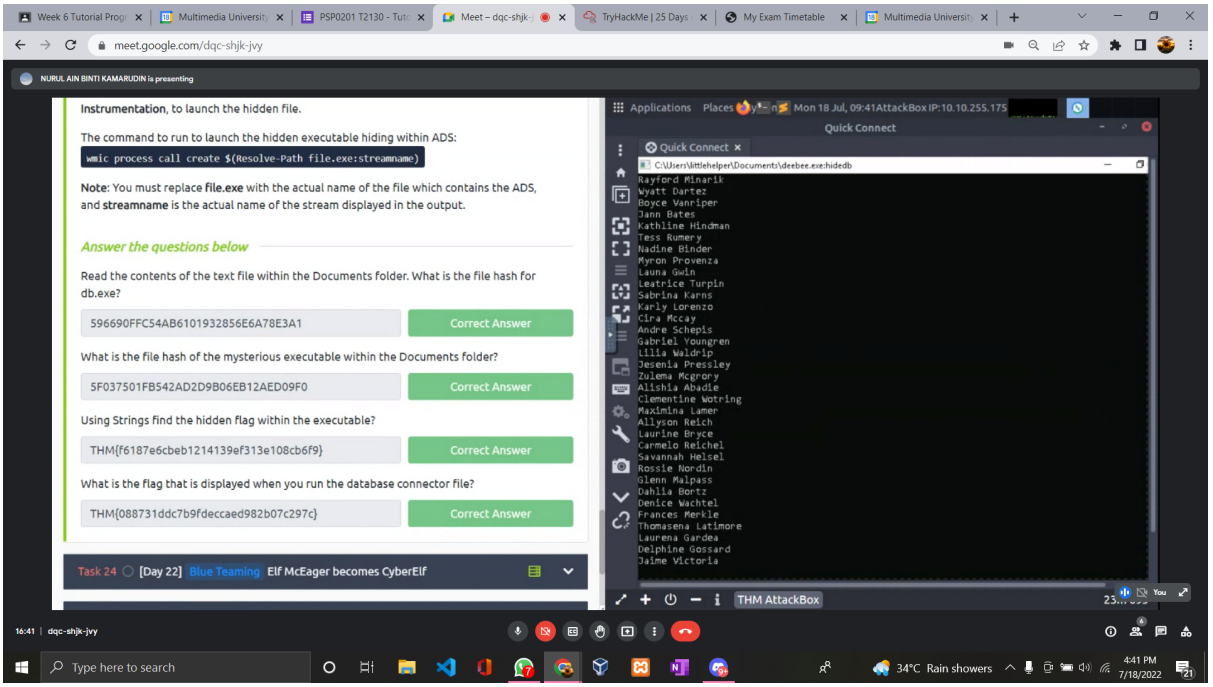
Question 7:

Type in number 2 inside select an option input box to view names inside Naughty List file. We found Sharika Spooner inside Naughty List



Question 8:

Type in number 1 inside select an option input box to view names inside Nice List file. We found Jaime Victoria inside Nice List.



Thoughts Process / Methodology:

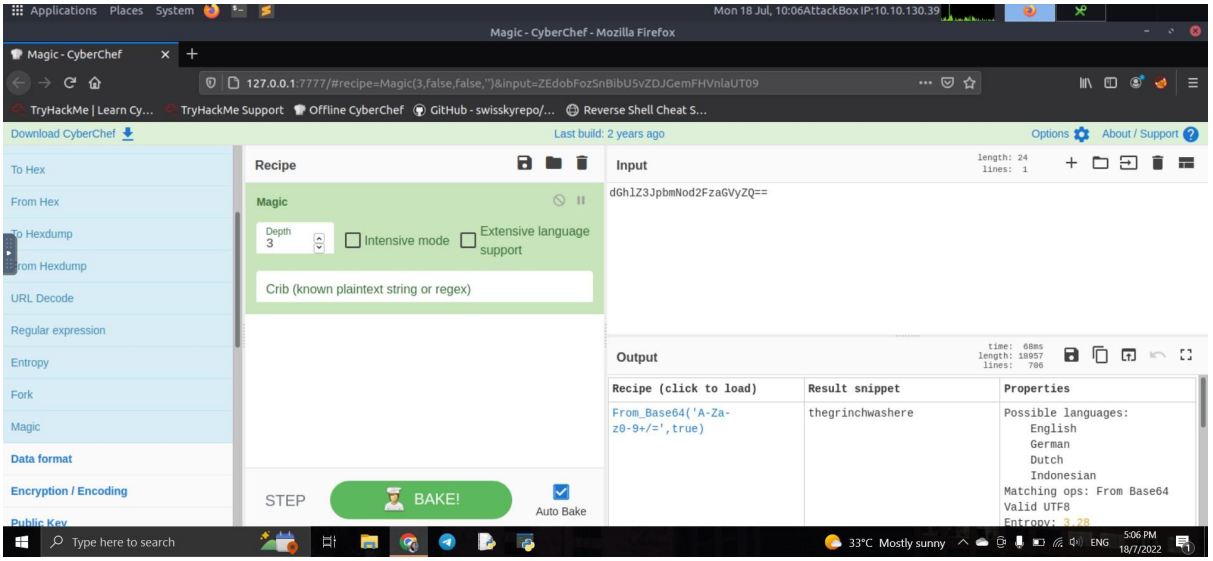
First of all, we need to open Remmina and connect to the remote machine by inputting ip address of remote machine, username and password. Make sure to change color depth to RemoteFX (32bpp). After that, we open Windows powershell and change directory to Documents. To view the hash value of db file hash.txt, we use *more* command to display the contents of the file. We then used *Get-FileHash -Algorithm MD5 .\deebee.exe* command to obtain the hash for deebee.exe. We also used SHA256 algorithm to view hash value of deebee.exe file. Next, we used tools such as String.exe to displays strings of printable characters found in the deebee.exe file. To view ADS of deebee.exe file in powershell, we used Get-Item -Path .\deebee.exe -Stream * command. Lastly, we run wmic process call create $(Resolve-Path .\deebee.exe:hidedb) command to execute database connector file hidden inside ADS.

Day 22: Elf McEager becomes CyberElf

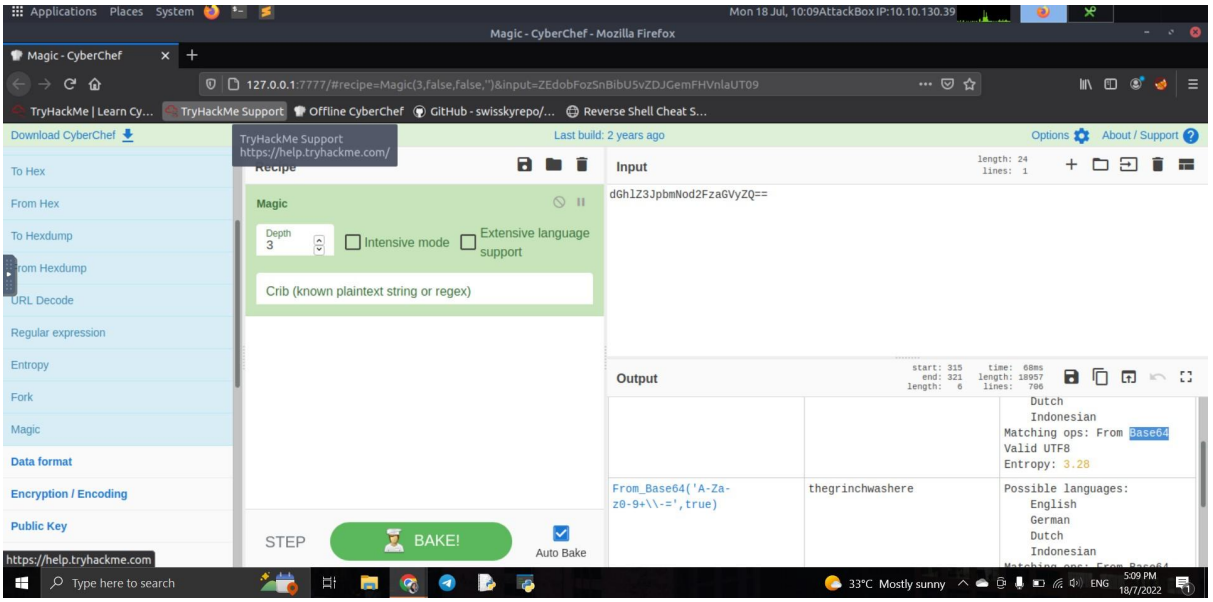
Tools used: terminal, remmina, firefox (cyberchef)

Solution / walkthrough:

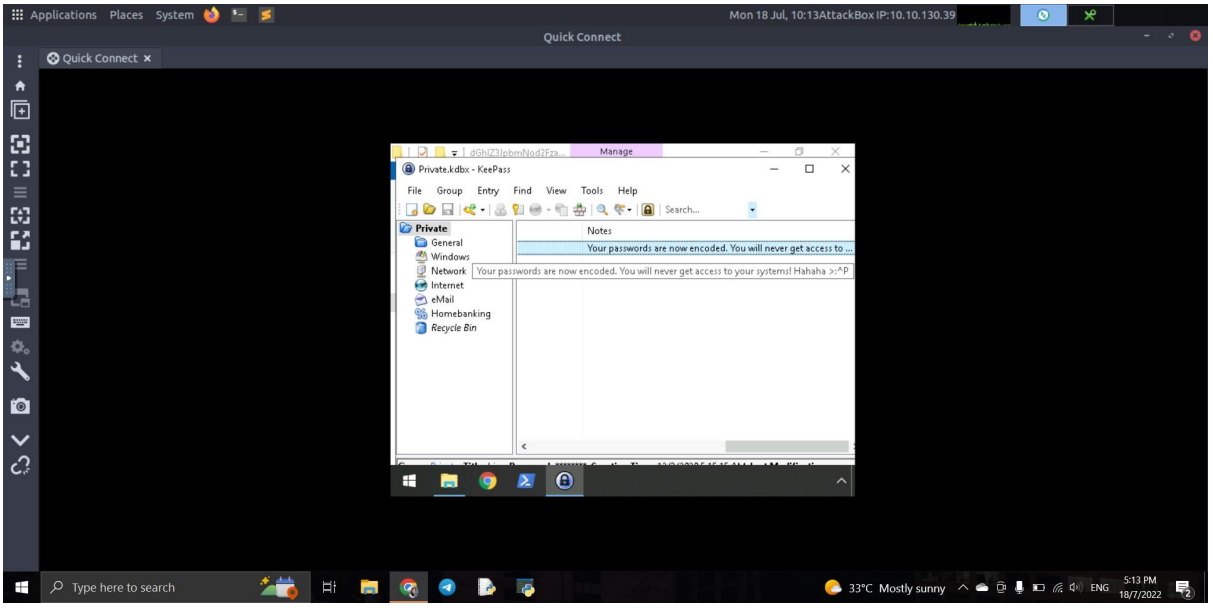
Question 1: the number that has been put in the input was received in the folder that appeared on the desktop. Then, we opened cyberchef on firefox and inserted the address of the file as the input. We used “magic” as the recipe. The answer appeared on the result snippet.



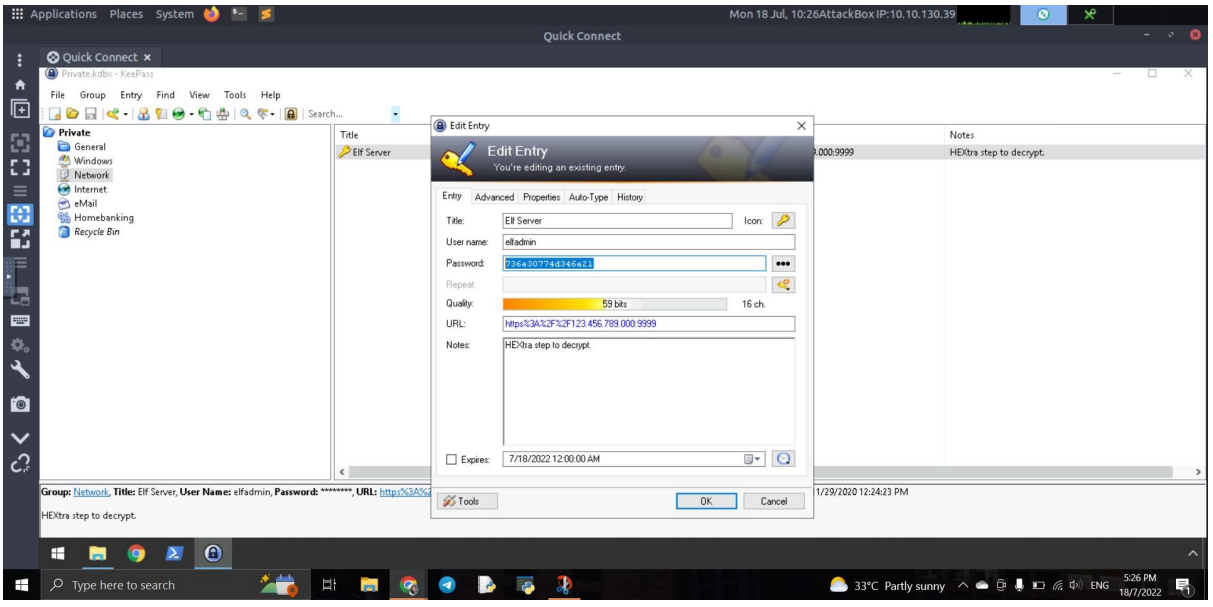
Question 2: the same step has been done as the first question, the answer has been provided at the properties as shown below.

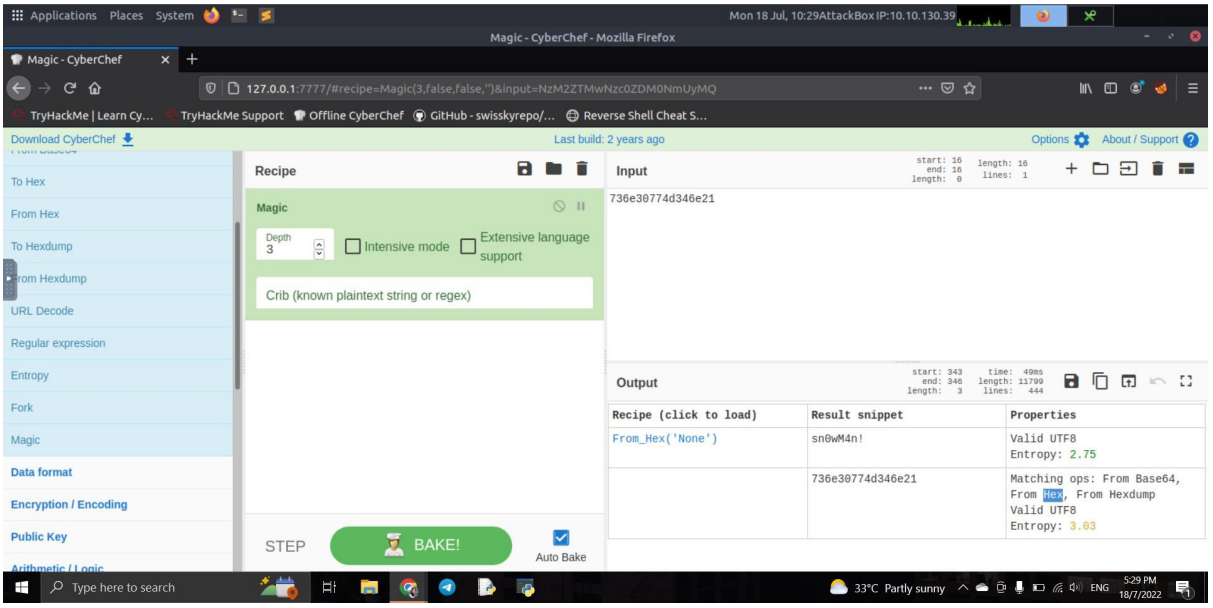


Question 3: After that, we opened KeePass at the folder and pressed the hiya key. After scrolling through the page, we found the notes for hiya key

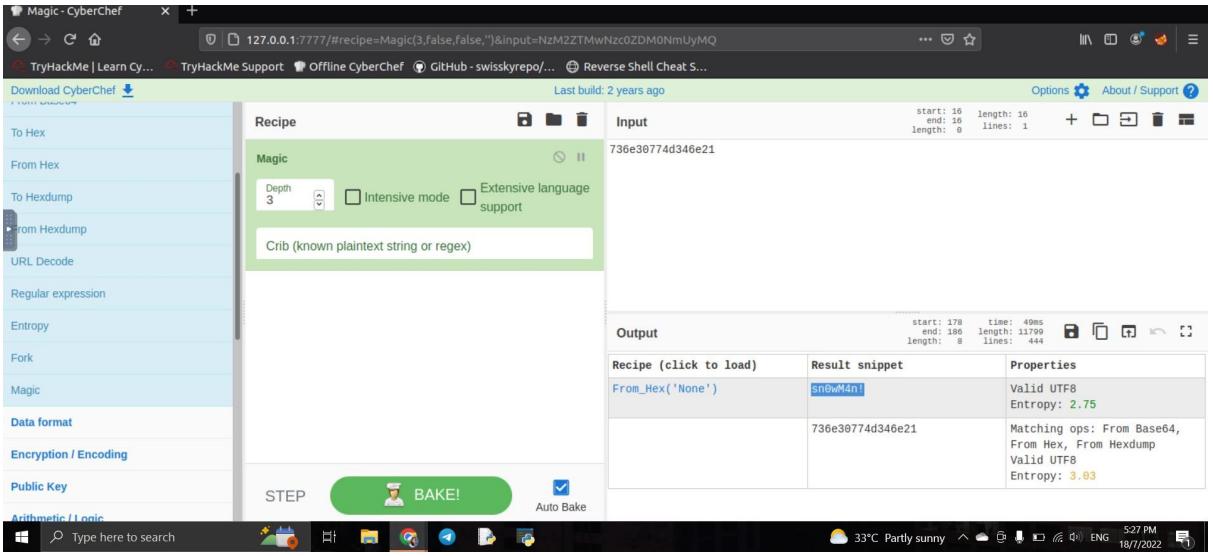


Question 4: Then, we searched for the elf server at the network folder. We pressed the network button and changed the password to viewable using the toggle button. After we receive the password, we paste it in the cyberchef and bake it using the “magic” recipe. The answer is shown at the properties which were hex.

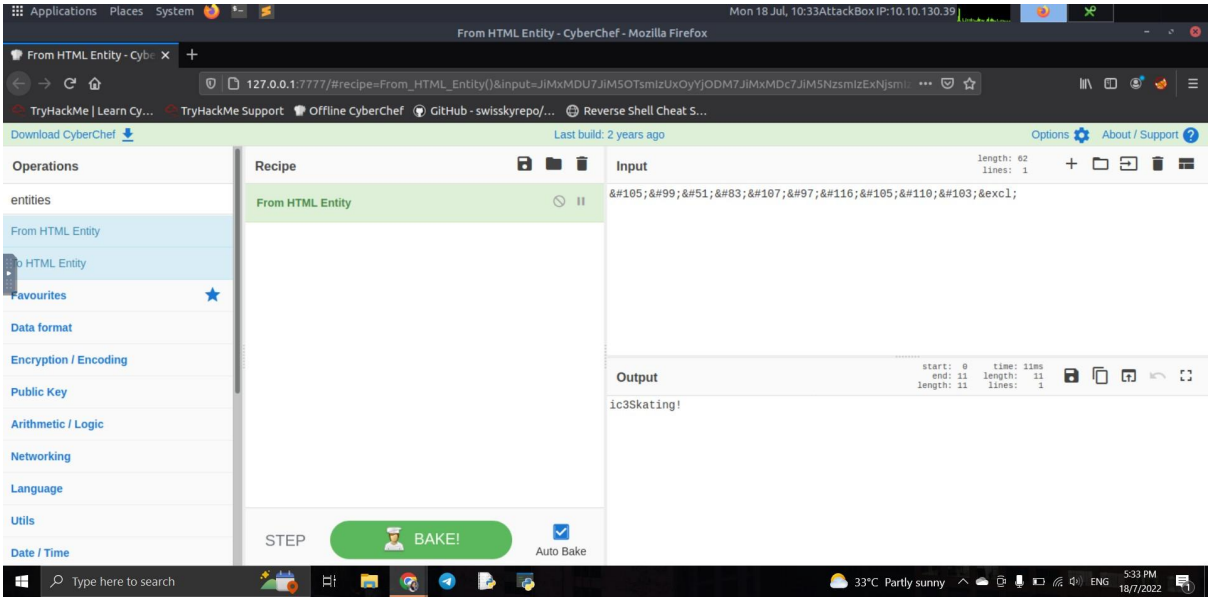




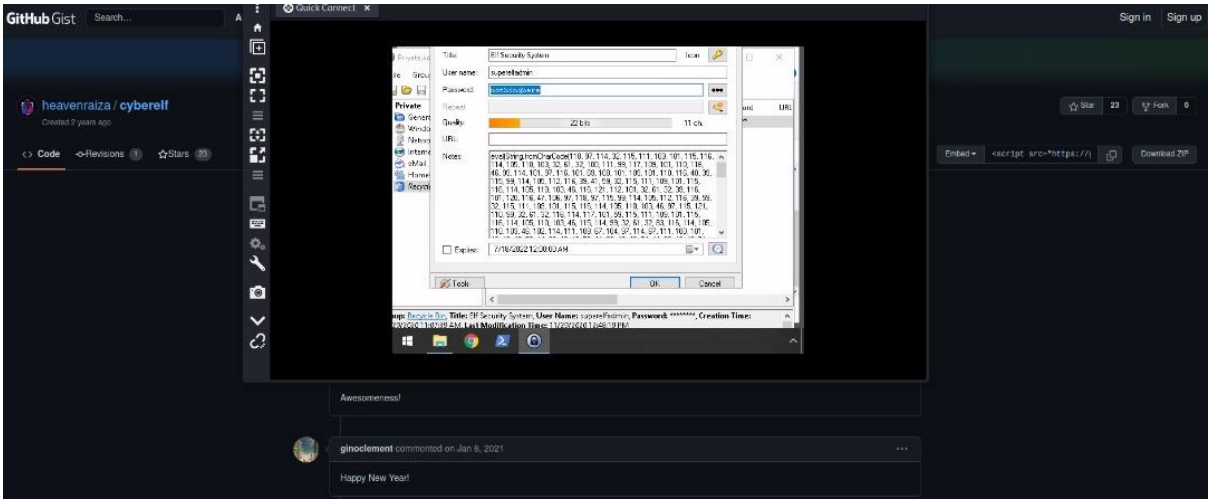
Question 5: the answer has been obtained as we searched for the previous question, it was shown at the result snippet.



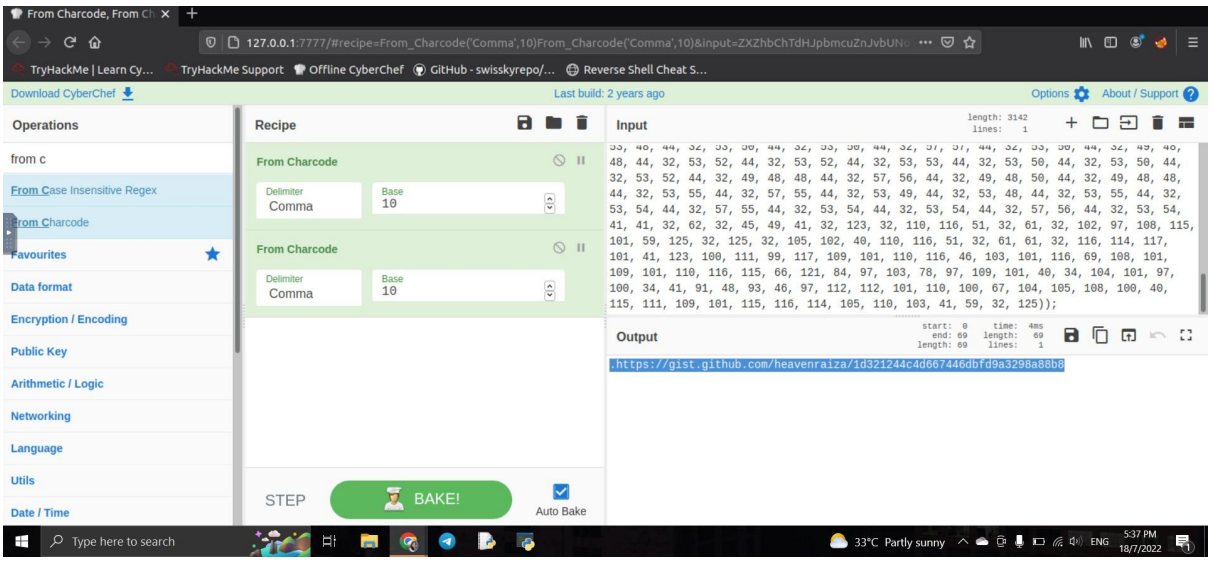
Question 6: after that, we searched for the input in the folder provided at the attackbox desktop. Then, we found its properties and paste it as the input. By using html entity, we obtained the output as ic3Skating.

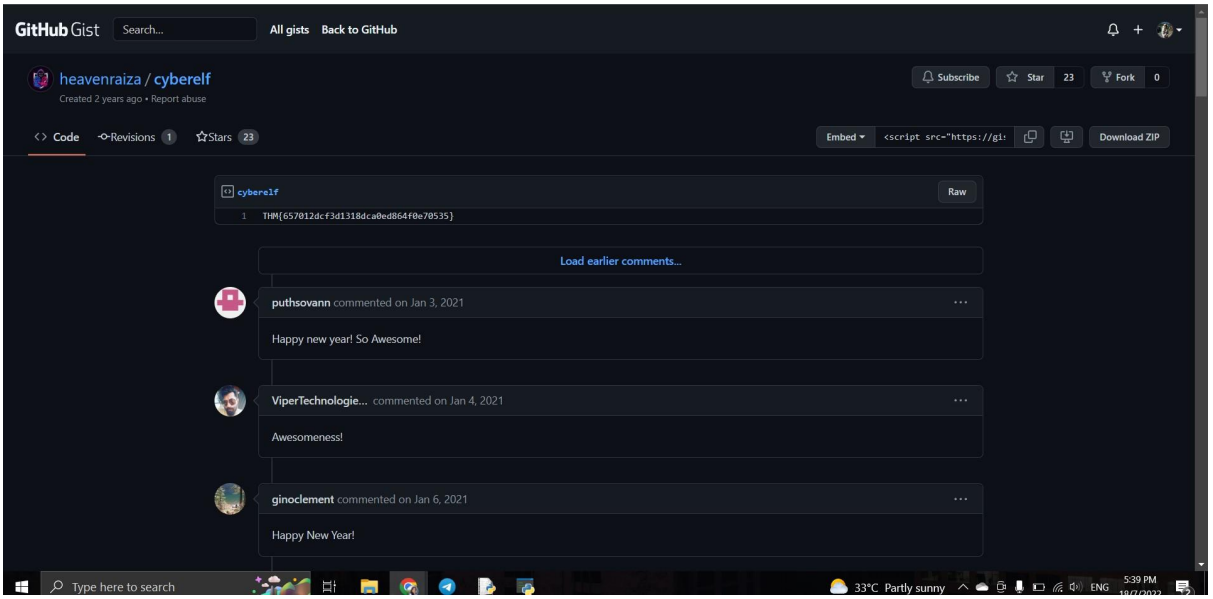


Question 7: Then, we opened the recycle bin. It shows what was the password and the username. The answer is shown after the toggle has been pressed .



Question 8: Then, we pressed the system security and received the properties. We paste the properties in cyberchef and by using double from charcode with delimiter “comma” and base 10, we have received an output which leads to a github web. The flag was provided in the github web as we opened it by using firefox**.**





Thoughts Process/ Methodology:

First thing first we started the machine and opened the remmina application we have installed. In the remmina apps, we add a new connection profile with our machine IP as the server, Administrator as the username and sn0wF!akes!!! As the user password. After we saved and connected, we found a file in the remmina desktop. We copy the file name and paste it in the cyberchef input. Then we use magic as the recipe and get the output. We got the password to the KeePass database from the output. After that, we open “Network” in the KeePass and copy the password of the Elf Server. After that we paste the password in the cyberchef and we are able to get the decoded password value of the Elf Server. Then, we searched for the input in the folder provided at the

attackbox desktop. Then, we found its properties and paste it as the input. By using html entity, we obtained the output as ic3Skating. Then, we pressed the system security and received the properties. We paste the properties in cyberchef and by using double from charcode with delimiter “comma” and base 10. We received an output that leads to the github web and the flag was provided there.

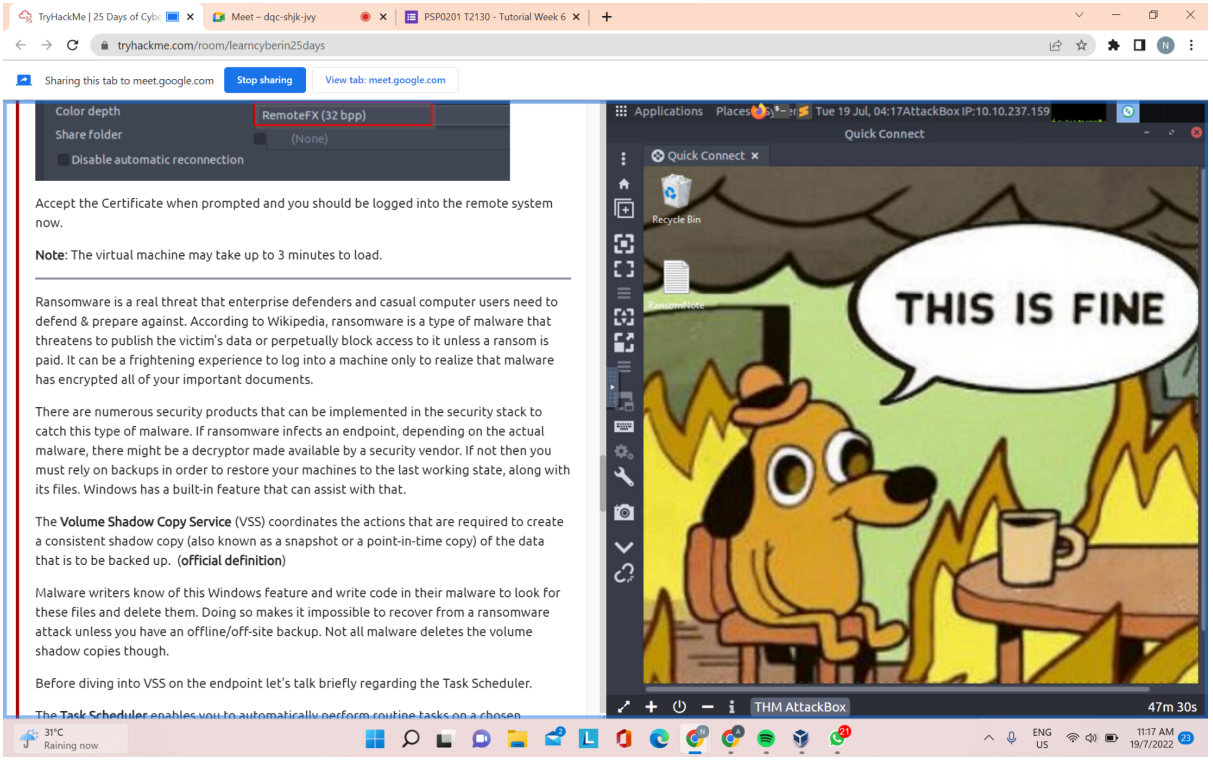
Day 23: The Grinch strikes again!

Tools used: Remmina, Cyberchef

Solution / walkthrough:

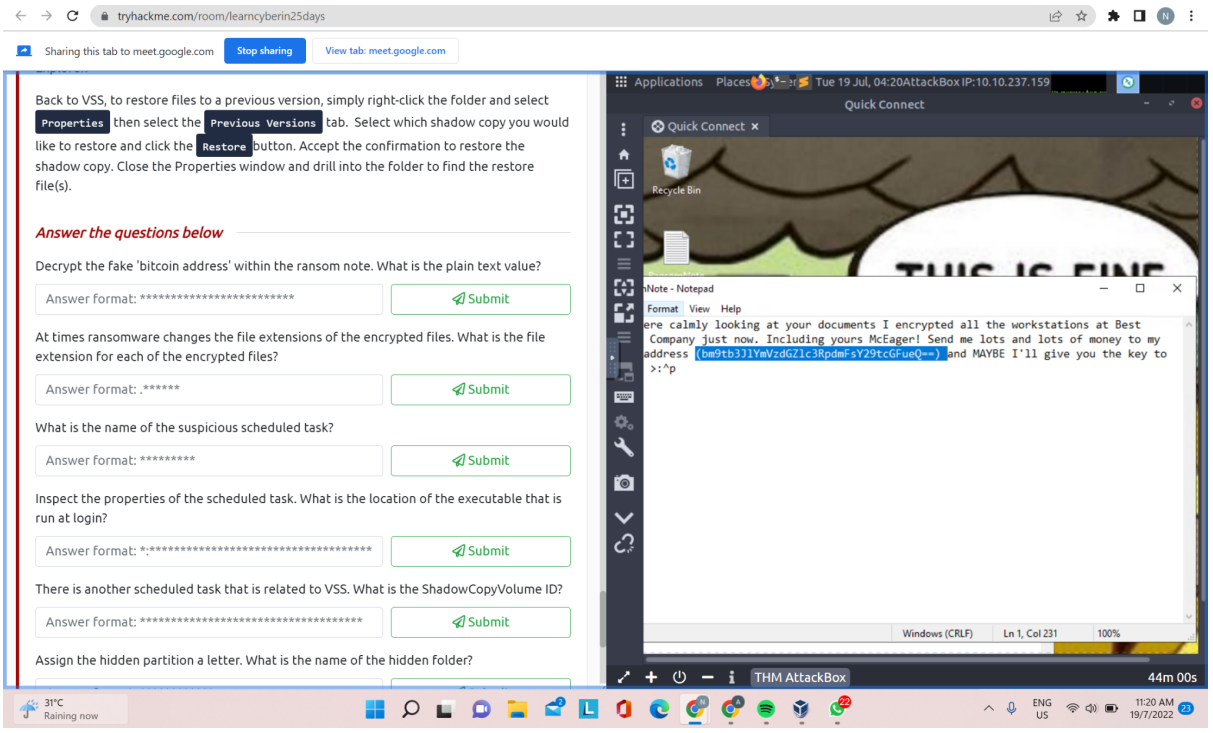
Question 1:

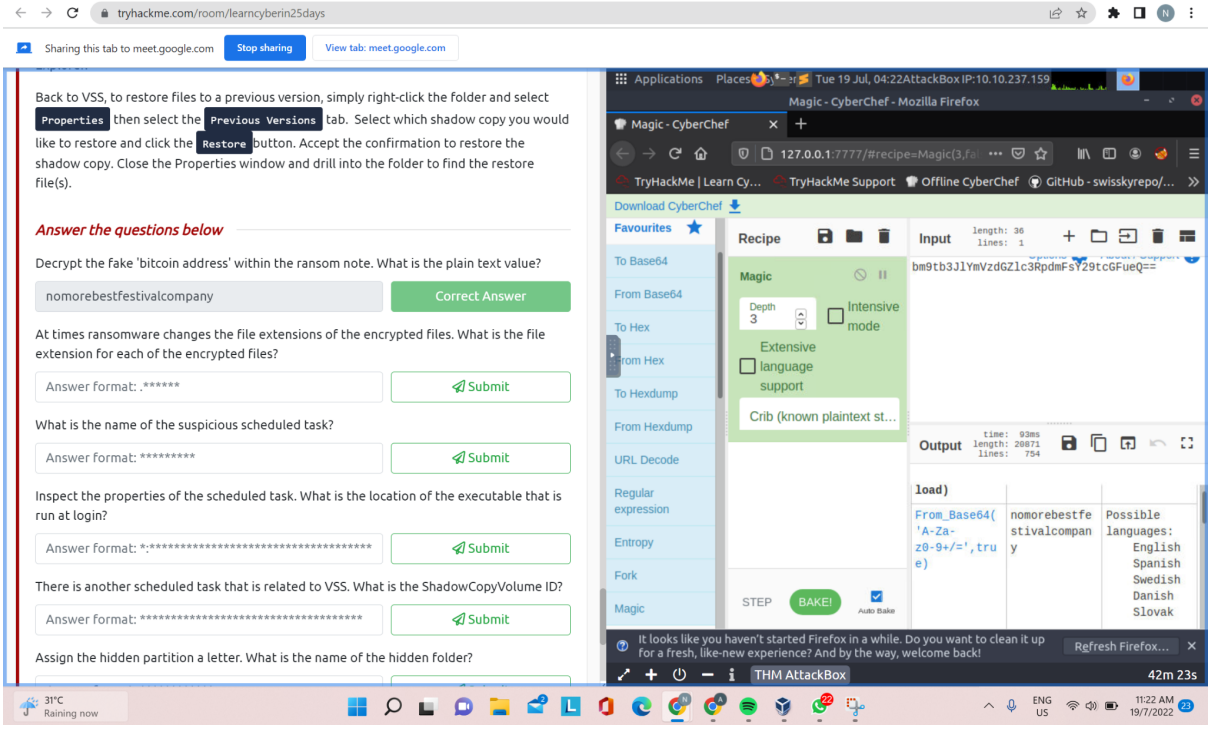
Open Remmina and change the preferences in tab RDP. Make some changes on quality settings and connect to the remote machine using the IP address, username and user password provided. When logged in, we can see the desktop with the wallpaper.



Question 2:

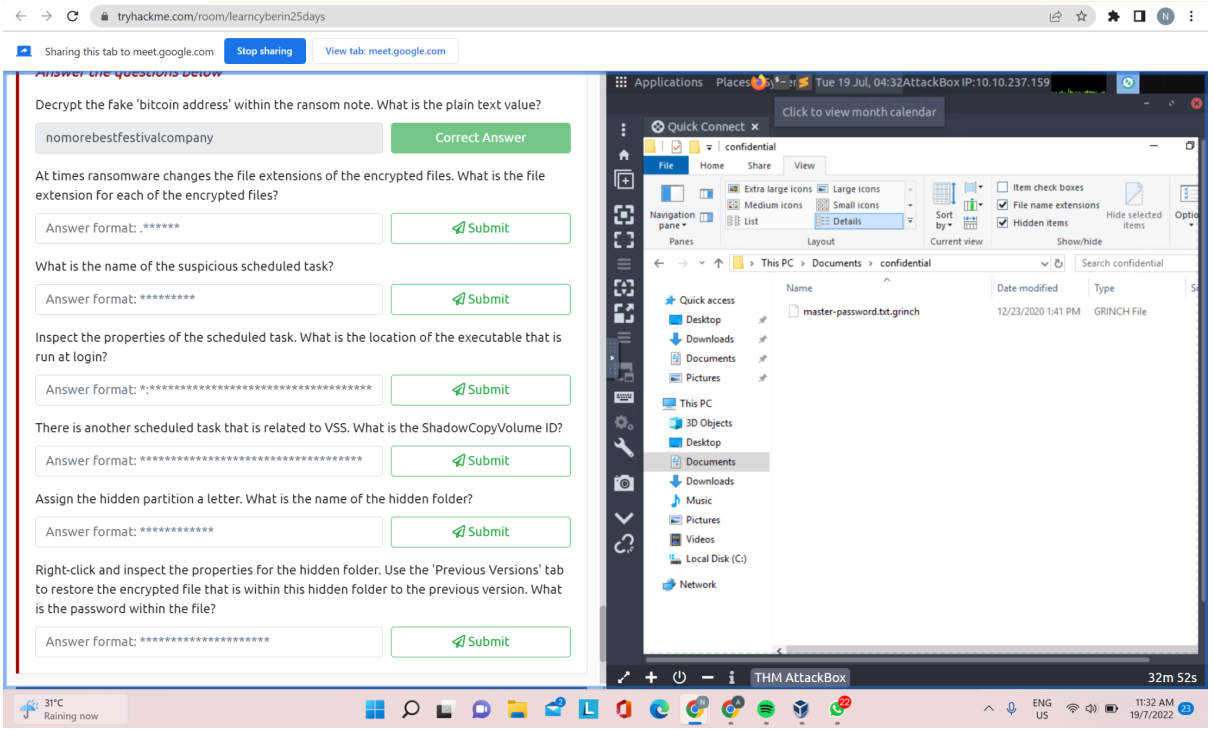
On the desktop, we can see a file named ransom note. Open the file to look for a bitcoin address. Copy the address and open cyberchef to convert the value. Use Magic recipe to gain the output. We can see the plain text value is nomorebestfestivalcompany.





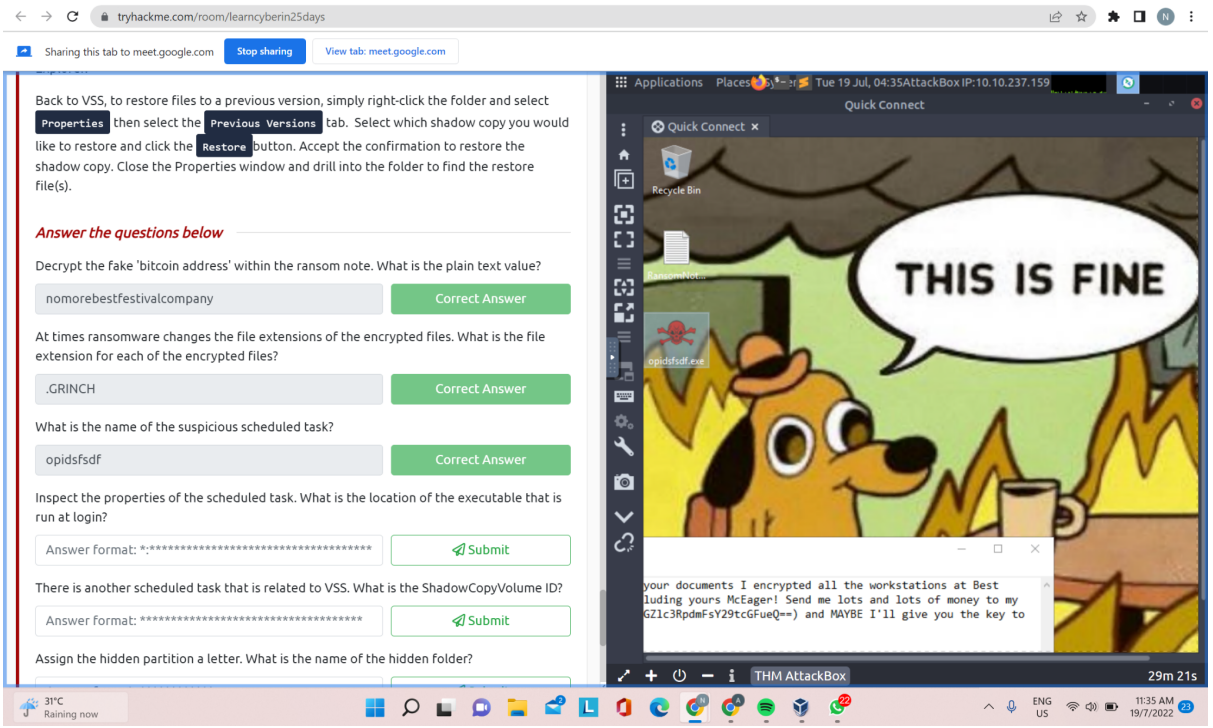
Question 3:

To look for the encrypted files, open documents and click the view tab. Tick file name extensions and hidden items boxes. The encrypted files will be displayed eventually. The file extension can be seen next to the date modified.



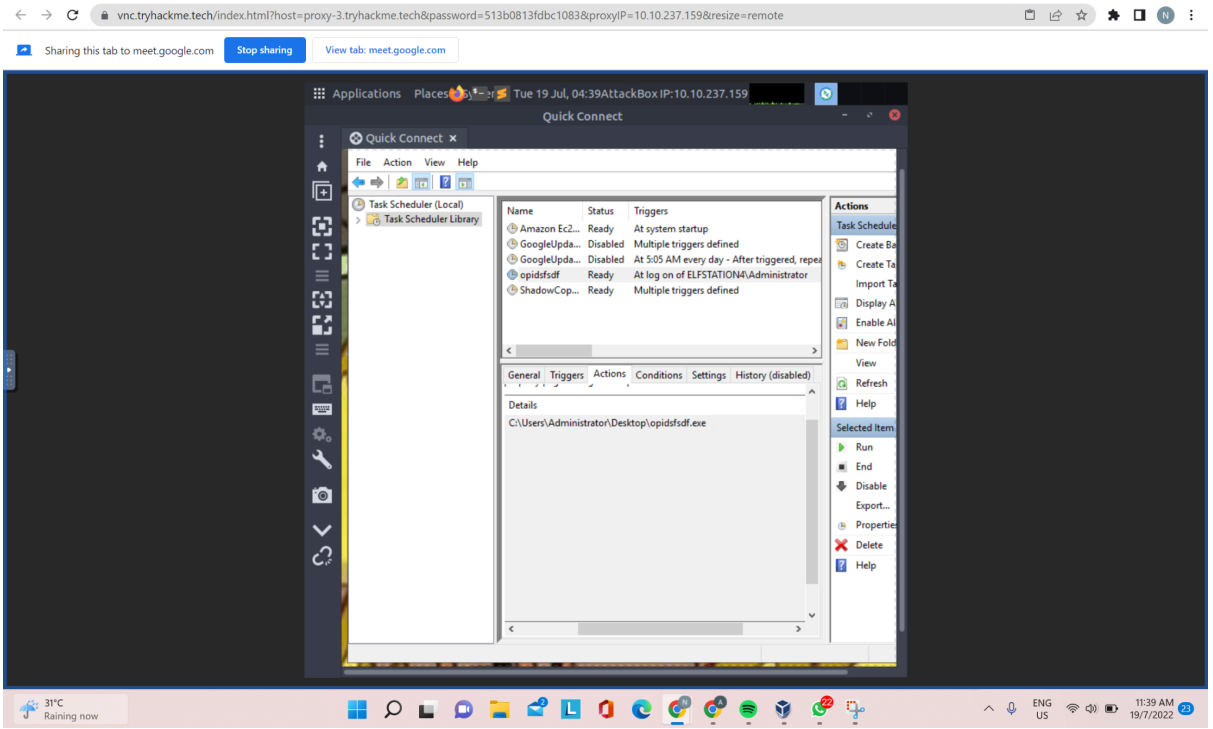
Question 4:

Go back to the desktop. Now we can see that there is a new file on the desktop. That is the new suspicious file. Alternatively, we can also go to Task Scheduler to see the suspicious scheduled task. The same file can be seen there.



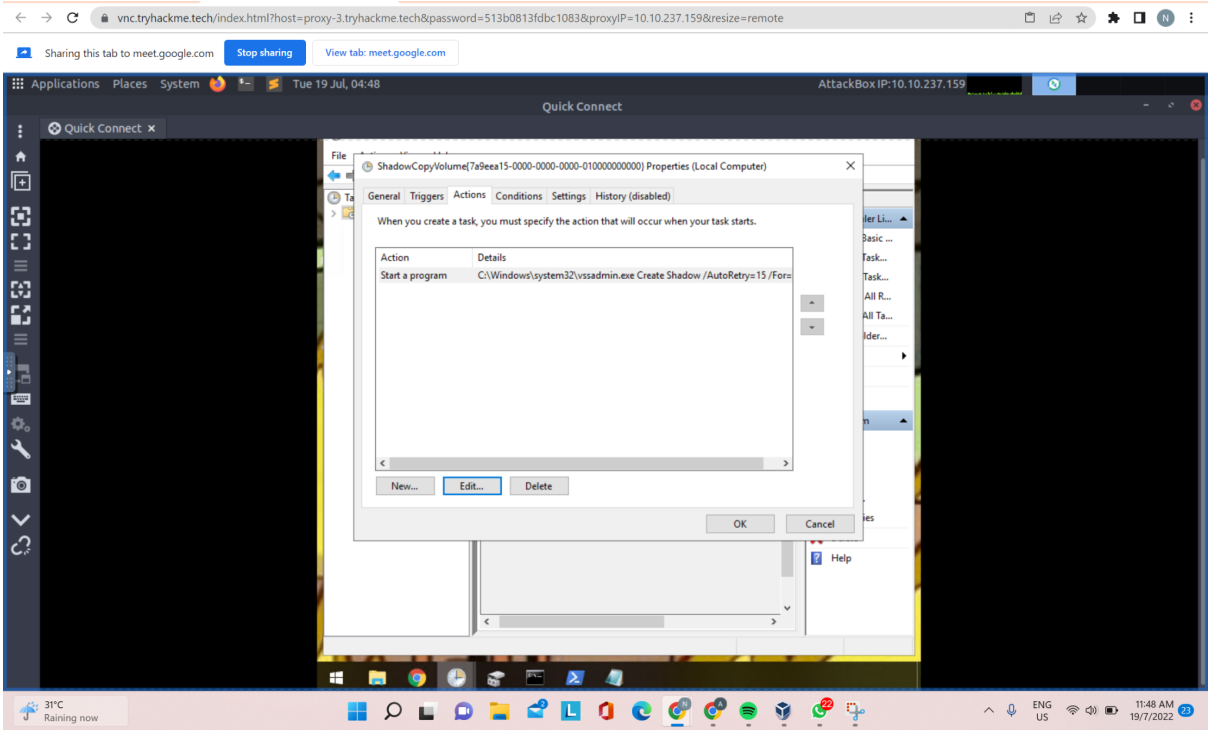
Question 5:

To inspect the location of the scheduled task, in Task Scheduler, click on the suspicious file and choose Actions. We can now see the details of the location of this task.



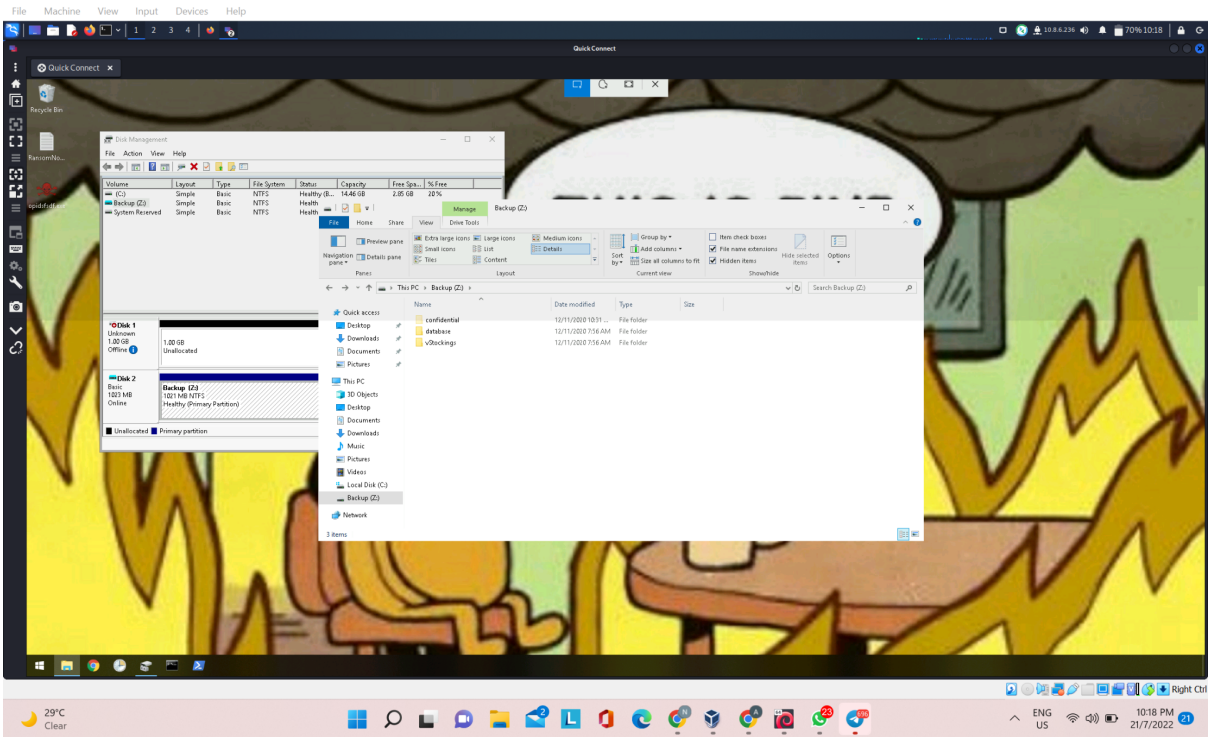
Question 6:

On Task Scheduler, click on the ShadowCopyVolume file. The id of the file is the one next to its name.



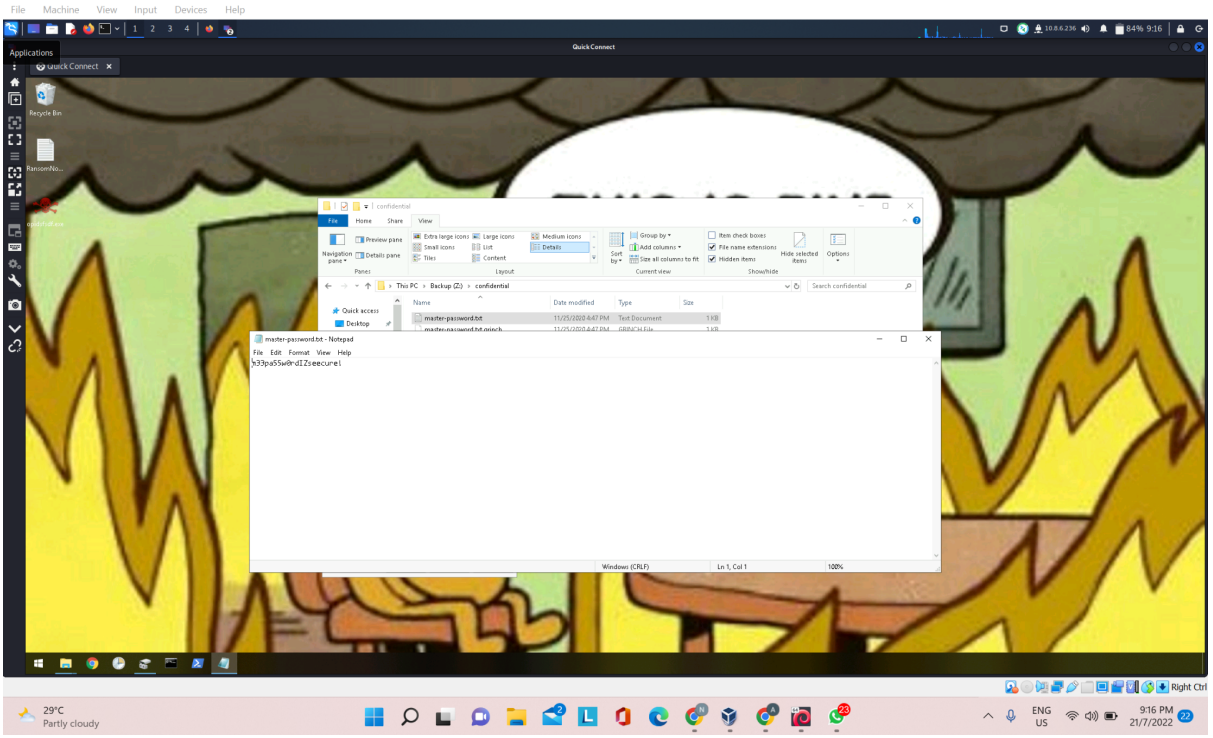
Question 7:

On file explorer, click view and tick file name extensions and hidden items. We can now see the hidden folder named confidential.



Question 8:

Using Disk Management, we change the drive letter and path of the backup file. We use letter Z as the path for the backup file. Now, we can see that the backup file will be shown on the file explorer as backup(Z). Click the file and select the file with text document extension. View its properties and restore the previous versions. After restoring, open the file using notepad. Now we can see the password in the file.



Thoughts Process / Methodology:

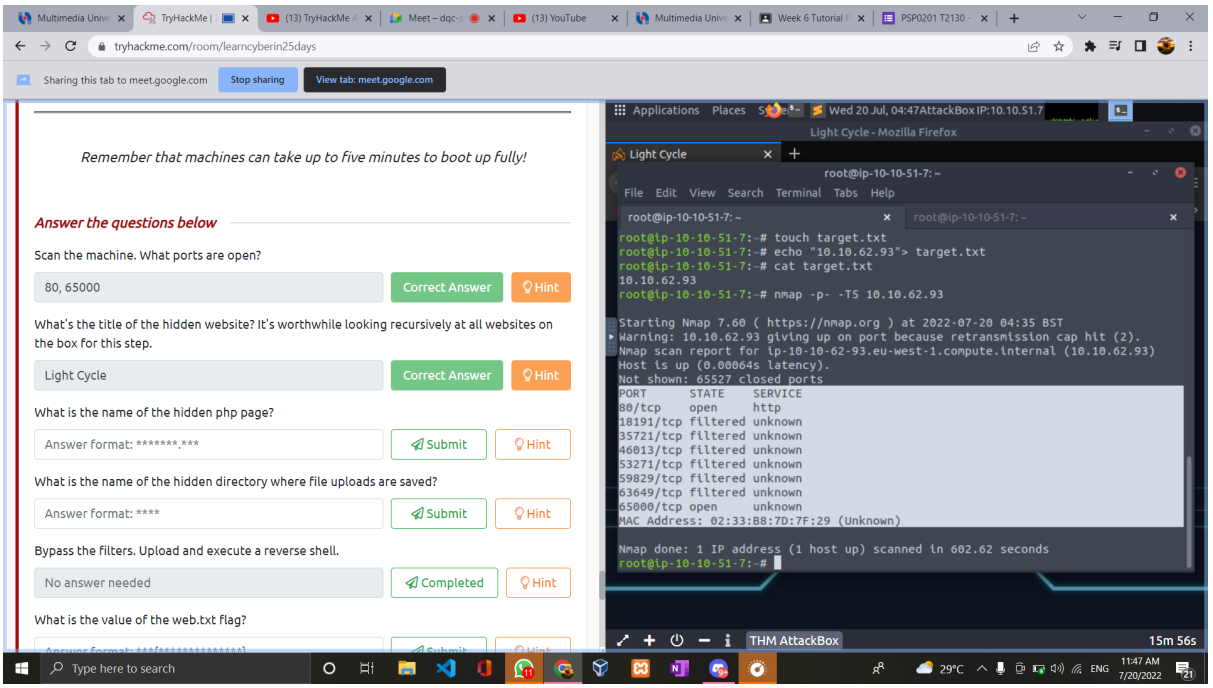
For this task, we will use Remmina to complete the task. Open Remmina and connect to the machine using the IP address, username and user password provided. Remember to make changes regarding quality settings on the preferences in the RDP tab. Once logged into the machine, we can now see the desktop. Open the ransom note file and copy the bitcoin address in the file to cyberchef. Here, we use Magic recipe to convert the bitcoin address to plain text value. To view encrypted files, we have to go to documents and in the view tab, tick hidden items and file name extensions boxes. A hidden file will now be shown. Back on the desktop, we can see there is a new file being added and it is suspicious. To look for the location of the scheduled task, open Task Scheduler and inspect its properties there. To look for the id of the ShadowCopyVolume file, click on the file and its id is displayed on top. Since we

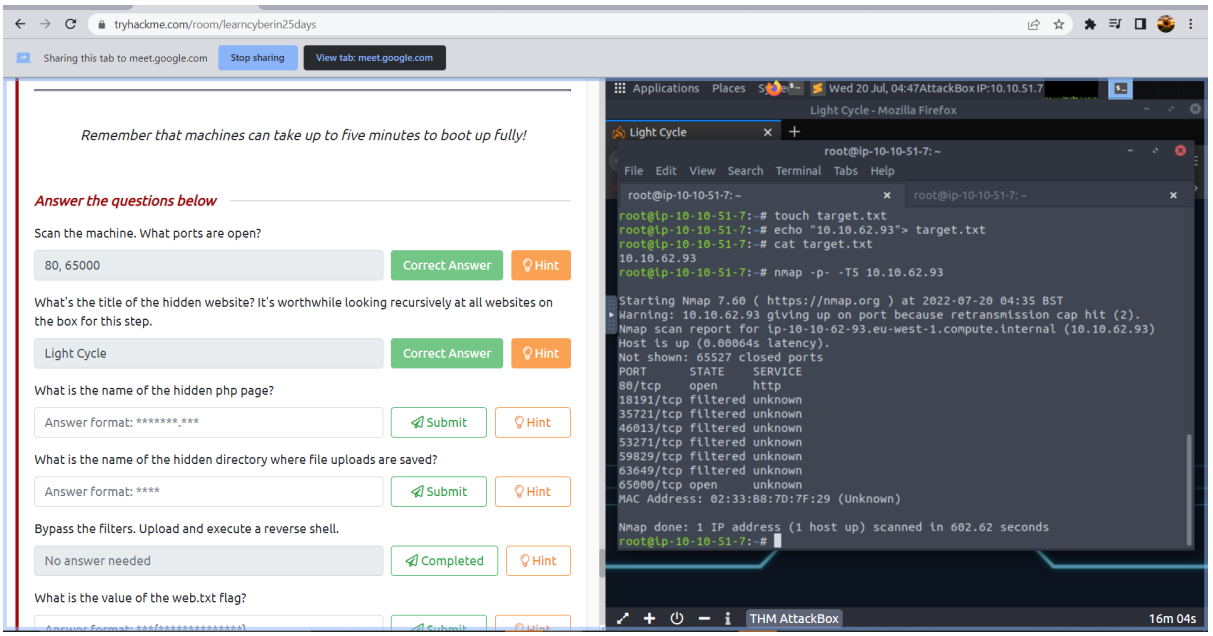
want to look for a password in a file that no longer exists, we have to restore the file back. In Disk Management, change the drive letter and path of the backup file. We can now see the new file being added to file explorer. In this file, click the file with text document extension and restore the previous sessions of the file. Launch the file and now we can obtain the password located in the file.

Day 24: The Trial Before Christmas
Tools used: burp suite, mozilla firefox, MySQL

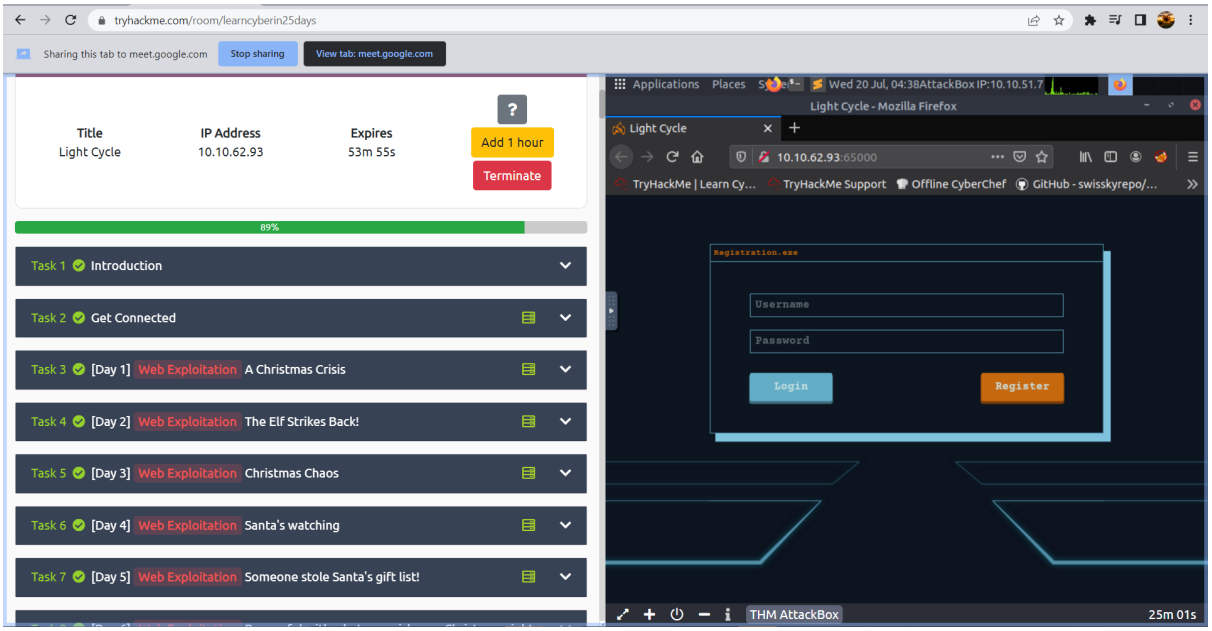
Solution / walkthrough:

Question 1: Firstly, start with nmap and our IP address. Because there are many closed ports in this machine, we have to wait for a while for it to run.

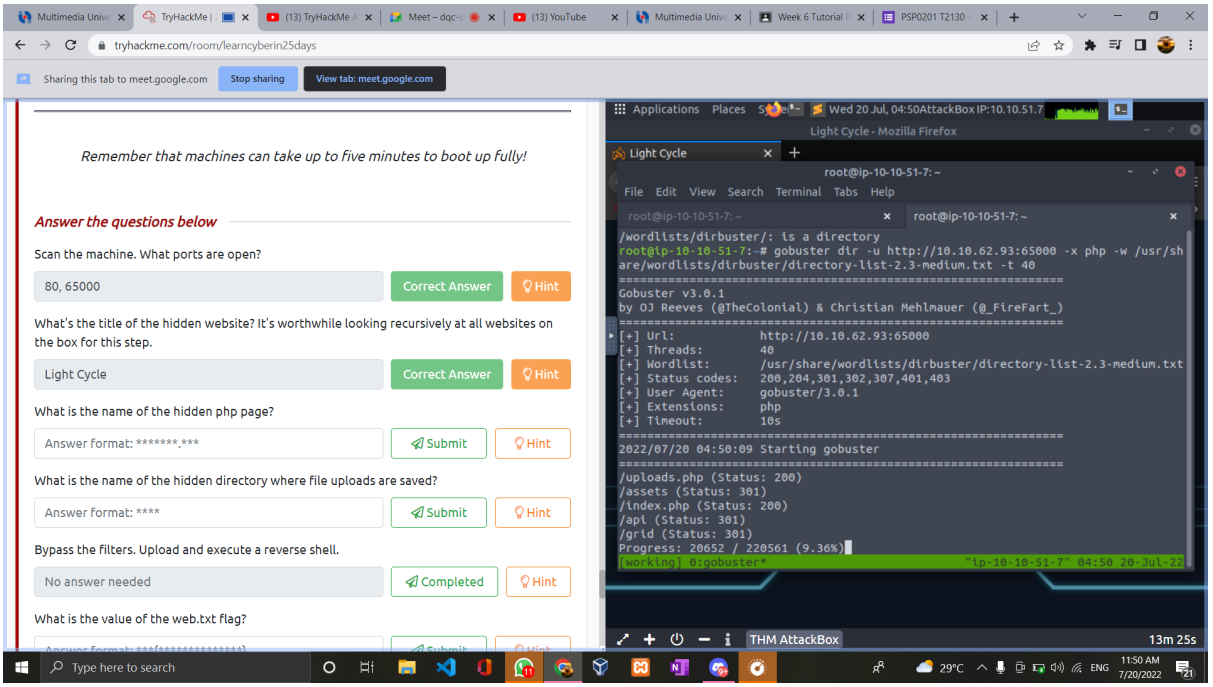




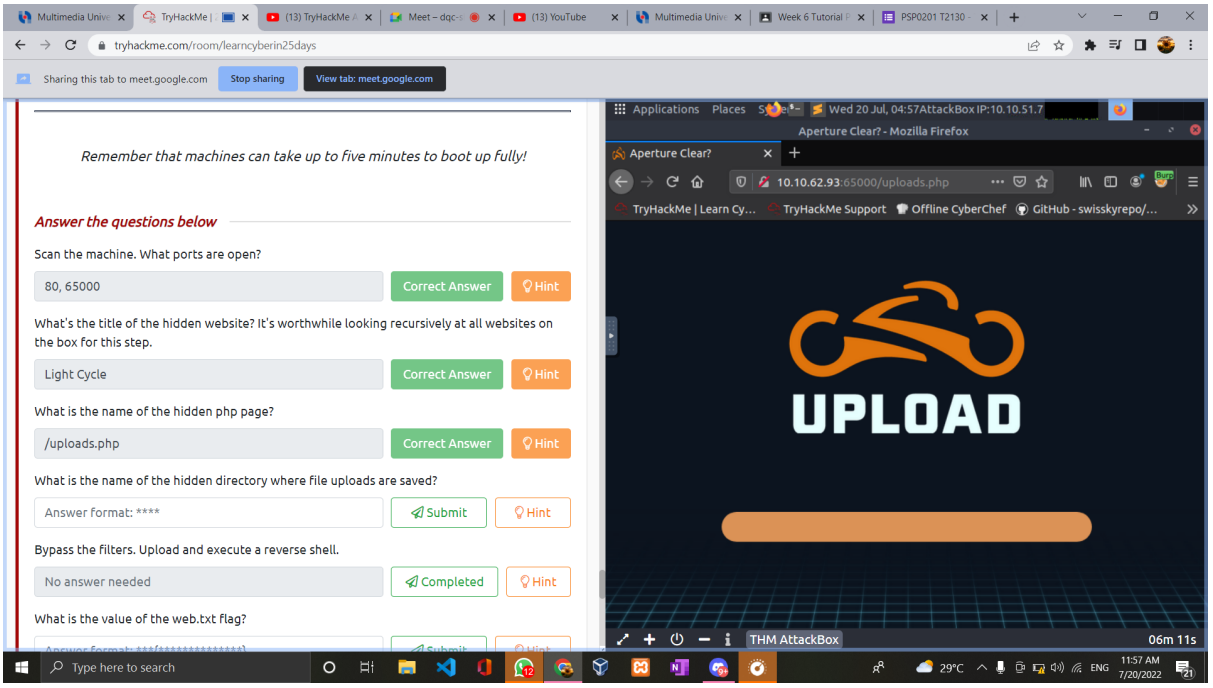
Question 2: We search the ip addresses with port 65000 in the mozilla firefox. Then we will find the title of the hidden website.

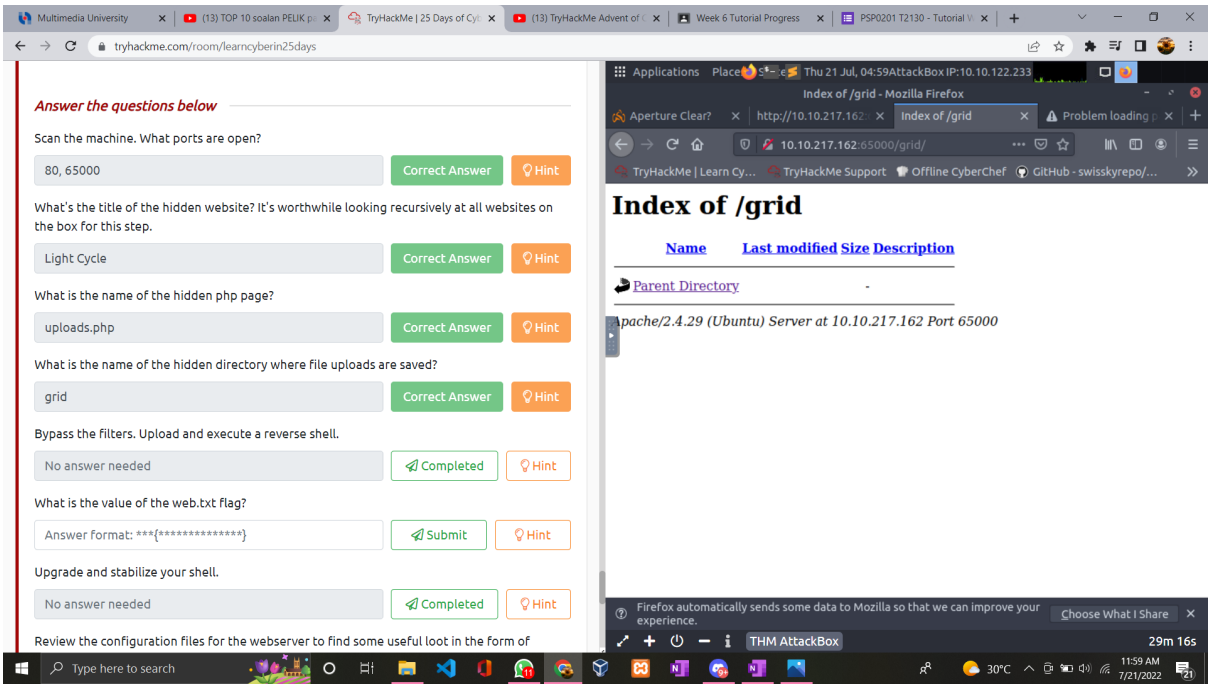


Question 3: Then, launch the new tmux session. After that, we should do with gobuster and use php and directory '-x' to find the hidden php file.



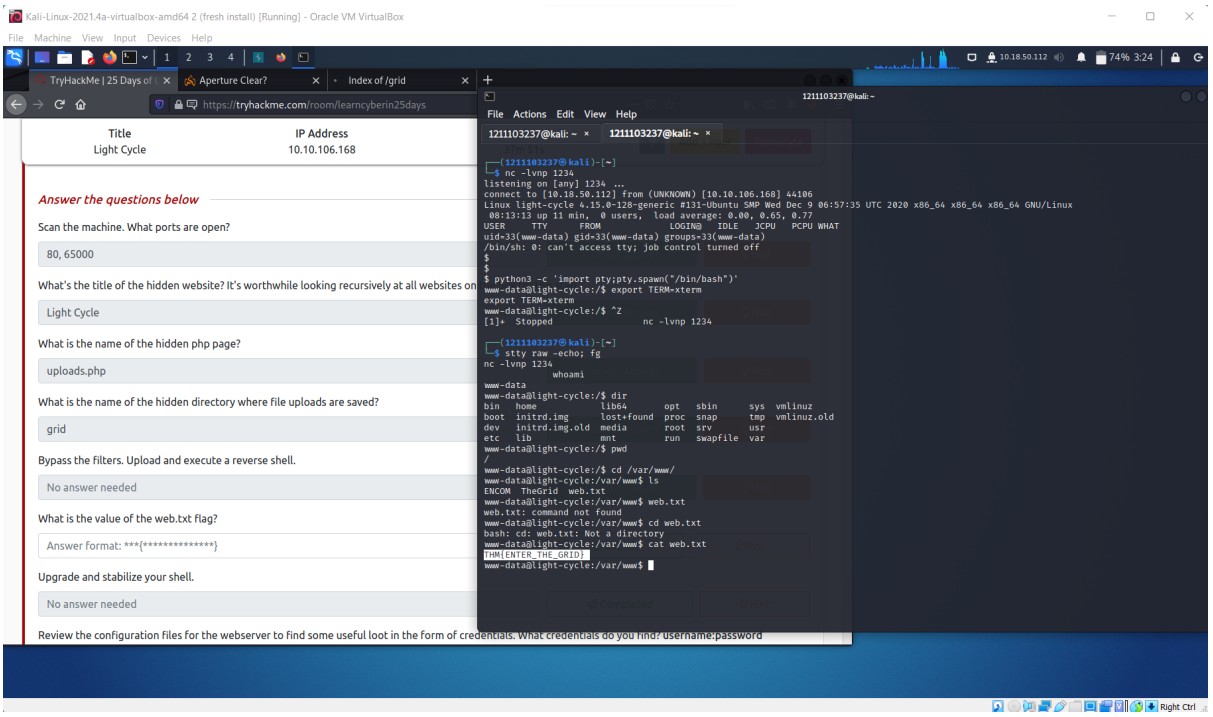
Question 4: After that, in the burp suite which is at the “proxy” tab and “Options” section. We have to edit the file extension in the ‘Intercept Client Request’ and remove the ‘|^js$’ and refresh page. Next, we have to open the upload page by searching the Ip address:65000/uploads.php . After that, we have to upload the shell.jpg.php that we created in the powershell by clicking the upload image. After the file is successfully upload, we will open the secret page with /grid.



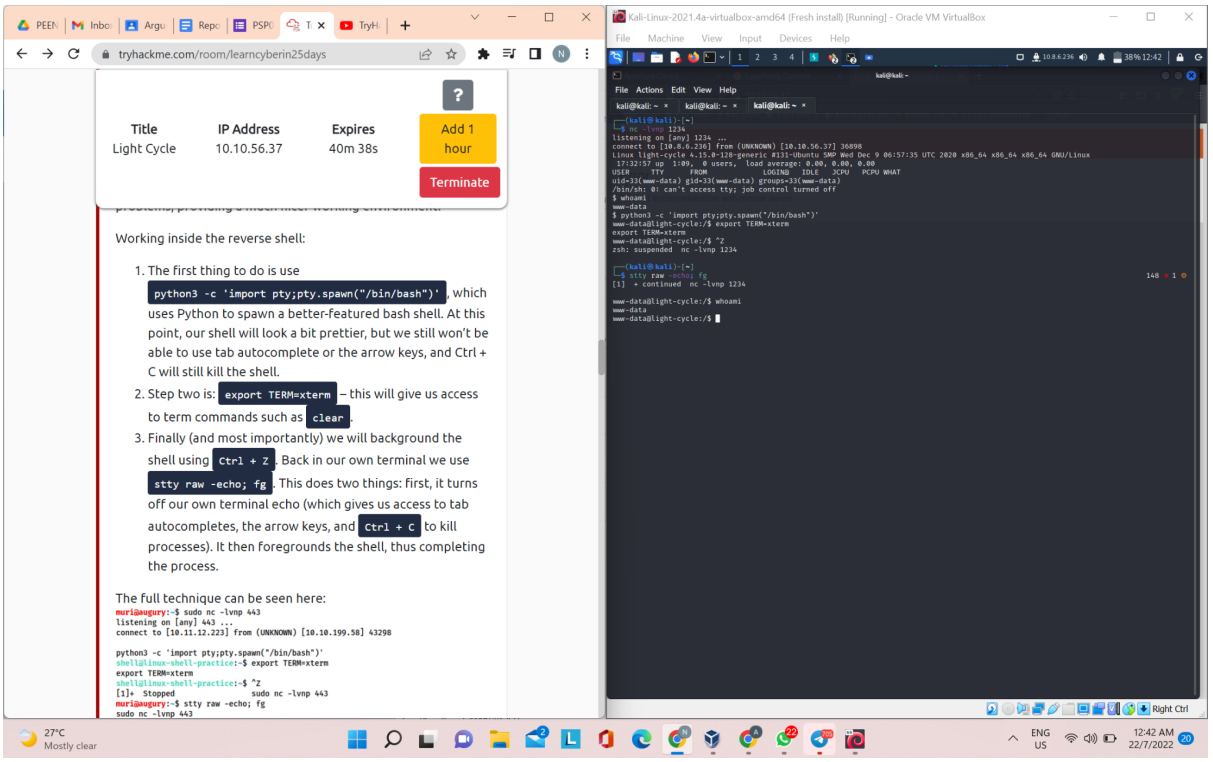


Question 5:

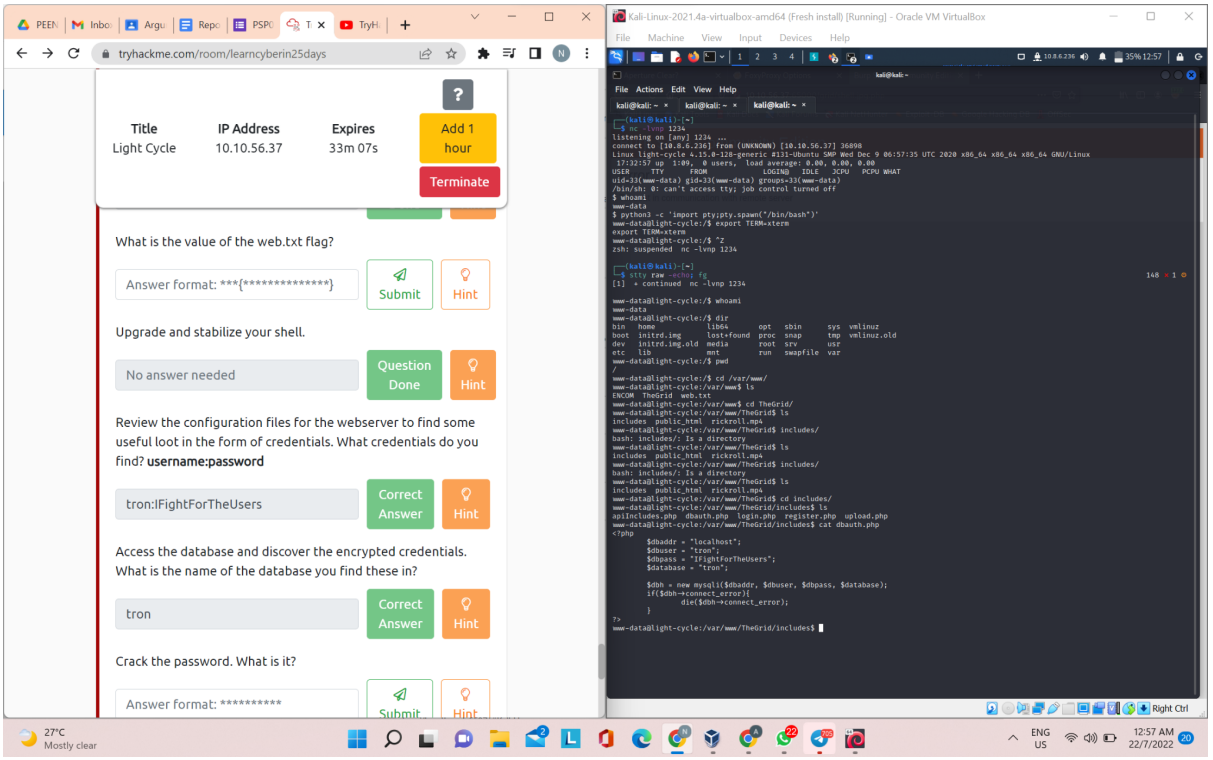
Next, we have to find the web flag in the shell. First, we have to open the shell first. So we will do in the netcat lvnp 1234. After that, we make a quick search of the file system revelas it is located in var/www/. We can easily access the contents with cat and find the flag THM{ENTER_THE_GRID}



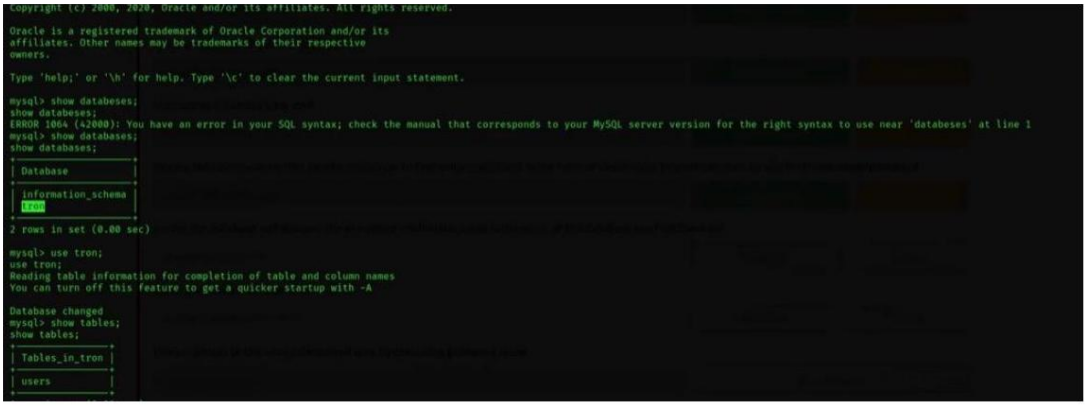
Question 6: After uploading the file, Netcat that listens to the file will detect the file being uploaded. After that we use the command python3 -c 'import pty;pty.spawn("/bin/bash")',export TERM=xterm and stty raw -echo; fg to stabilise and upgrade the shell we have.



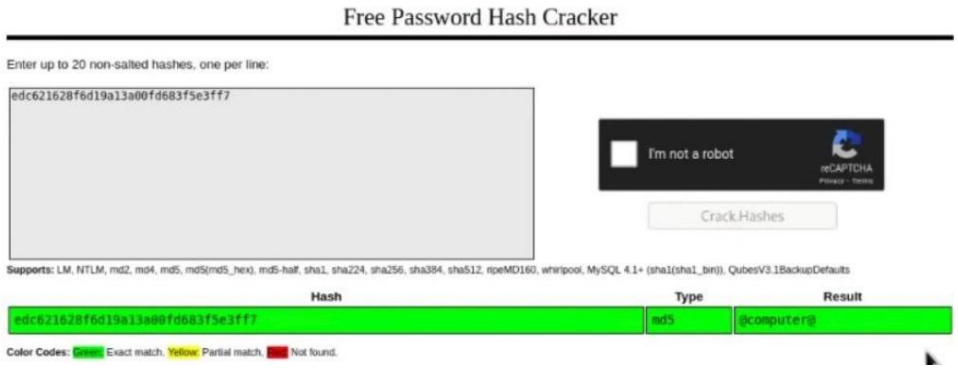
Question 7: After stabilising and upgrading our shell, we use the whoami to know where we currently are and see what is the current option to navigate to. After that, we use the command “cd /var/www/ “ and command “ls” to see what is there inside the navigation. From there on, we select the file TheGrid then includes. We used the command “ls” until we found the file dbauth.php. By using command “cat” we found the password and the username



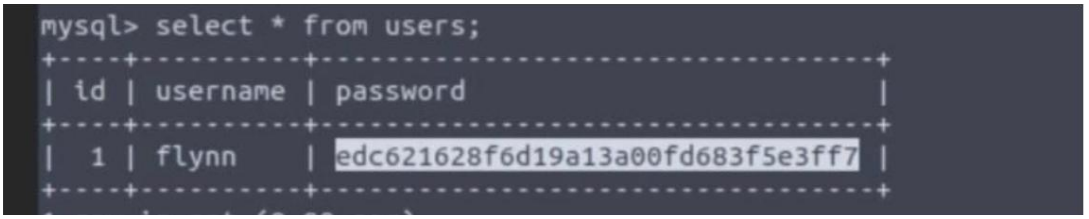
Question 8: We can now access the MySQL client using this login information. We can enter the shell with the command mysql -utron -p and then enter the password when prompted.Once we are in MySQL, use the command SHOW DATABASES; to list all the available databases.



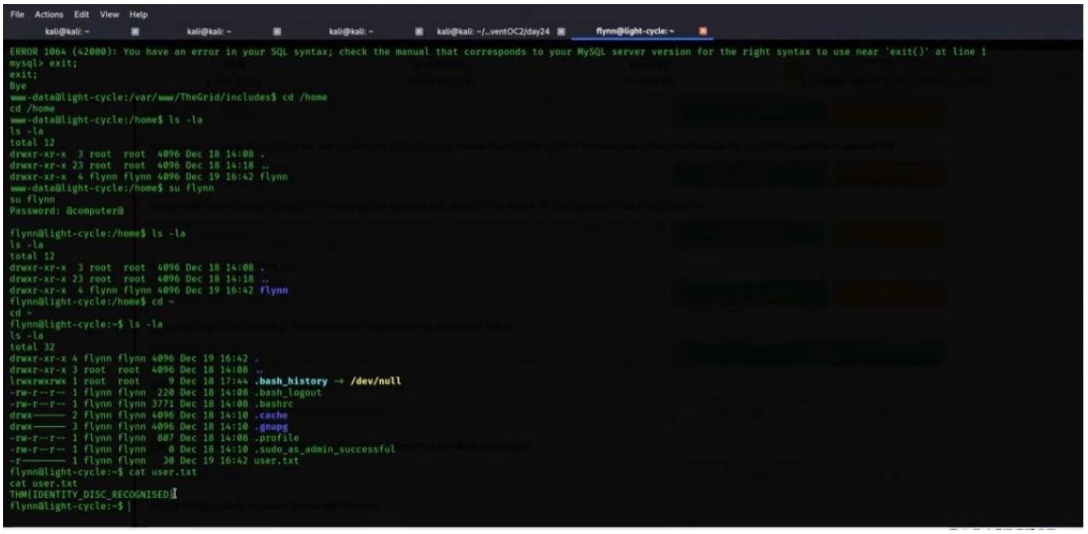
Question 9: We can select the tron database by using the command use tron; and then list the contents of the users table with SELECT * FROM users;. When we do this we see two users and their encrypted passwords.Let's head to the site https://crackstation.net/ and see if it can make sense of Flynn's password. It is able to do this pretty easily and determines it has been hashed with md5. The password is @computer@.



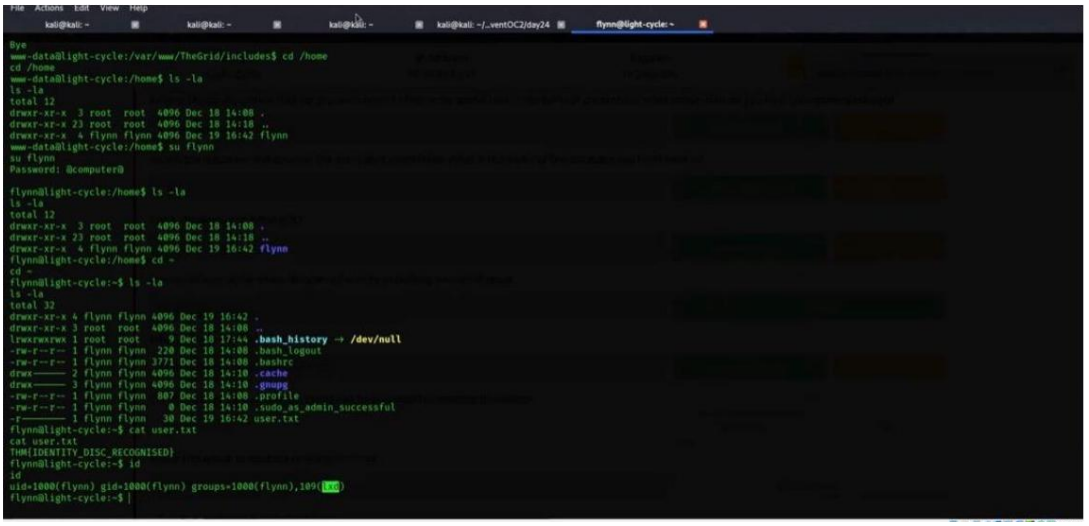
Question 10: by seeing the password provided, we can detect the name has been changes from the original version to flynn



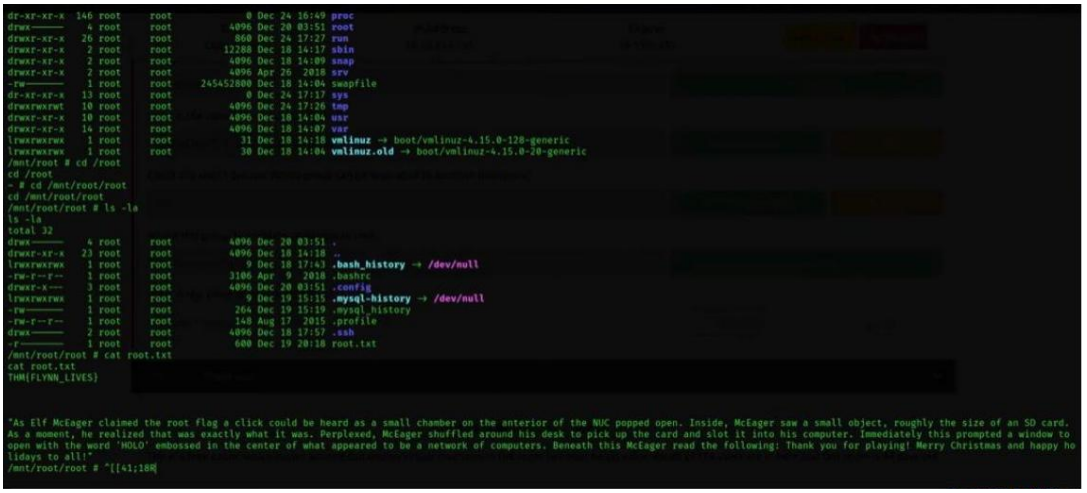
Question 11: Now that we know Flynn's password, we can log in as him using su. We can now read the contents of the flag located in Flynn's home directory. After using cat we see the flag is THM{IDENTITY_DISC_RECOGNISED}



Question 12: If we run groups to see what groups Flynn is a part of, we see he is in a group called lxd.



Question 13: There is a known flaw in lxd which will allow us to create a root shell. These steps come directly out of today's description so it is probably best to follow along there. Below is how I got my own lxd exploit to work.



Thoughts Process / Methodology:

For this task, we have to find the open port by using nmap. After we find the open port, we have to search our IP addresses with the port and the name of the website will shown. We find the secret php by launching the tmux session and gobuster. After that, go to the "proxy" tab and "Options" section of the burp suite. The "|js$" must be removed from the file extension in the "Intercept Client Request" before refreshing the page. The upload page must then be accessed by typing in the IP address 65000/uploads.php. The

shell.jpg.php file we made in the powershell must then be uploaded by selecting the upload image button. We will use /grid to access the secret page once the file has been successfully uploaded. The web flag must then be located in the shell. We must first crack open the shell. Determining what to do in the netcat lvnp 1234. Then, after a fast check of the file system, we discover that it is located at var/www/ . With cat command, we can quickly access the data and locate the flag THM{ENTER THE GRID}. Back to the uploading file in the secret page, the file that already uploaded will be discovered by Netcat that is listening to the file. Then, to upgrade and stabilise our existing shell, we use the commands python3 -c "import pty;pty.spawn("/bin/bash")", "export TERM=xterm," and "stty raw -echo; fg.". After upgrading and updating our shell, we use the whoami to determine our location and the available navigational options. Then, to view the contents of the navigation, we use the commands "cd /var/www/" and "ls." Next, we choose the file that TheGrid will include. To locate the file dbauth.php, we used the command "ls." We discovered the login and password using the command "cat." Now that we have the login credentials, we can visit the MySQL client. Mysql -utron -p can be used to launch the shell, and when prompted, the password should be entered. Use the command SHOW DATABASES; to list all the available databases once we are in MySQL. After that, the use tron command can be used to choose the tron database, and the SELECT * FROM users command can be used to list the users table's contents. When we do this, two users' encrypted passwords are displayed. See if the website https://crackstation.net/ can decipher Flynn's password by going there. It can simply accomplish this and concludes that it has been hashed with MD5. @computer@ is the password. Next, we can see the name has been changed from the original version to flynn by looking at the password that has been provided. Then, we can use su to log in as Flynn now that we have his password. Now that we have access to Flynn's home directory, we can examine the information on the flag. Using cat, we can observe that the flag is THM{IDENTITY DISC RECOGNISED}. Flynn belongs to a group called lxd, which can be found out by running a groups search. Because of a known vulnerability in lxd, we can build a root shell. It would definitely be better to follow along in today's description since these steps are directly taken from there. Here's how I created my own lxd exploit and made it function.