PSP0201

Week 6

Writeup

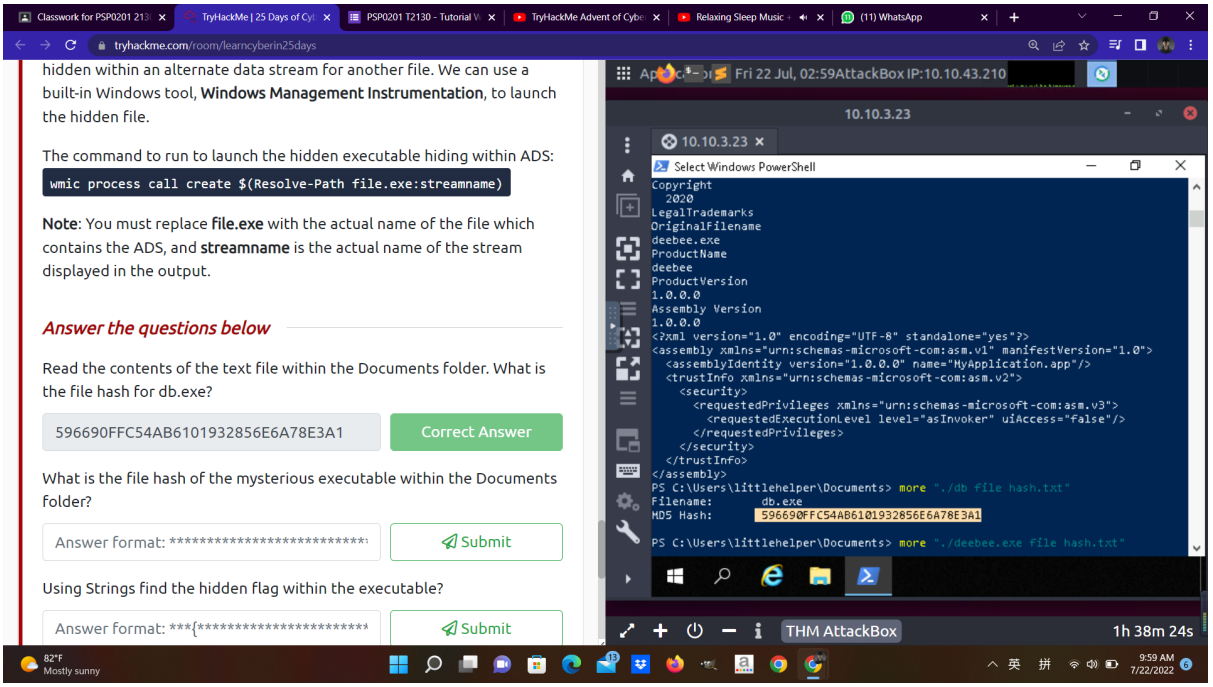
Group Name: SupremeChickens

Members

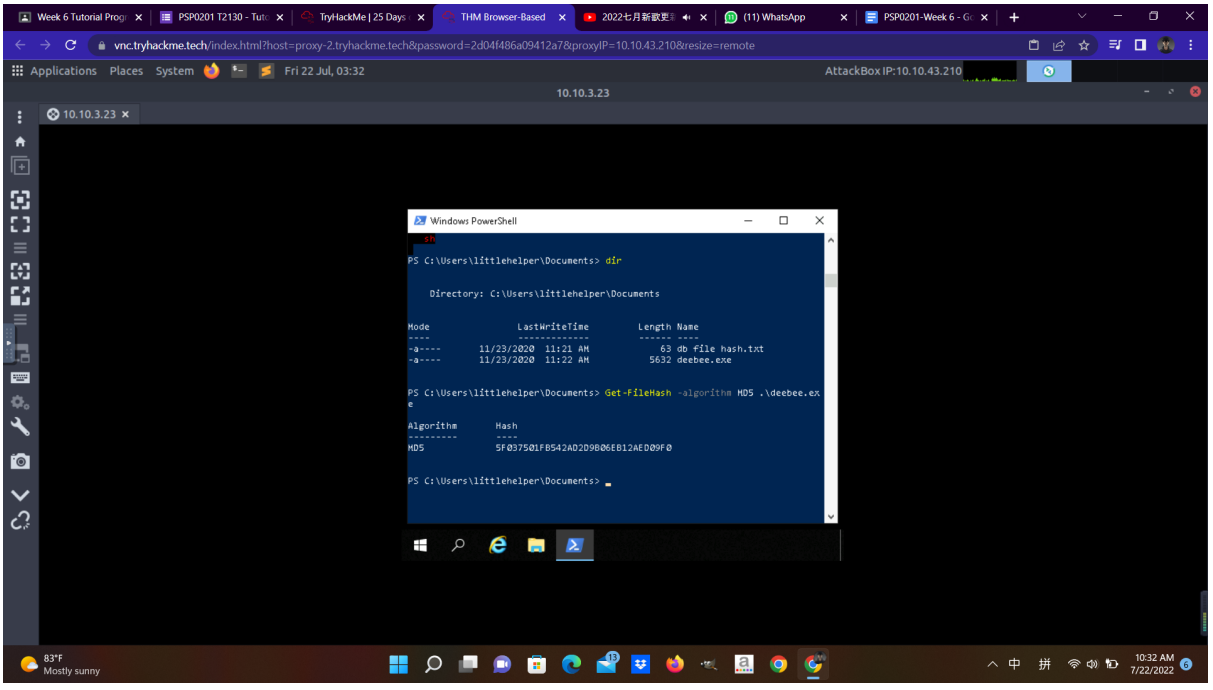
ID	Name	Role
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	Member
1211101198	Fam YI Qi	Member
1211103978	Yong Dick Shen	Member

day 21

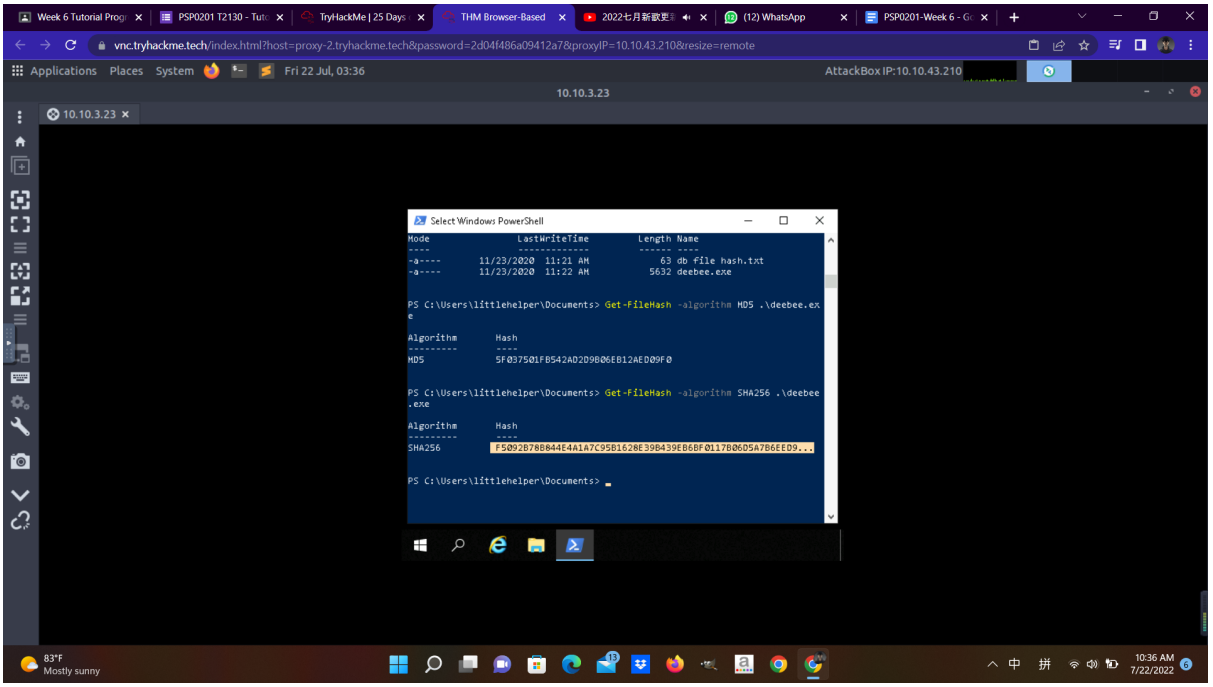
question 1



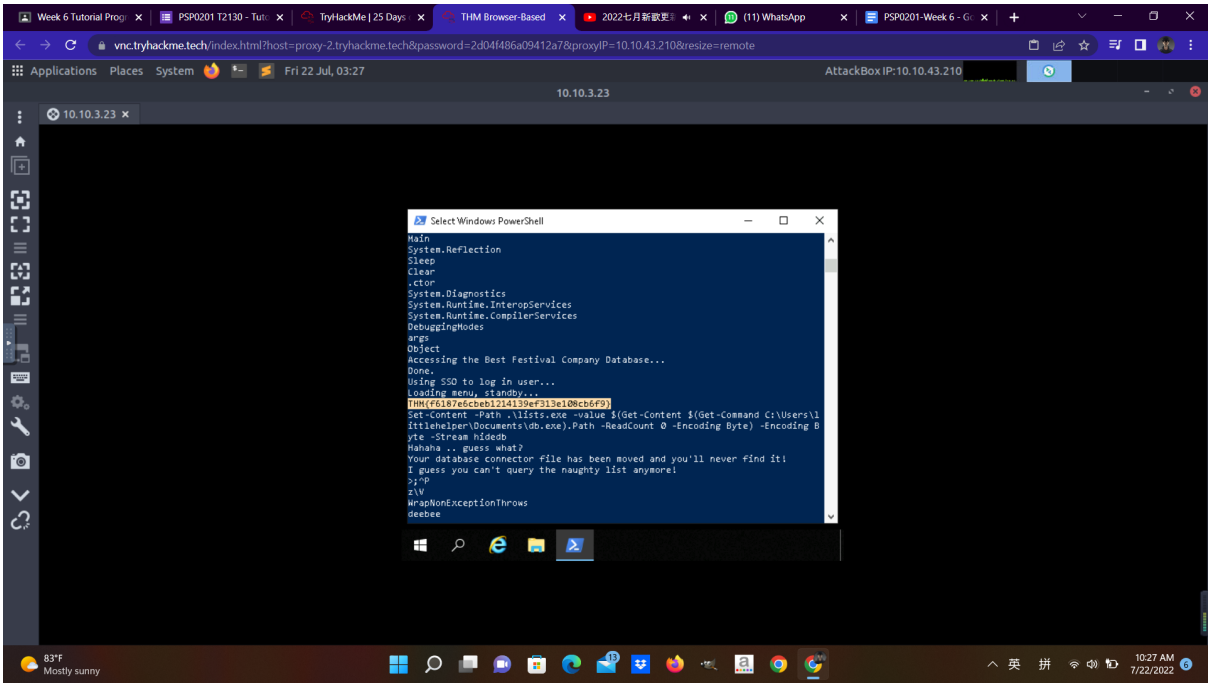
question2



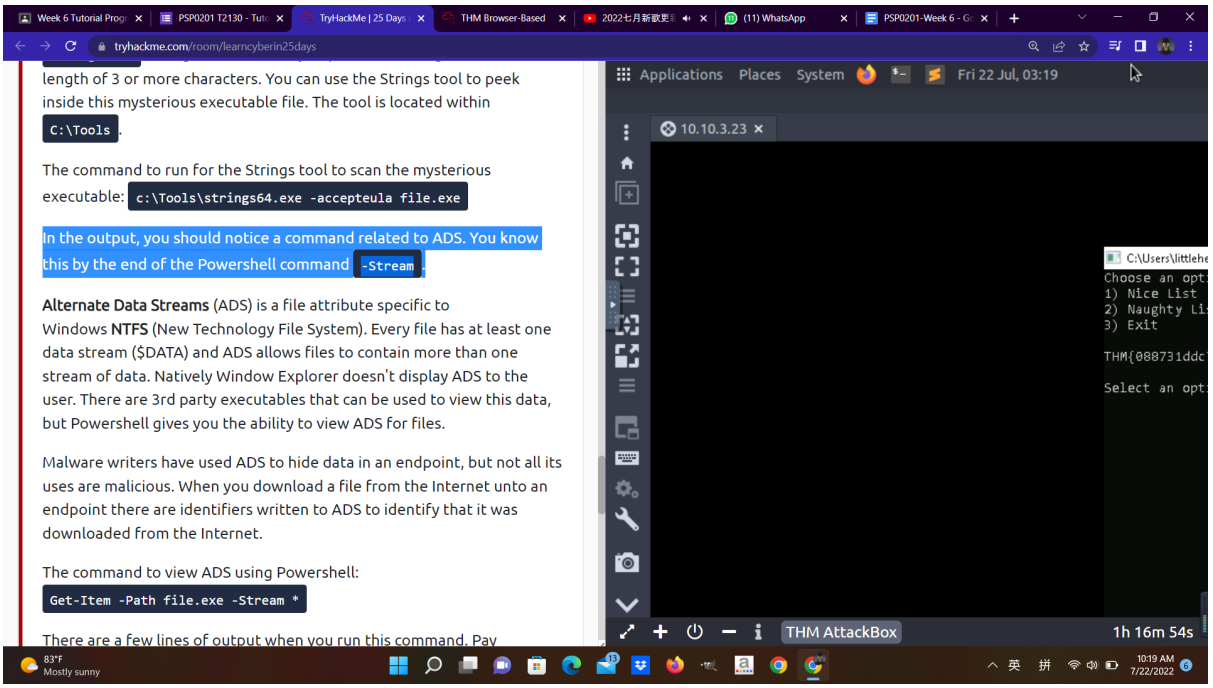
question 3


Week 6 Tutorial Progr
PSP0201 T2130 - Tutc
TryHackMe | 25 Days
THM Browser-Based
2022七月新歌更
(12) WhatsApp
PSP0201-Week 6 - Gc
vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=2d04f486a09412a7&proxyIP=10.10.43.210&resize=remote
Applications Places System Fri 22 Jul, 03:36
AttackBox IP:10.10.43.210
10.10.3.23
10.10.3.23
Select Windows PowerShell
Mode LastWriteTime Length Name
---- ------------- ------ ----
-a---- 11/23/2020 11:21 AM 63 db file hash.txt
-a---- 11/23/2020 11:22 AM 5632 deebee.exe
PS C:\Users\littlehelper\Documents> Get-FileHash -algorithm MD5 .\deebee.exe
Algorithm Hash
MD5 5F03750FB542AD2D9B06EB12AED09F0
PS C:\Users\littlehelper\Documents> Get-FileHash -algorithm SHA256 .\deebee.exe
Algorithm Hash
SHA256 F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED9...
PS C:\Users\littlehelper\Documents>
83°F
Mostly sunny
10:36 AM
7/22/2022

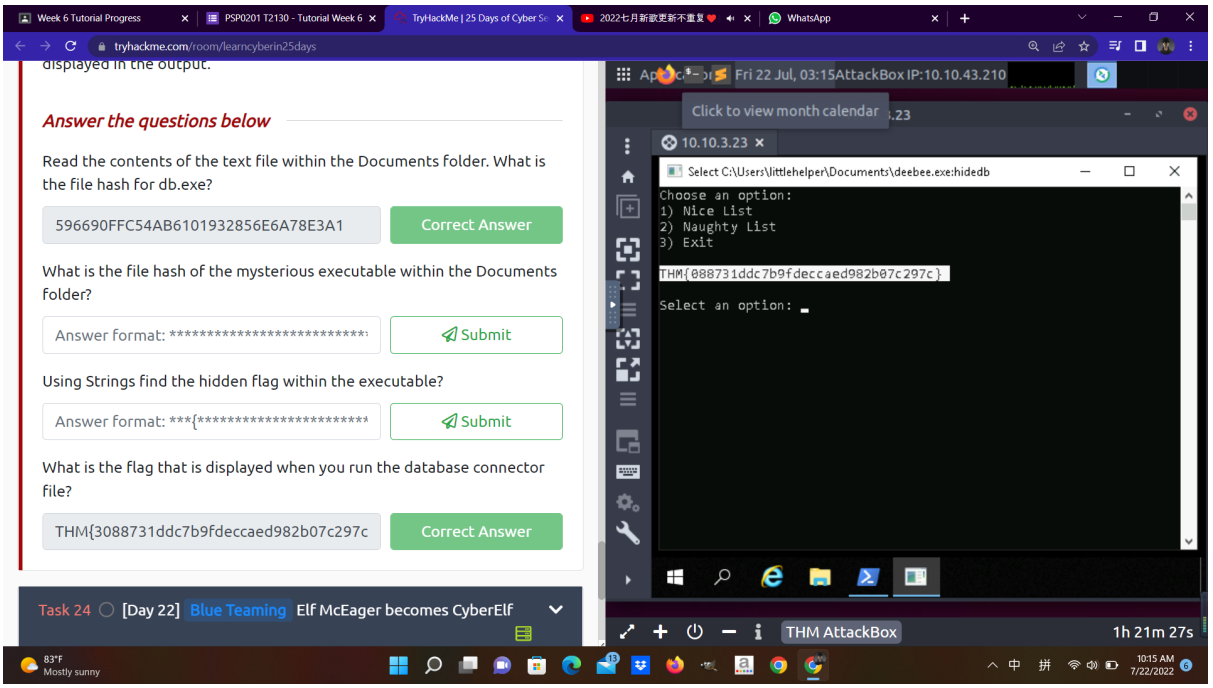
question 4


Week 6 Tutorial Progr
PSP0201 T2130 - Tutc
TryHackMe | 25 Days
THM Browser-Based
2022七月新歌更
(11) WhatsApp
PSP0201-Week 6 - Gc
vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=2d04f486a09412a7&proxyIP=10.10.43.210&resize=remote
Applications Places System Fri 22 Jul, 03:27
AttackBox IP:10.10.43.210
10.10.3.23
10.10.3.23
Select Windows PowerShell
Main
System.Reflection
Sleep
Clear
.ctor
System.Diagnostics
System.Runtime.InteropServices
System.Runtime.CompilerServices
DebuggingModes
args
Object
Accessing the Best Festival Company Database...
Done.
Using SSO to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\Documents\db.exe).Path -ReadCount 0 -Encoding Byte) -Encoding Byte -Stream hidedb
Hahaha .. guess what?
Your database connector file has been moved and you'll never find it!
I guess you can't query the naughty list anymore!
>;^P
zlV
WrapNonExceptionThrows
deebee
83°F
Mostly sunny
10:27 AM
7/22/2022

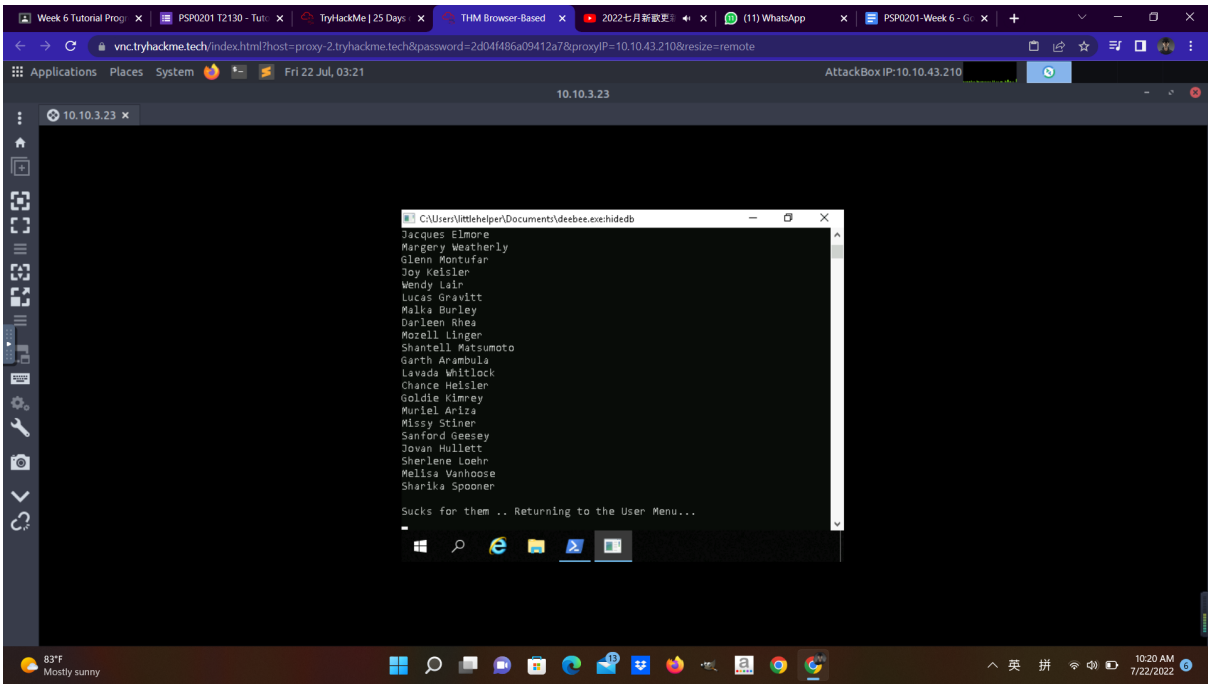
question 5



question 6

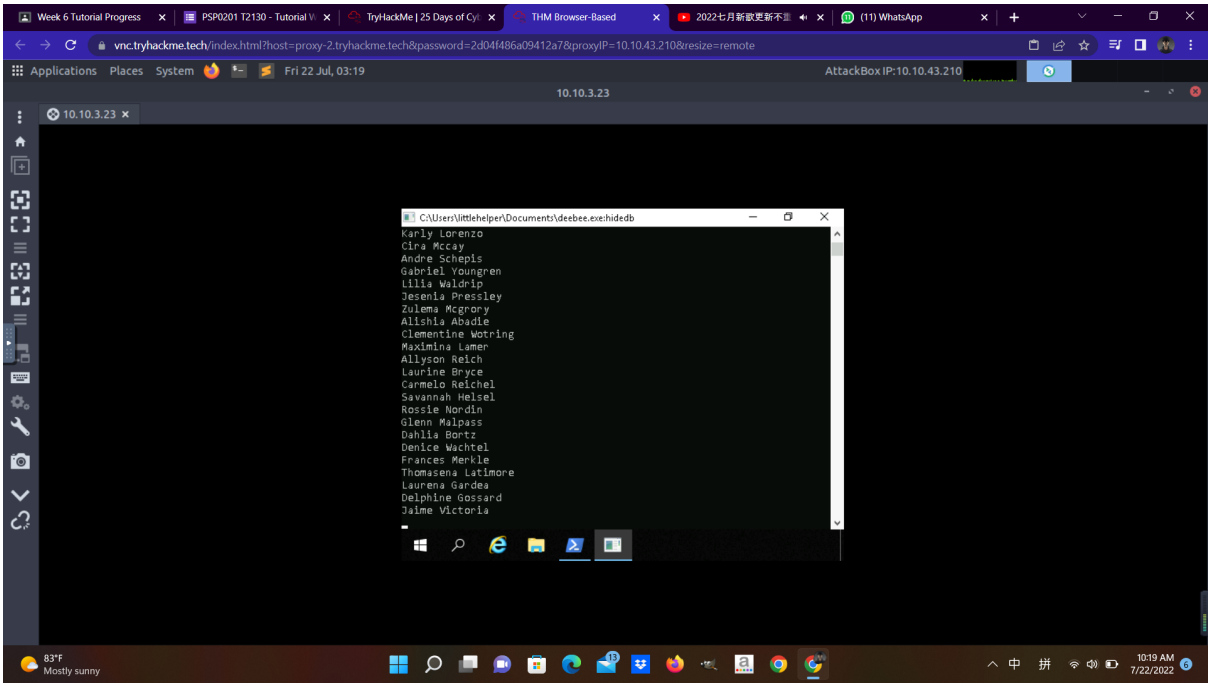


question7



Sharika Spooner is in the naugthy list

question 8



Jaime Victoria is in the nice list

Thought Process/Methodology:

we know that the file is sitting inside the 'Documents' so let's use the command 'cd' to 'Documents'.After that use 'dir' command to see the file name which is "deebee.exe".In order to see what is the file hash for db.exe(question 1) , we type the command 'more .\db file hash.txt'.Next, for the MD5 file hash of the mysterious executable within the Documents folder (question 2), we are able to use the command 'Get-FileHash -Algorithm MD5 file.txt' . For question 3 , we use the same command as question 2 ,but just change the MD5 to SHA256. Furthermore, use this command 'c:\Tools\strings64.exe -accepteula file.exe' to find the hidden flag .Lastly,this command : 'wmic process call create $(Resolve-Path file.exe:streamname)'is able to run to launch the hidden executable hiding within ADS but how can we know the streamname? we need to use this command `Get-Item -Path file.exe -Stream *`.after we know the streamname ,we are able to see the flag inside the hidden db.For question 7 and 8,just tye 1(nice list) or 2(naughty list) to see the name list.

Day 22: Blue Teaming Elf McEager becomes CyberElf

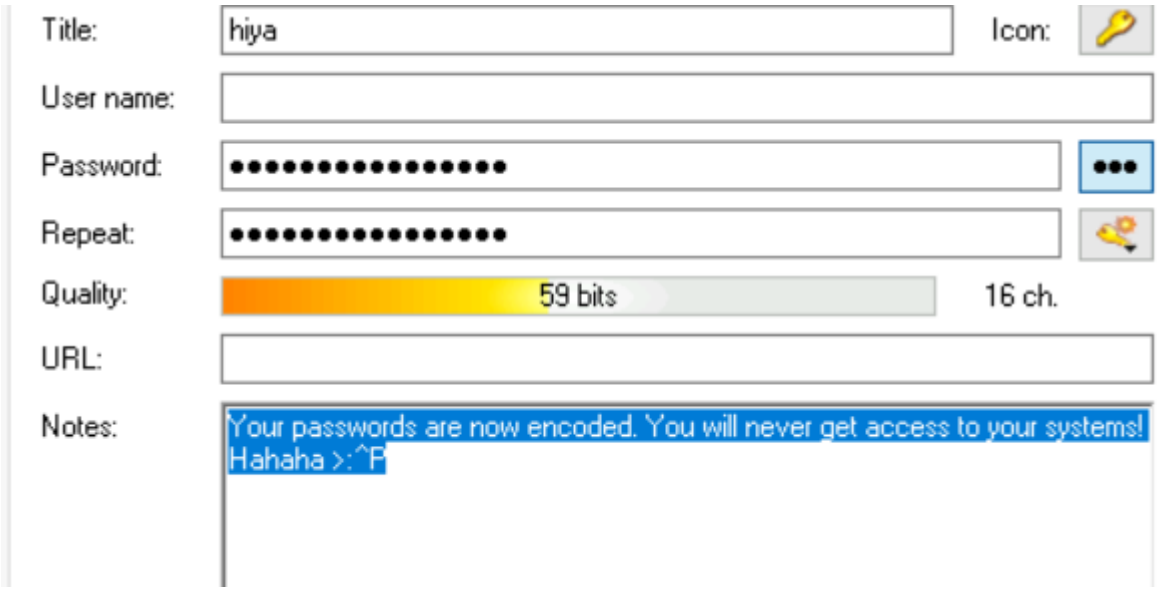
Tools used : Kali Linux, Cyberchef, Remmina

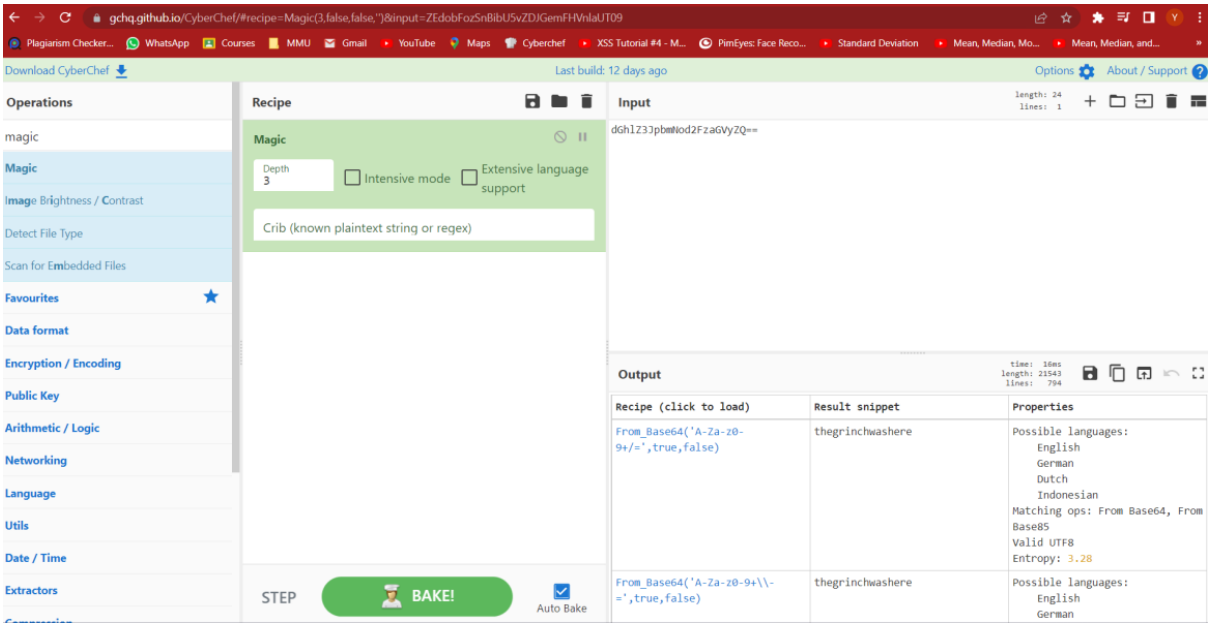
Walkthrough/ Solution : John Hammond

Q1: What is the password to the KeePass database?

Q2: What is the encoding method listed as the 'Matching ops'?

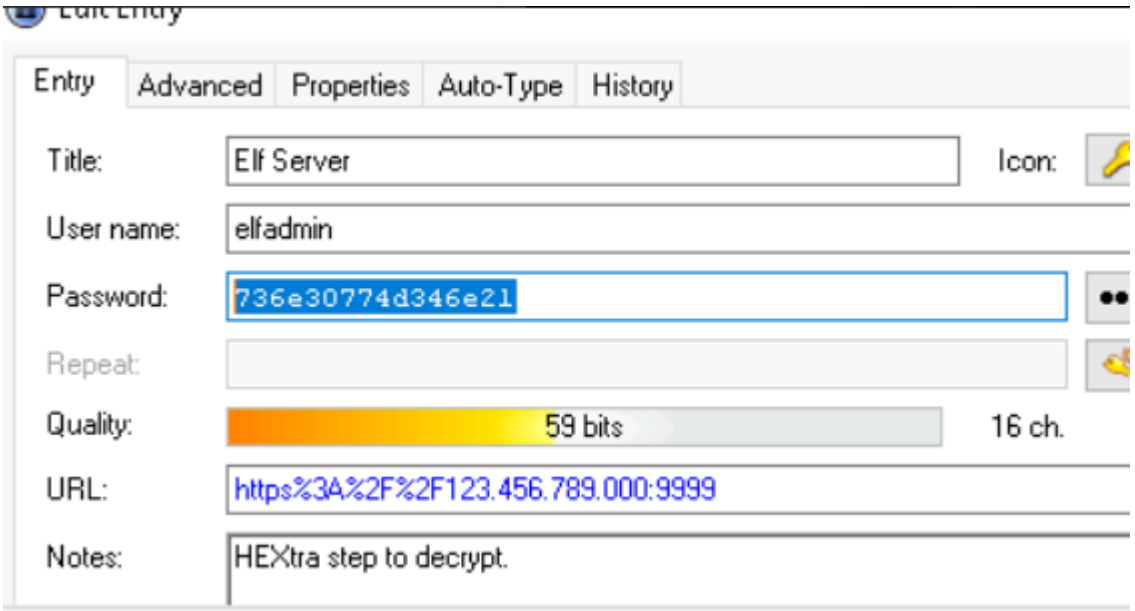
Q3: What is the note on the hiya key?





Q4: What is the decoded password value of the Elf Server?

Q5: What was the encoding used on the Elf Server password?



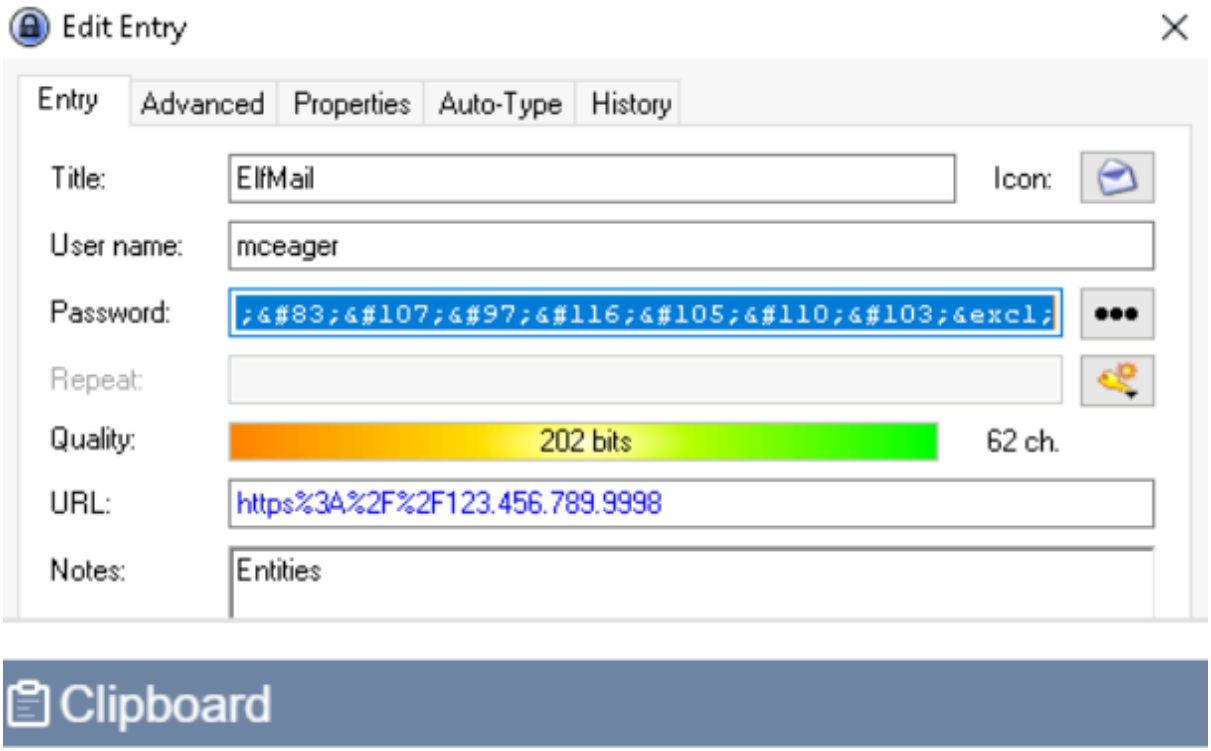
736e30774d346e21

Output

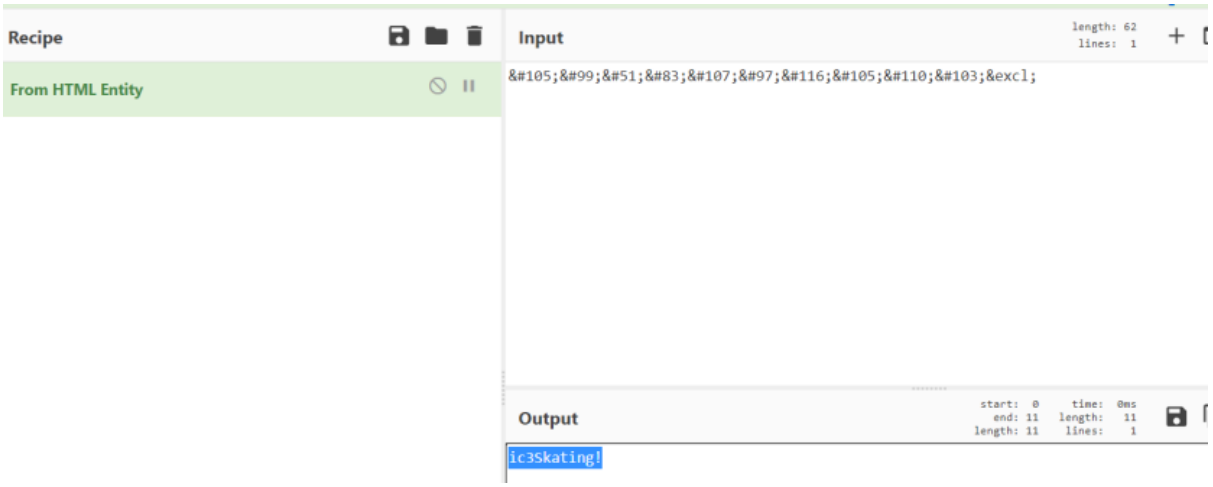
time: 14ms
length: 12389
lines: 466

Recipe (click to load)	Result snippet	Properties
From_Hex('None')	sn0wM4n!	Valid UTF8 Entropy: 2.75
	736e30774d346e21	Matching ops: From Base64, From Base85, From Hex, From Hexdump Valid UTF8 Entropy: 3.03

Q6: What is the decoded password value for ElfMail?

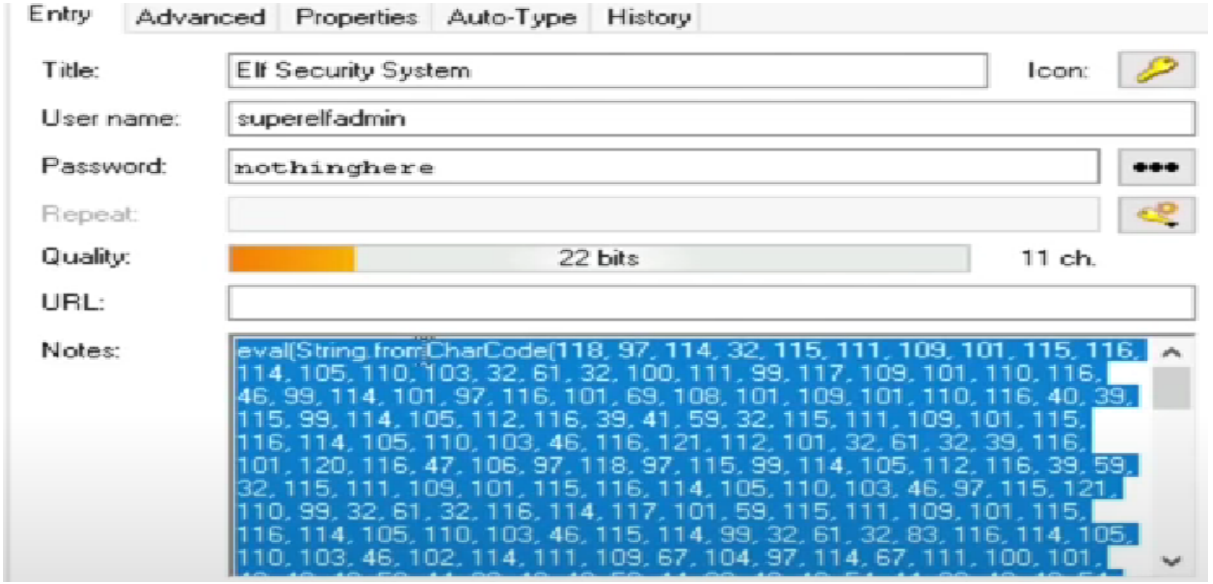


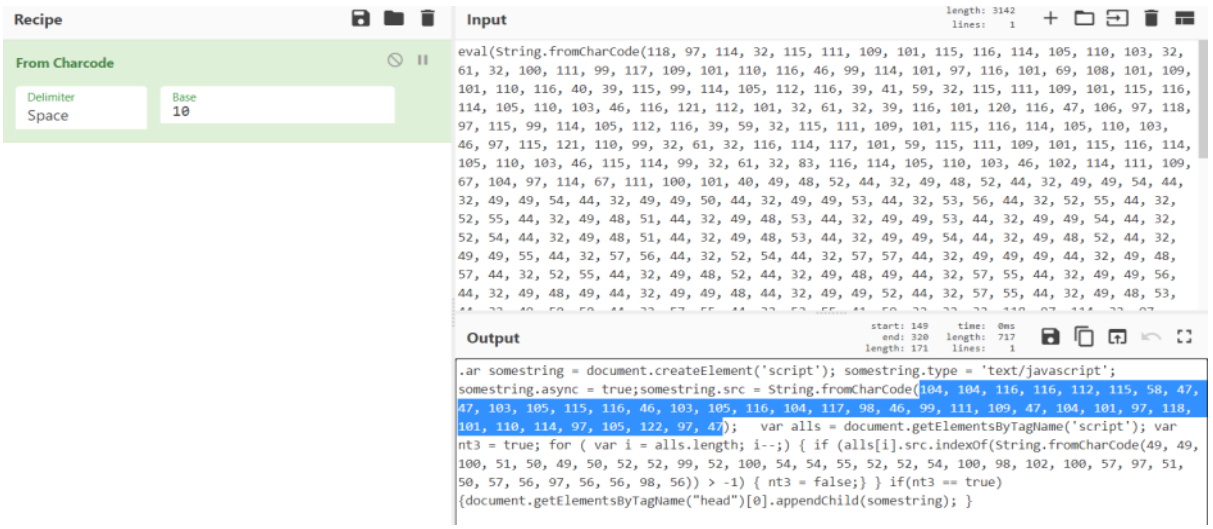
Clipboard

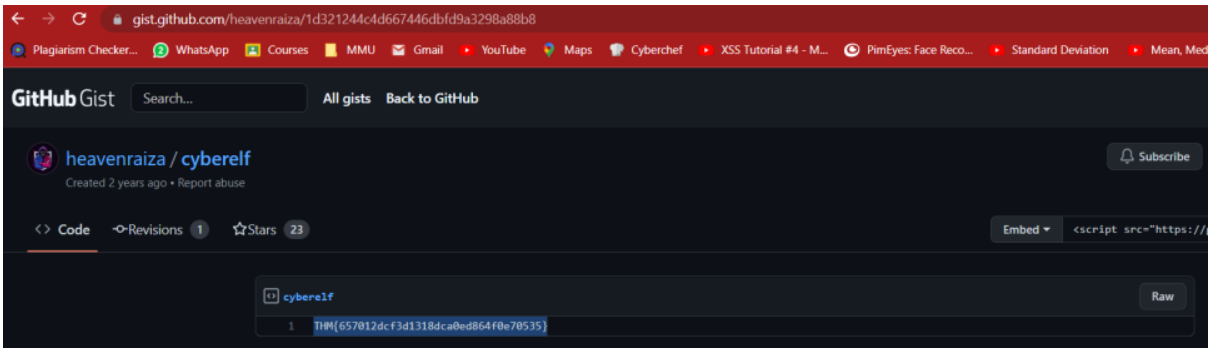


Q7: What is the username:password pair of Elf Security System?

Q8: Decode the last encoded value. What is the flag?







Thought process:

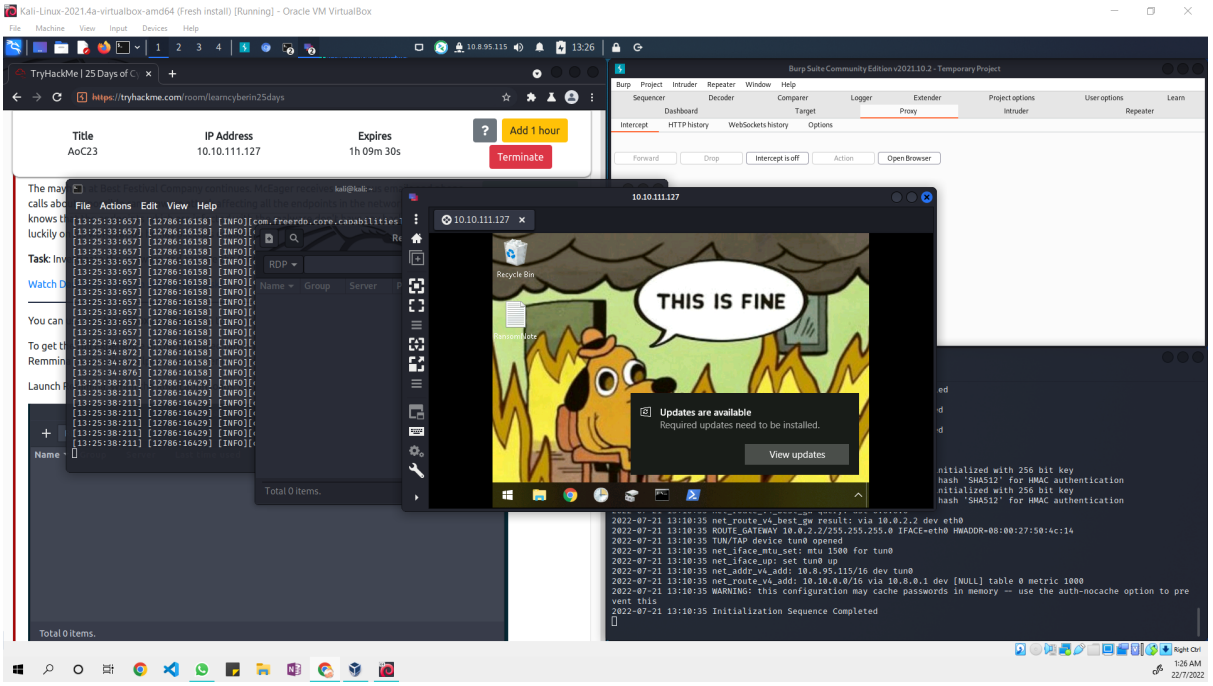
After accessing the remmina and clicking into the weird folder, we see a keepass which is a free source password manager. After that we use the cyberchef to decode the password given in the keepass with Magic and get the password and know the matching ops. The same steps are used for question 4 and 5. For question 6 , we have decoded the password with the help of the hint provided by thm which is decoding the password using html entity and getting the password. Q7 and Q8 we tried to decode the weird text at the note with the hint 'from charcode' by thm and found the link to the flag.

Day 23: Blue Teaming - The Grinch strikes again!

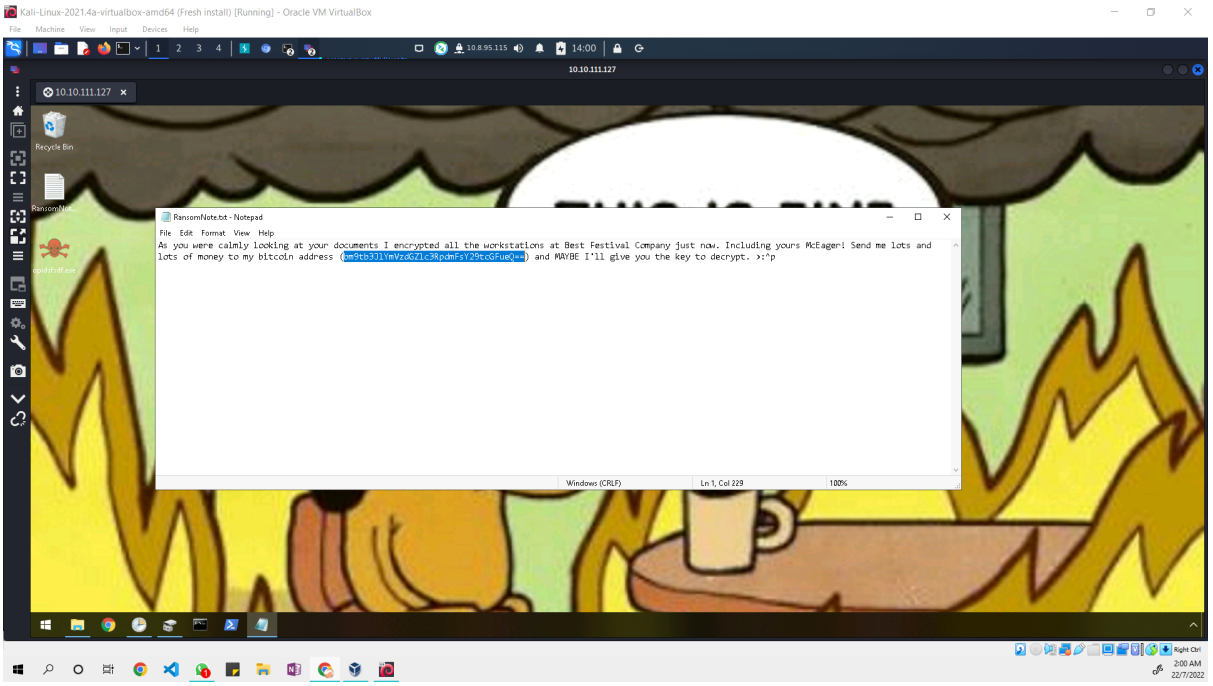
Tools used: Kali Linux, Chrome

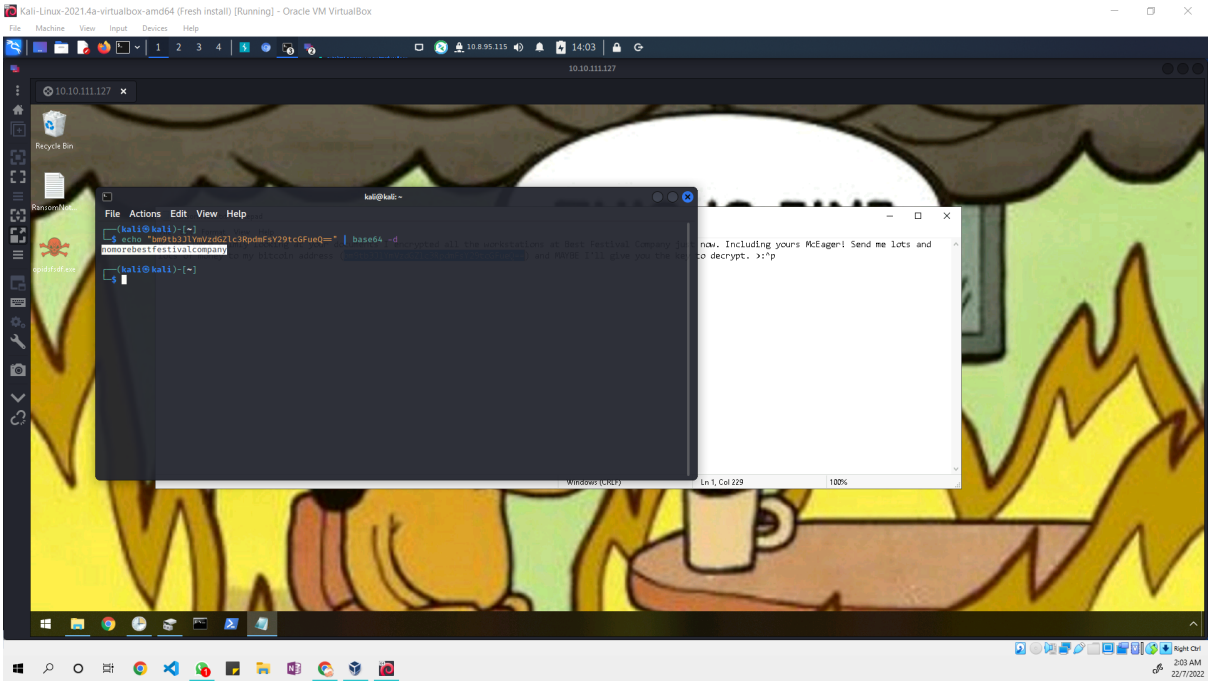
Solution/walkthrough:

Q1: What does the wallpaper say?

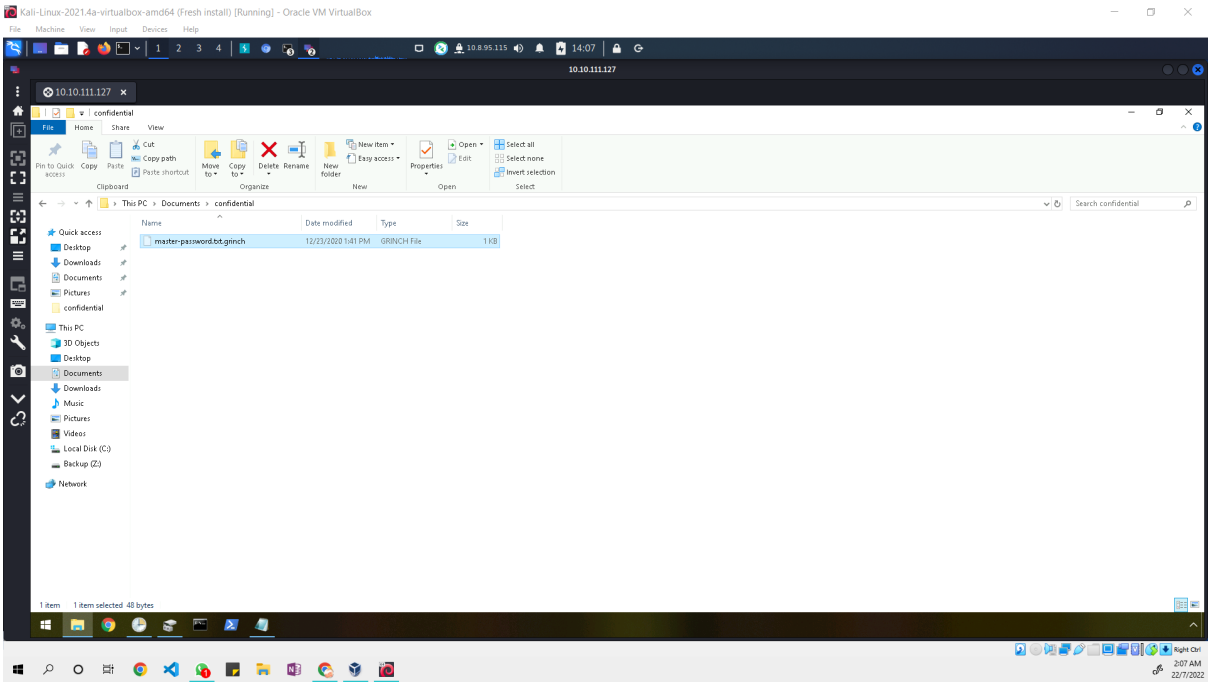


Q2: Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

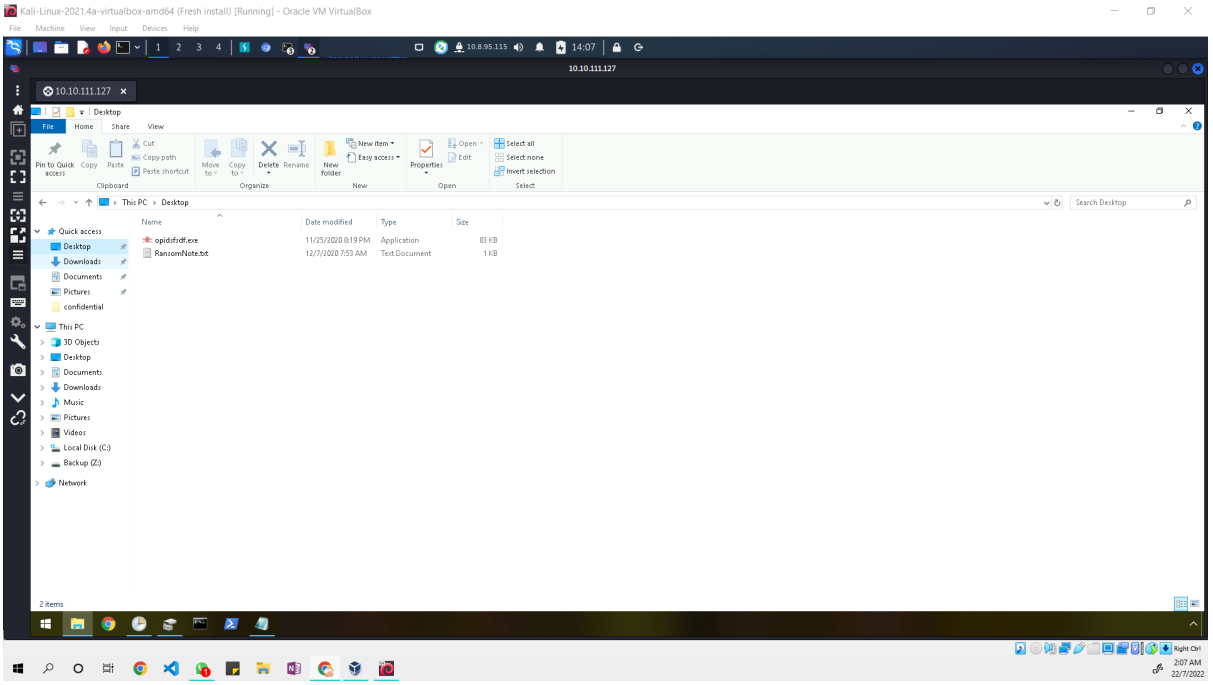




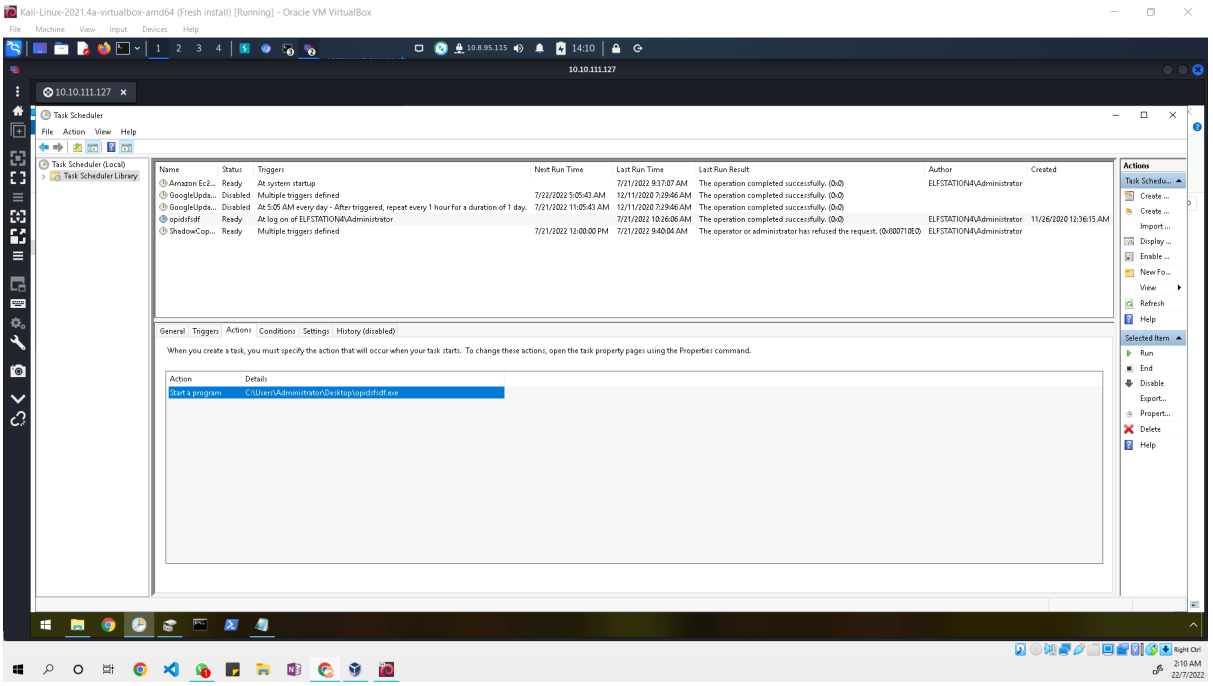
Q3: At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?



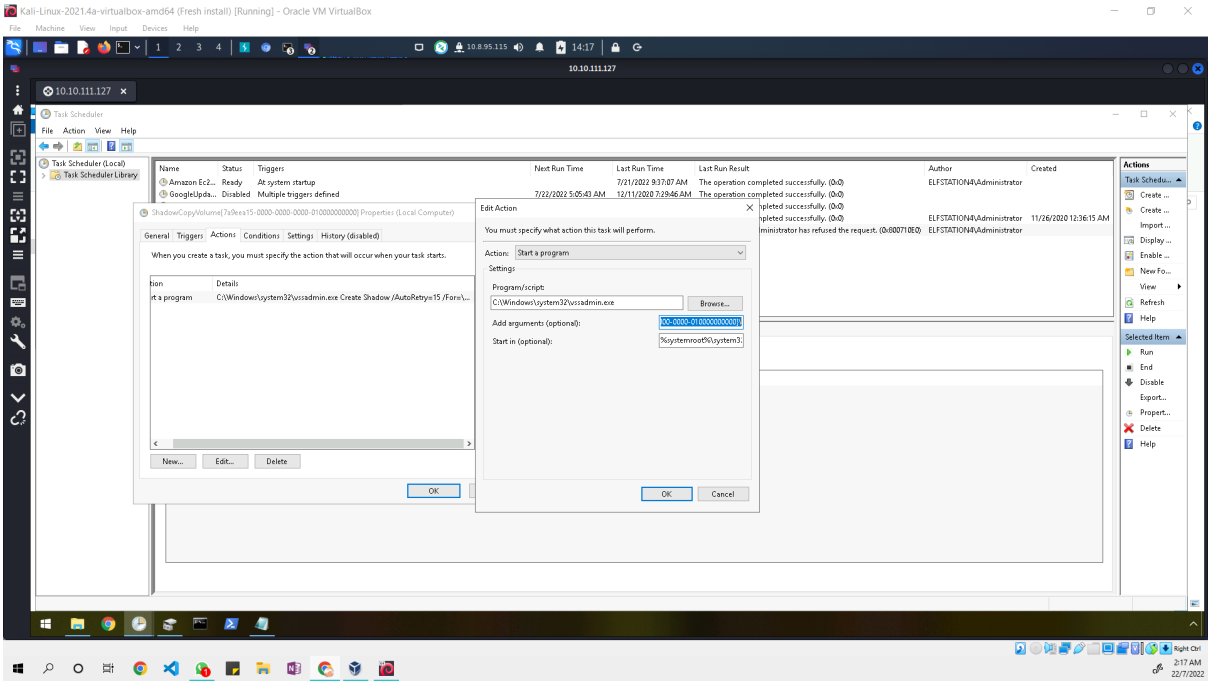
Q4: What is the name of the suspicious scheduled task?



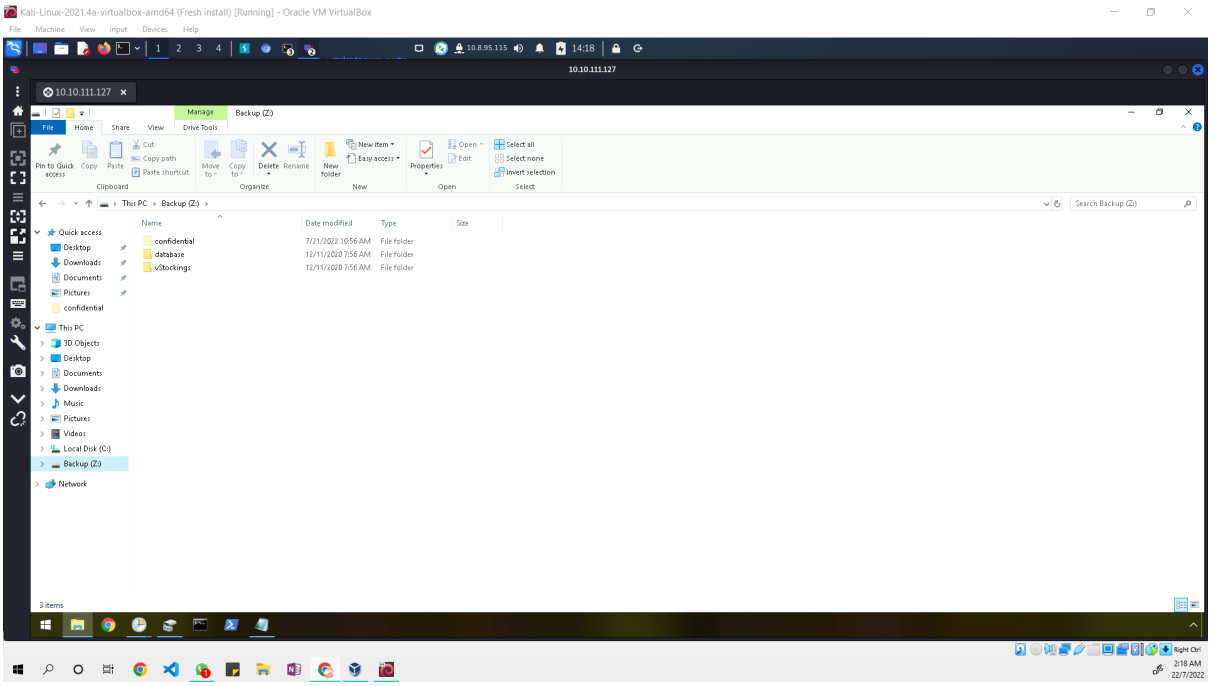
Q5: Inspect the properties of the scheduled task. What is the location of the executable that is run at login?



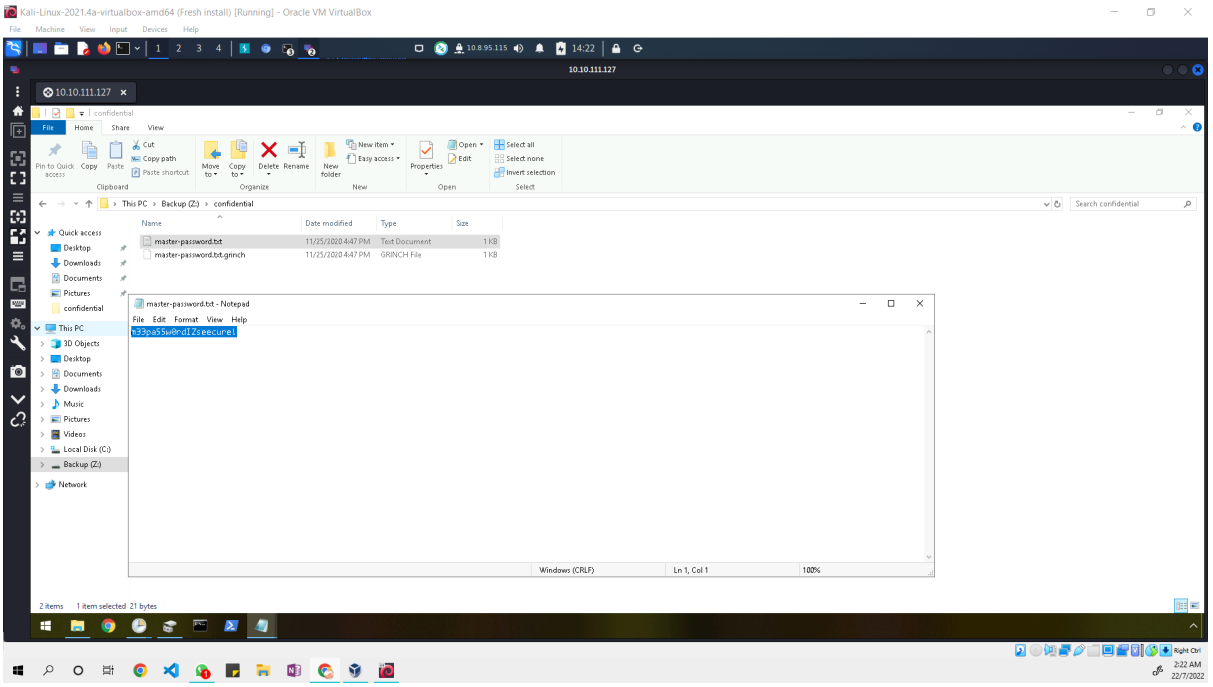
Q6: There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?



Q7: Assign the hidden partition a letter. What is the name of the hidden folder?



Q8: 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?



Thought Process/Methodology:

First, we open the terminal and type in ‘remmina’ to install remmina. After installing, we type in ‘remmina &’ and it pops out the ‘Remmina Remote Desktop Client’ window. We click on the ellipsis button and open the ‘Preferences’ option. We go to RDP and change the quality settings to poor (fastest) and tick the ‘Wallpaper’. We close the ‘Preferences’ and click on the plus button (+). It pops out the ‘Remote Connection Profile’ window. We type in our IP address in the server column. We also type in the username (administrator) and password (sn0wF!akes!!!) in the username and password column respectively. Afterwards, we change the color depth into RemoteFX (32 bpp) and save as default. We click on the connect button. It pops out the IP address window with certificate details to let us accept the certificate. We accept it. It pops out another IP address window but with a desktop view. We click on the Task Scheduler button. It pops out the Task Scheduler window. We click on the ‘Task Scheduler Library’ and click on the ‘opidsfsdf’. We see the content of ‘Triggers’ and ‘Actions’. Then, we open the ‘Disk Management’. We right click on the Backup and click on Properties. We click on the Security and see the Object name, then we close the Properties. We right click on the Backup again and click on Change Drive Letter and Paths. We click on ‘Add…’ and choose ‘Assign the following drive letter:’ and change the letter option to ‘Z’. The name of Backup has been changed to ‘Backup (Z:)’. Then, we click on ‘File Explorer’ and go to ‘Backup (Z:)’. We go to ‘View’ and tick the ‘Hidden items’ and ‘File name extensions’. It shows a hidden folder named ‘confidential’. We right click on it and click on ‘Properties’. We click on the ‘Previous Versions’, select the ‘confidential’ file and click on ‘Restore’. After the folder has been successfully restored to the previous version, we go to the desktop and click on the ‘RansomNote.txt’. It shows us ‘As you were calmly looking at your documents I encrypted all the workstations at Best Festival Company just now. Including yours McEager! Send me lots and lots of money to my bitcoin address (bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==) and MAYBE I'll give you the key to decrypt. >:^p’ . We copy the bitcoin address (bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==) and go to the terminal to key in ‘echo "bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==" | base64 -d’. It shows ‘nomorebestfestivalcompany’ to us. Afterwards, we go to File Explorer and go to Documents, and click on the ‘confidential’. It shows the file extension for each of the encrypted files, which is ‘.grinch’. Afterwards, we go to the

desktop and we see the name of the suspicious scheduled task, which is ‘opidsfsdf’. Afterwards, we go back to the Task Scheduler and click on ‘opidsfsdf’ and click on ‘Actions’. We see the details. Afterwards, we right click on the ‘ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}’ and click on ‘Properties’. We click on the ‘Actions’ and double click on the content under the details. We copy the ShadowCopyVolume ID from the ‘Add arguments (optional)’. Afterwards, we go back to the ‘confidential’ file again. We right click on the ‘confidential’ and click into the ‘Properties’. We click on the ‘Previous Versions’, select the ‘confidential’ and click on ‘Restore’. Then, we go back into the ‘confidential’, we click on the ‘master-password.txt’, it shows us the password within the file.

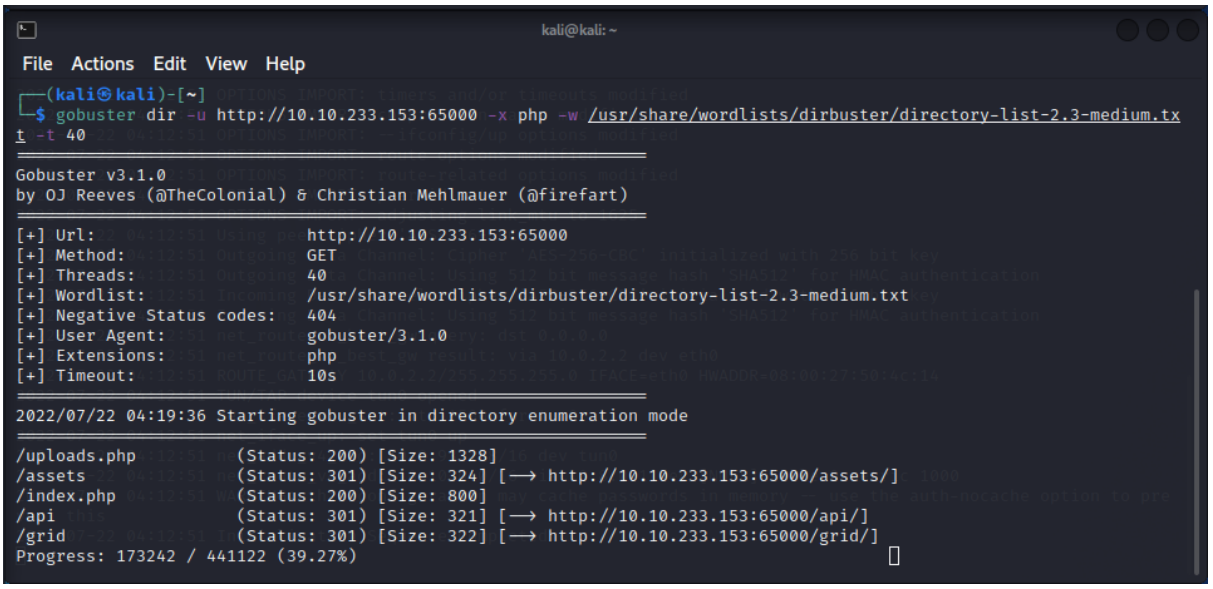
Day 24: Final Challenge – The Trial Before Christmas

Tools used: Kali Linux, Chrome

Solution/walkthrough: Darkstar

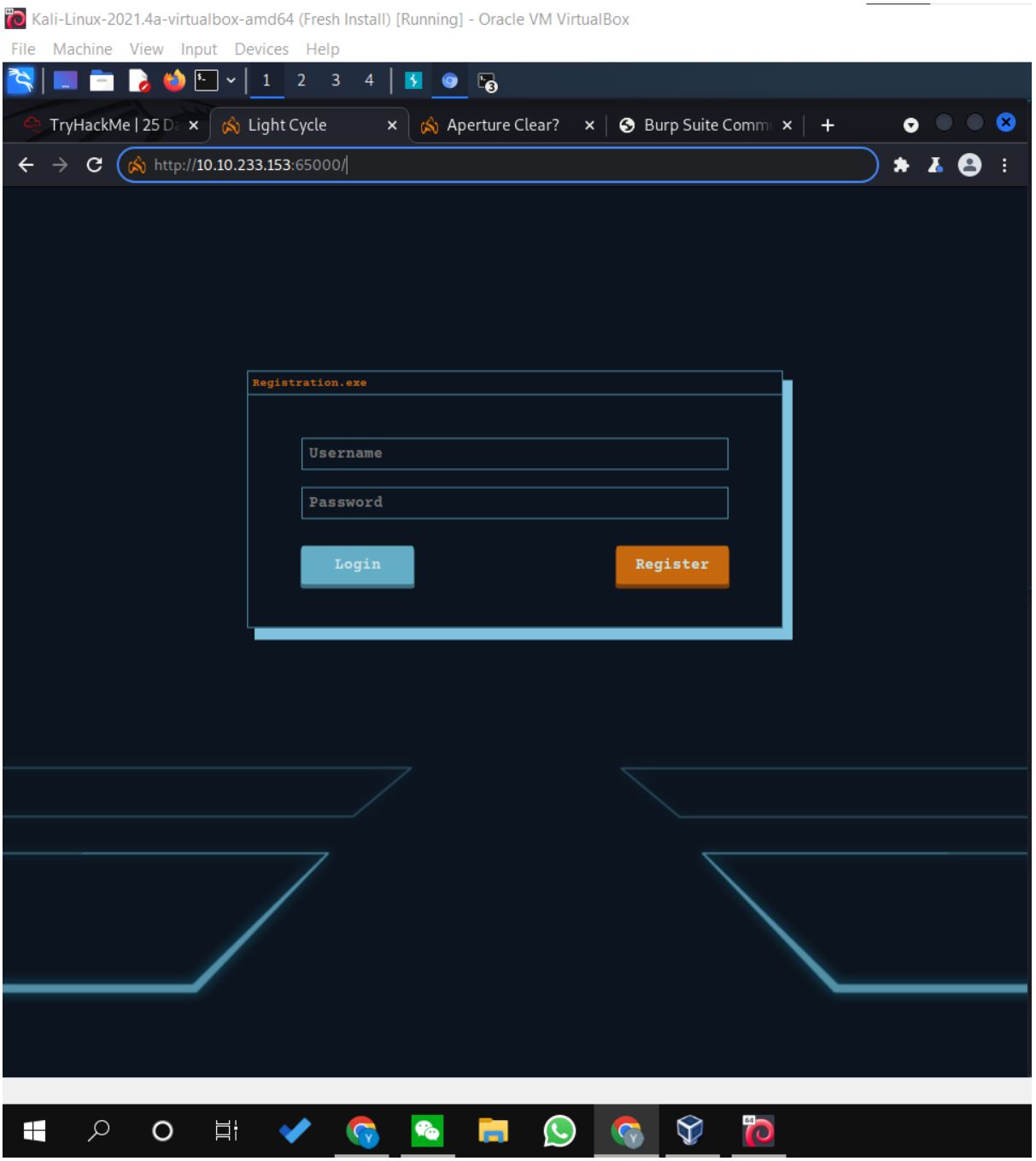
Question 1

Scan the machine. What ports are open?



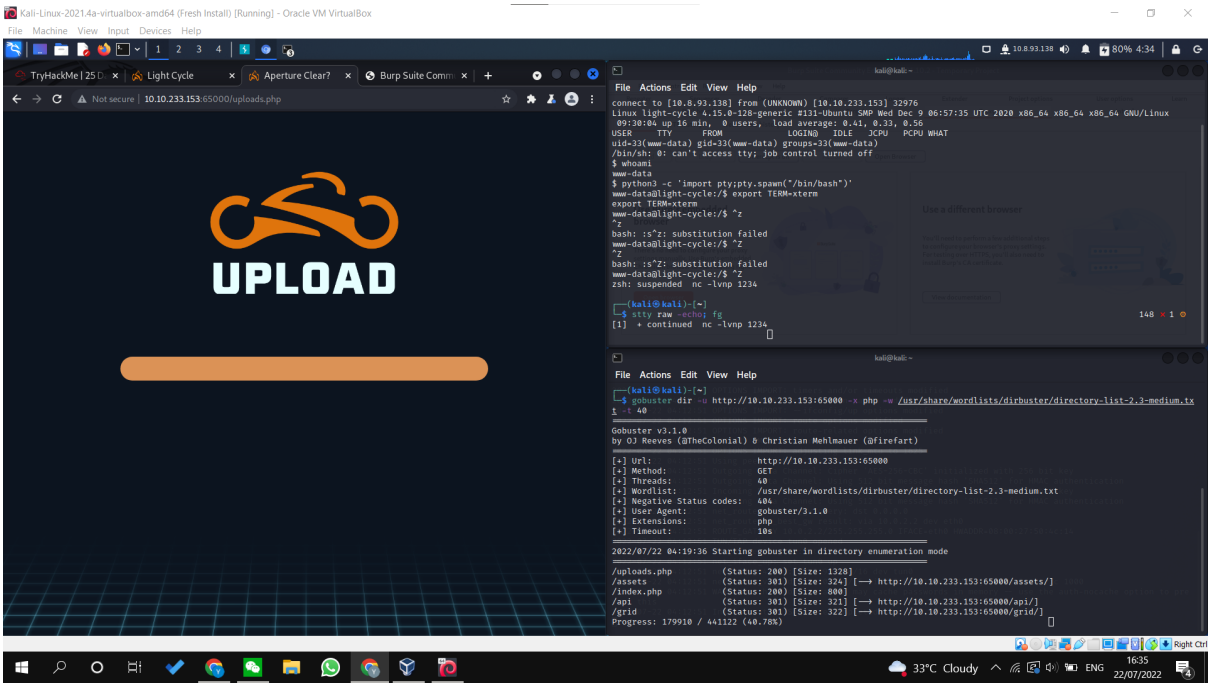
Question 2

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



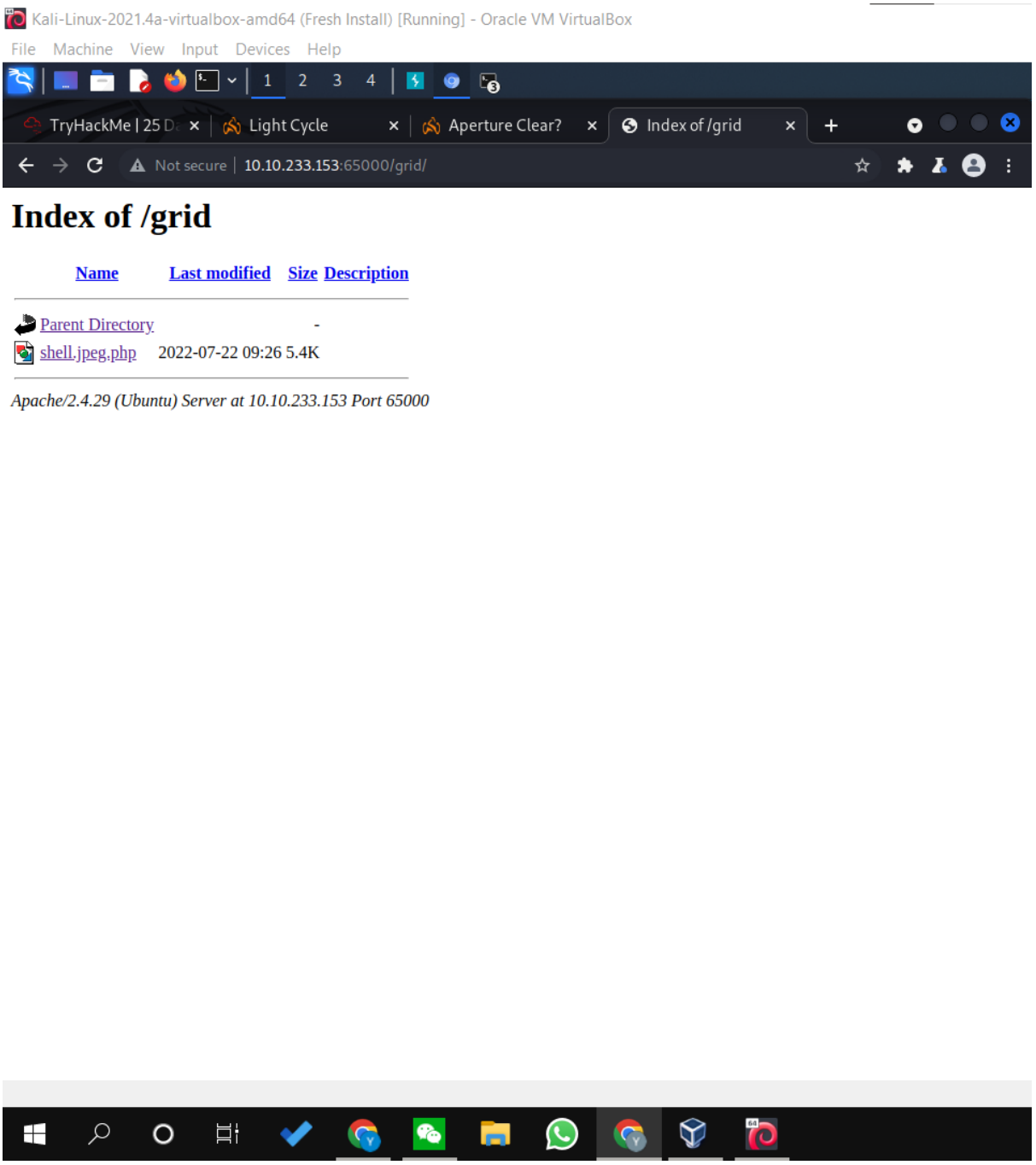
Question 3

What is the name of the hidden php page?



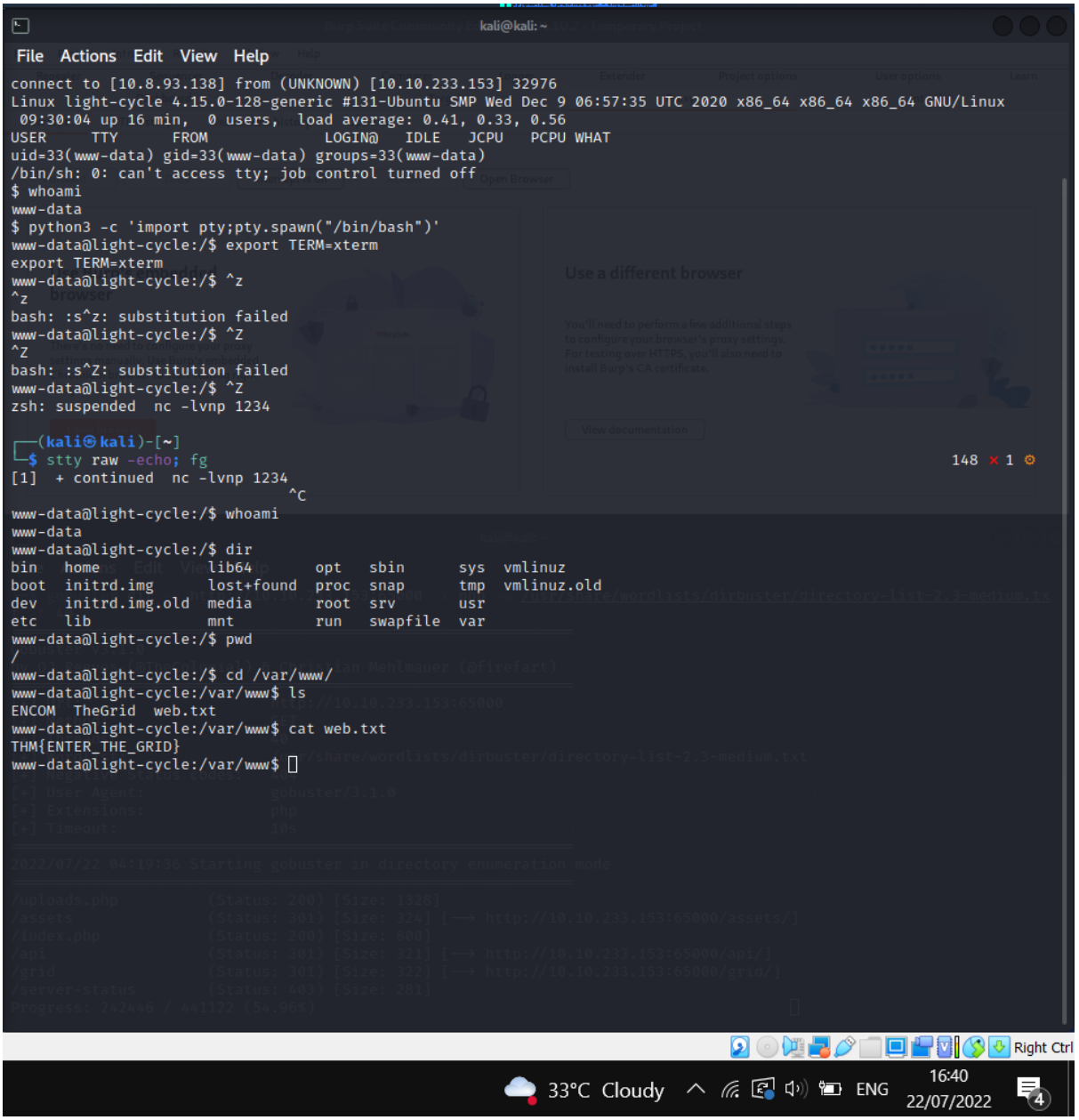
Question 4

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



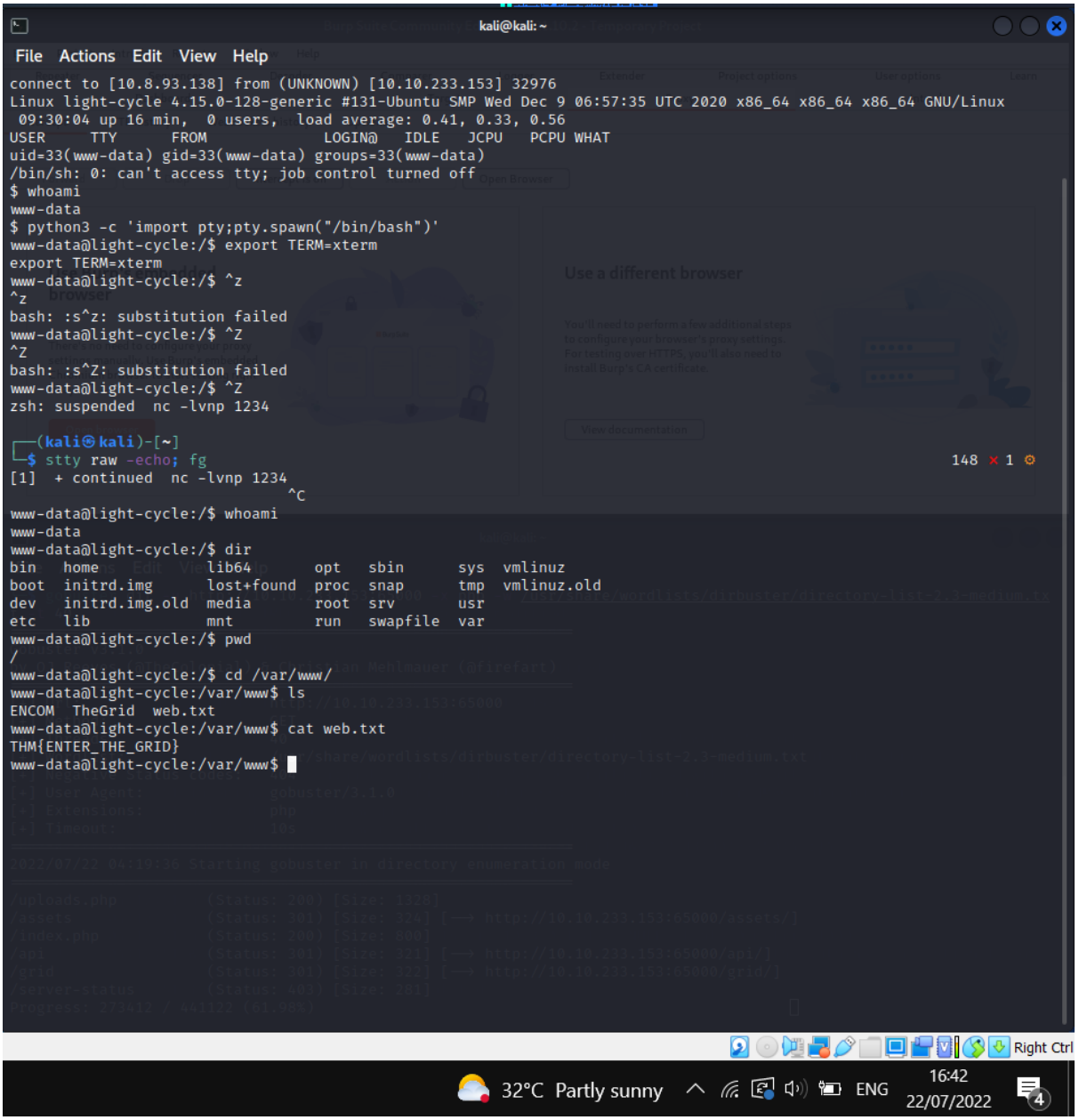
Question 5

What is the value of the web.txt flag?



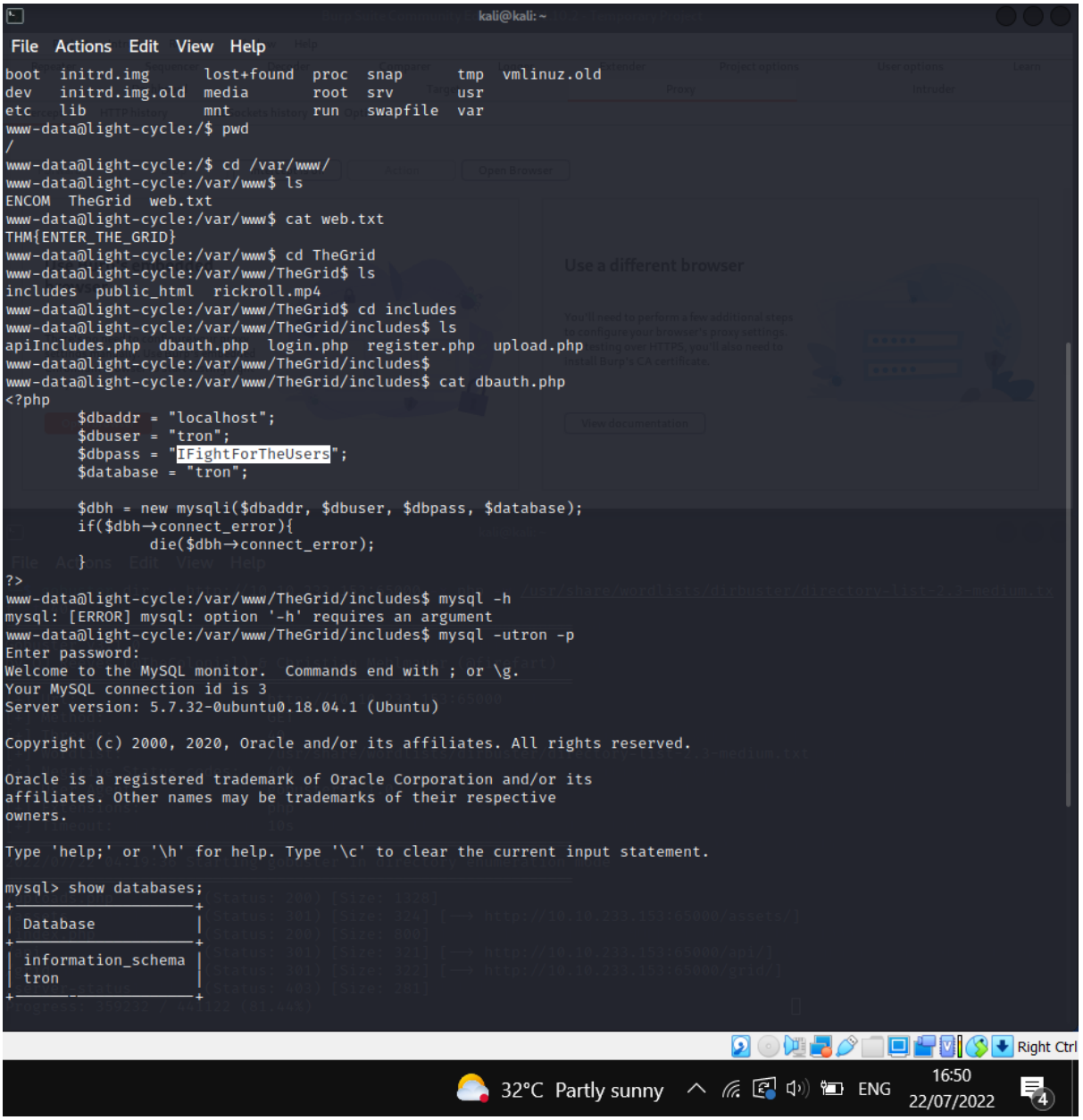
Question 6

What lines are used to upgrade and stabilize your shell?



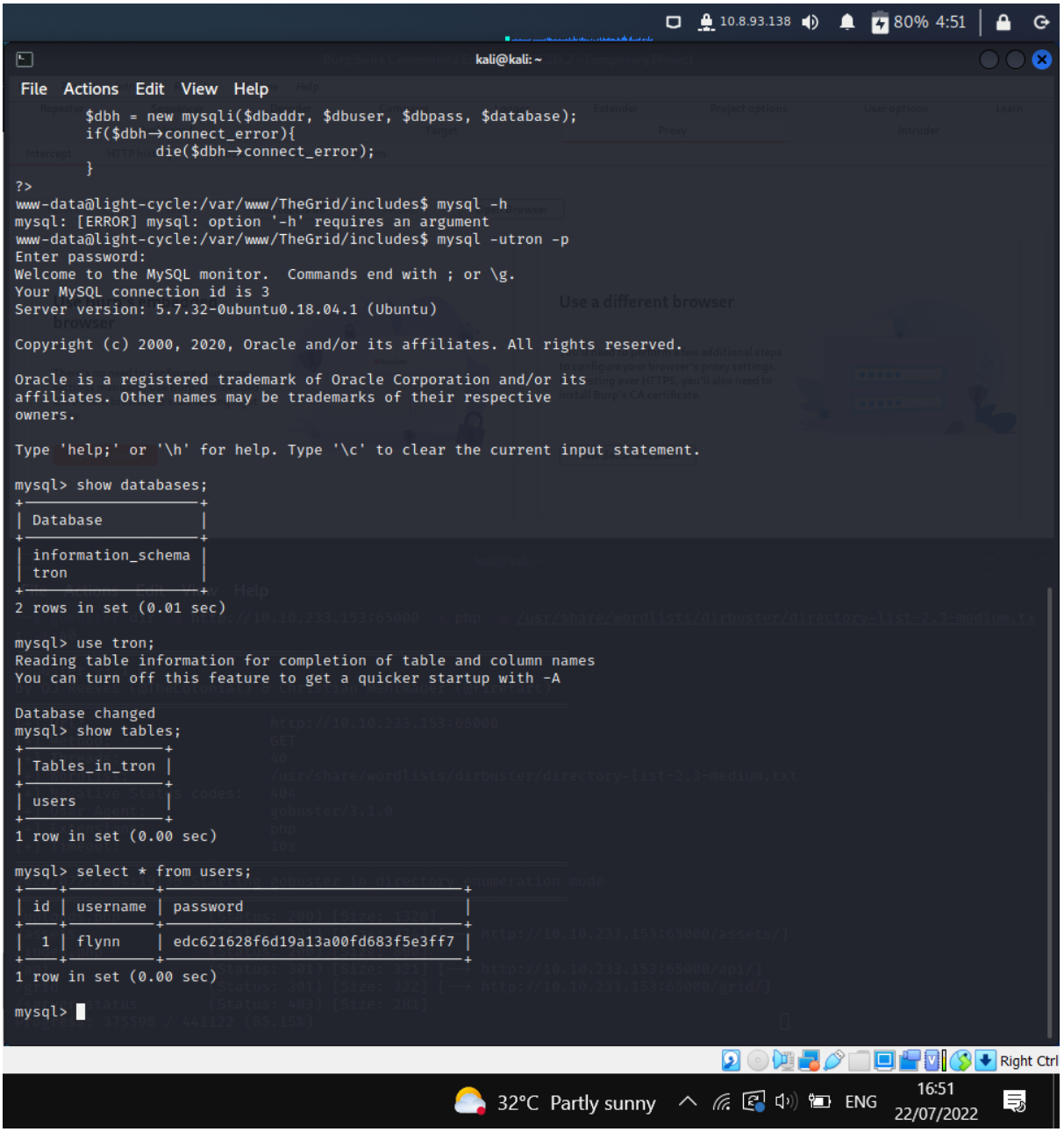
Question 7

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



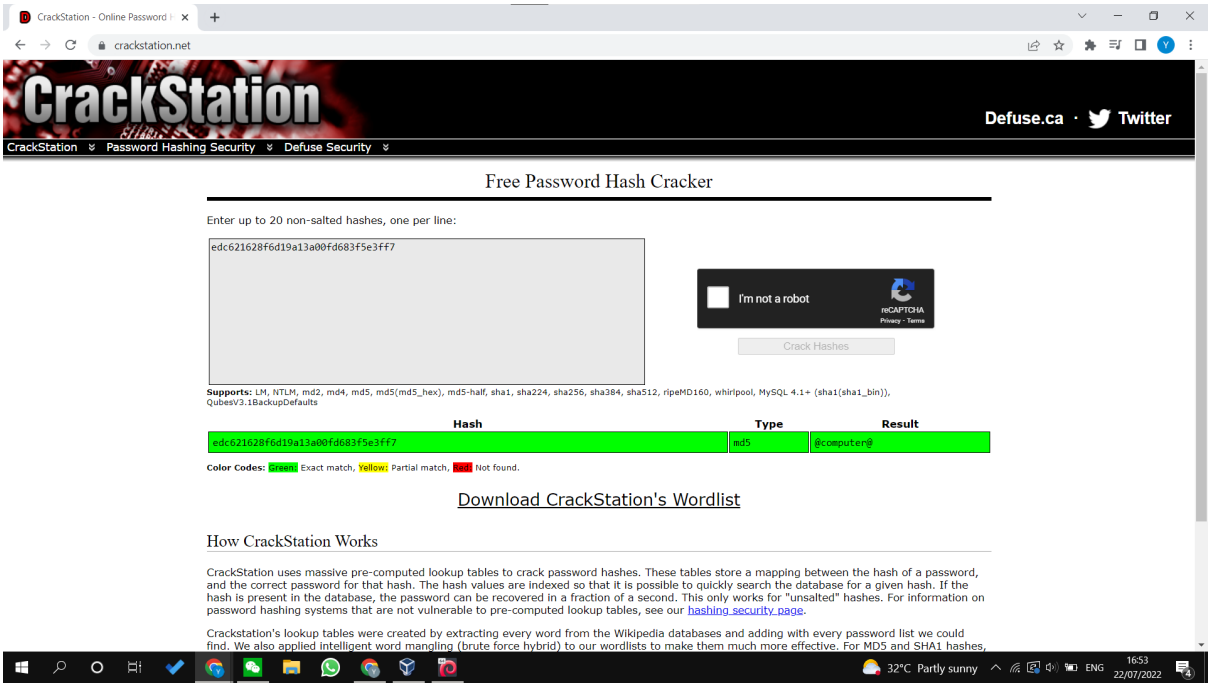
Question 8

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



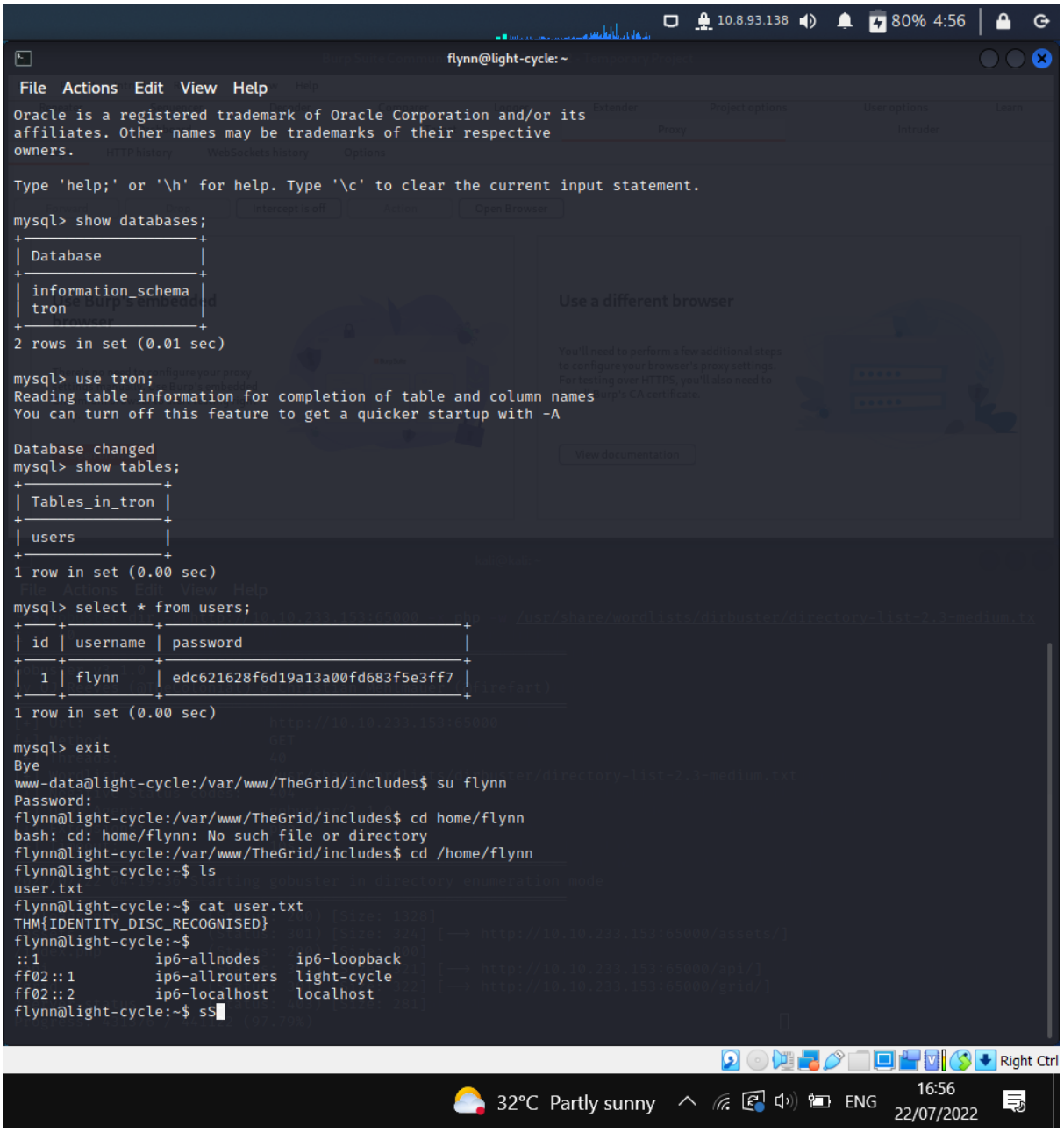
Question 9

Crack the password. What is it?



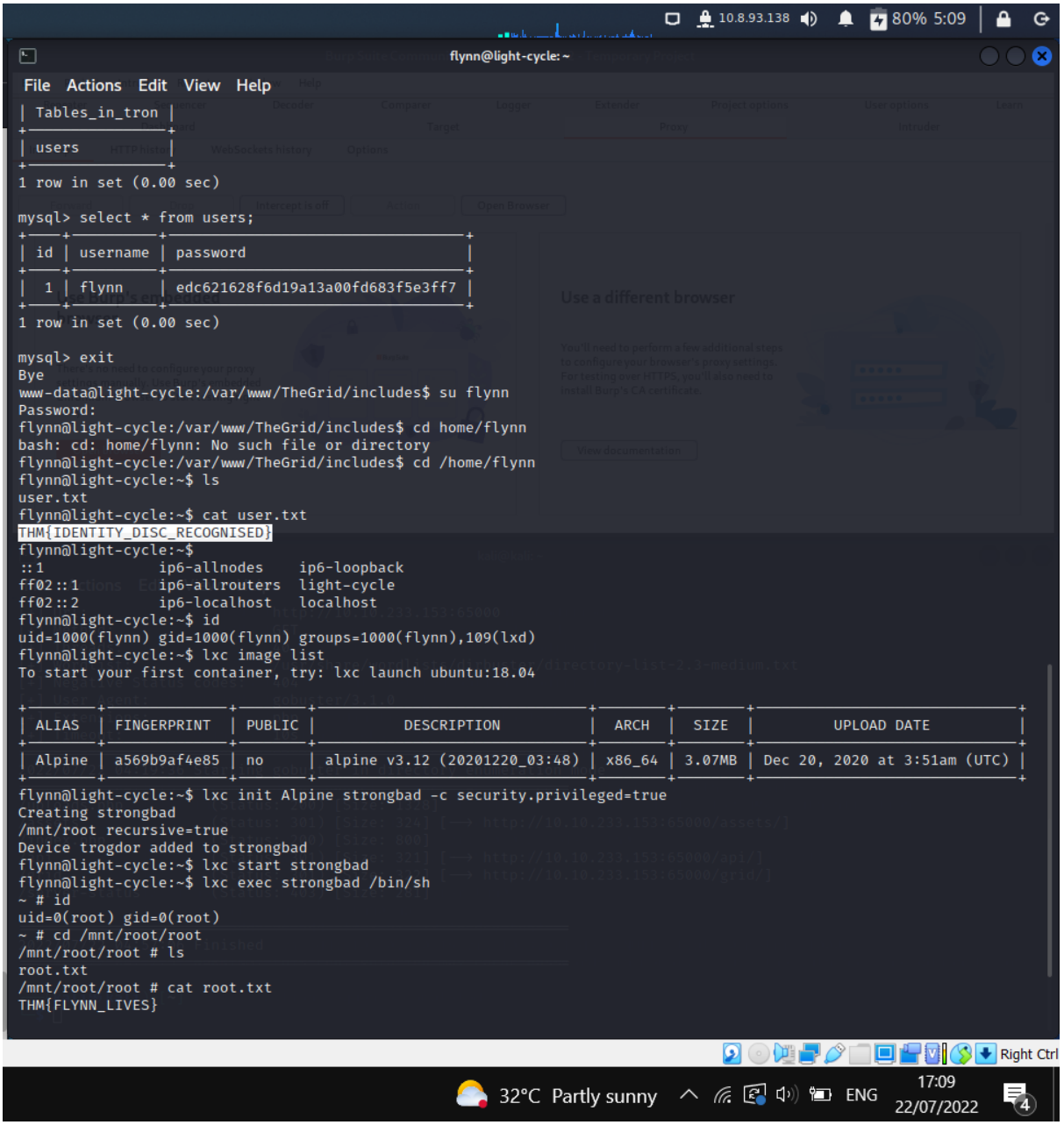
Question 10

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



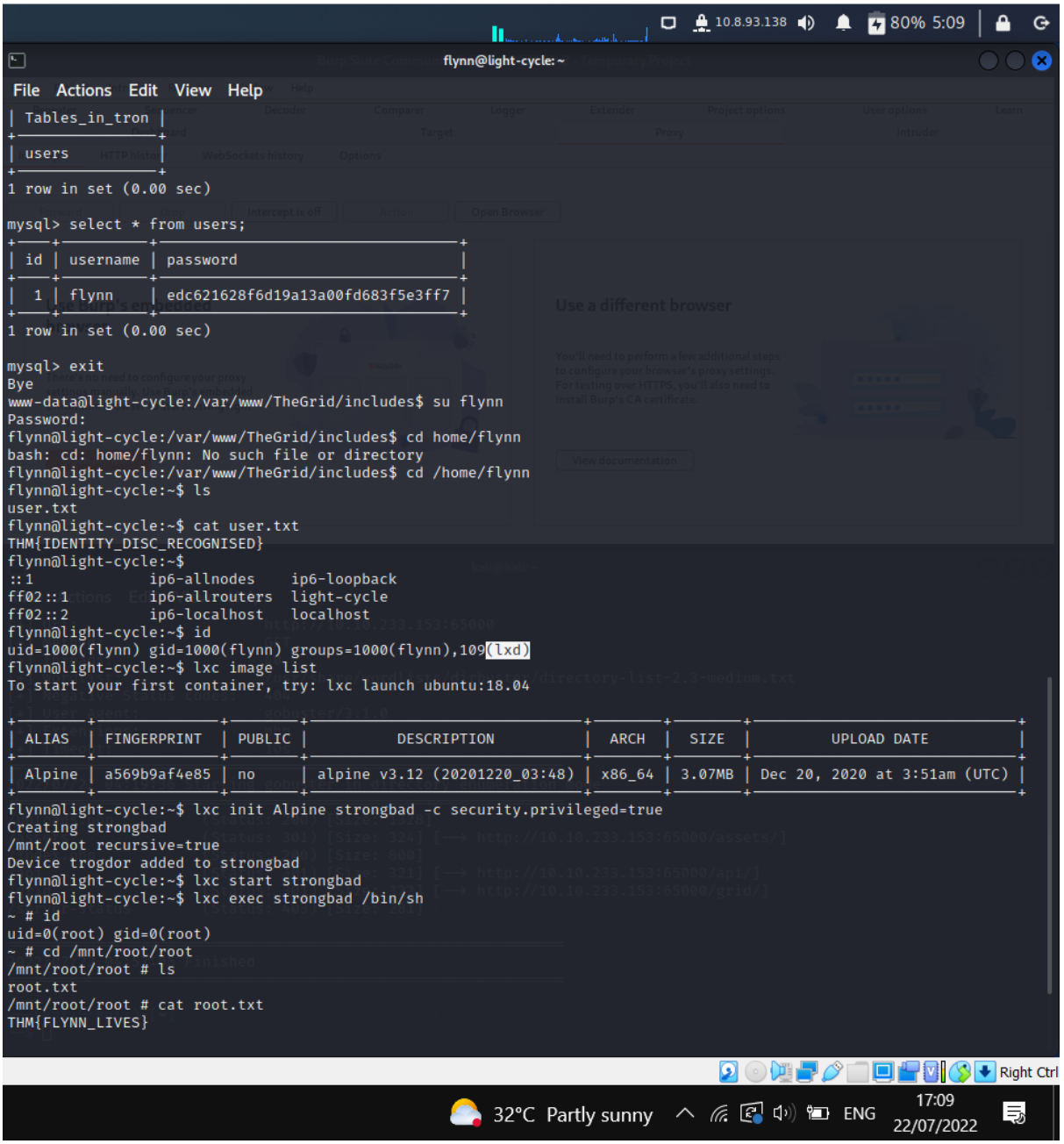
Question 11

What is the value of the user.txt flag?



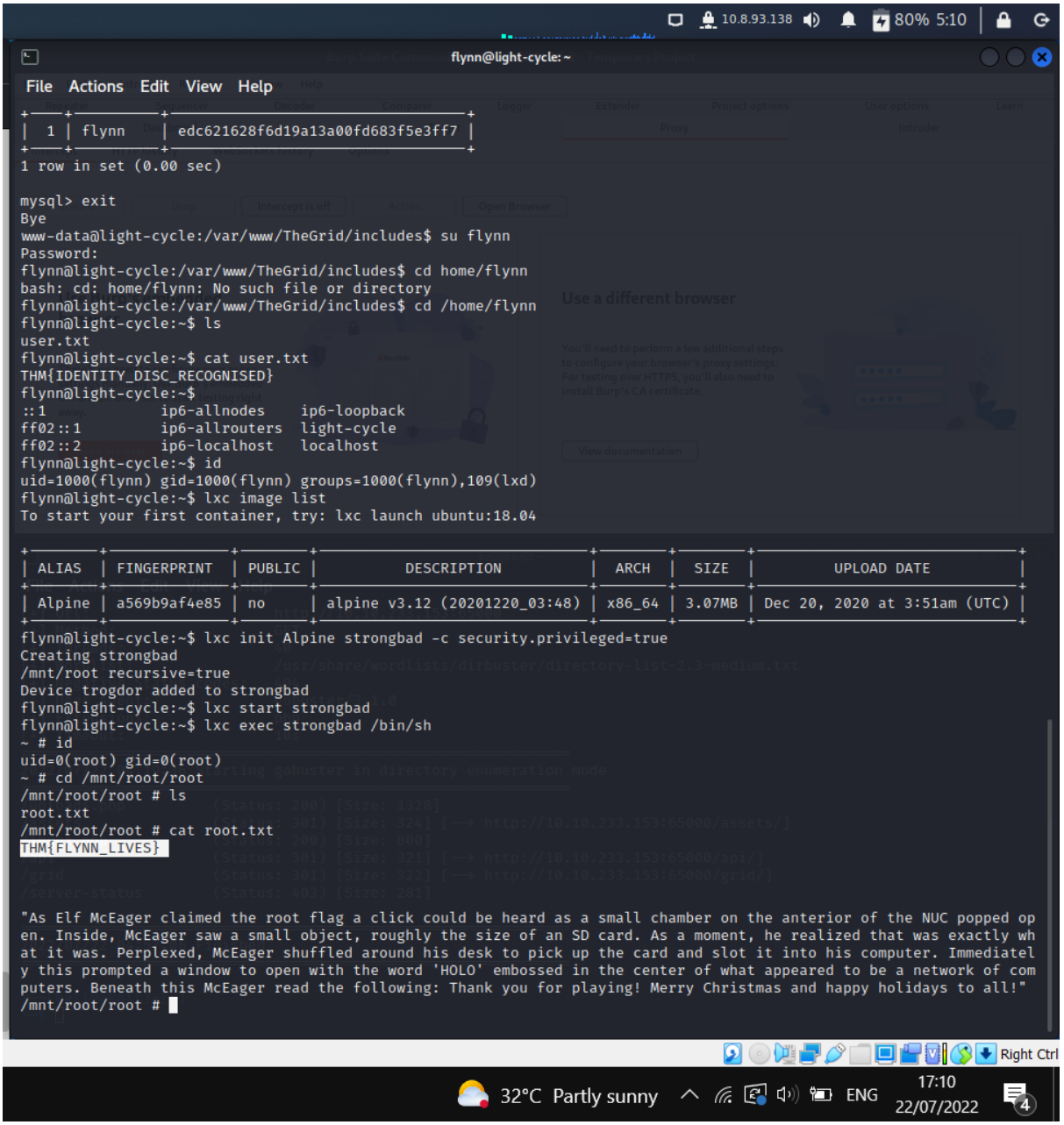
Question 12

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



Question 13

What is the value of the root.txt flag?



Thought Process/Methodology:

Having accessed the target machine, we used nmap with my IP address and viewed the needed information. Next, we went to the login webpage. After that, we used gobuster to find the hidden webpage and other information. Then, we removed the javascript filter on proxy and switched on proxy. Next, we forwarded the GET request and dropped the client-side filter. After that was done, we modified shell.jpg.php and opened a listener. Next, we uploaded the shell.jpg.php and clicked it on the file. When the listener connected to the file, we used python3 -c 'import pty;pty.spawn("/bin/bash")' to spawn a better-featured bash shell. Next, we used export “TERM=xterm” to access the command “clear”. Then, we stopped the listener and used “stty raw -echo; fg”. Next, we used dir and pwd. After that, we changed the directory to /var/www/ and opened web.txt. After that, we changed the directory to TheGrid/ and went into includes. Then, I

opened dbauth.php. After that, we used mysql -utron -p and keyed in the password. Then, we viewed the databases and tables. After that, we selected users and we were shown the encoded password of flynn. Next, we cracked the password and used su to exploit the new user. After that, we opened user.txt and used lxc image list. When we were shown images, we create the box (strongbad) with the device name (trogdor). Then, we start the container and changed directory to /mnt/root/root. Then, we opened the root.txt.