PSP0201

Week 6

Writeup

Group Name: DNA

Members

ID	Name	Role
1211102532	DHARVIN SHAH KUMAR BIN MOHAMAD SHAH RAVIN	Leader
1211101179	ALIPH RAIHAN BIN ANUAR	Member
1211102427	NUR NATHIFA BINTI MOHD IZHAR	Member

Day 21 - [Blue Teaming] Time for some ELForensics

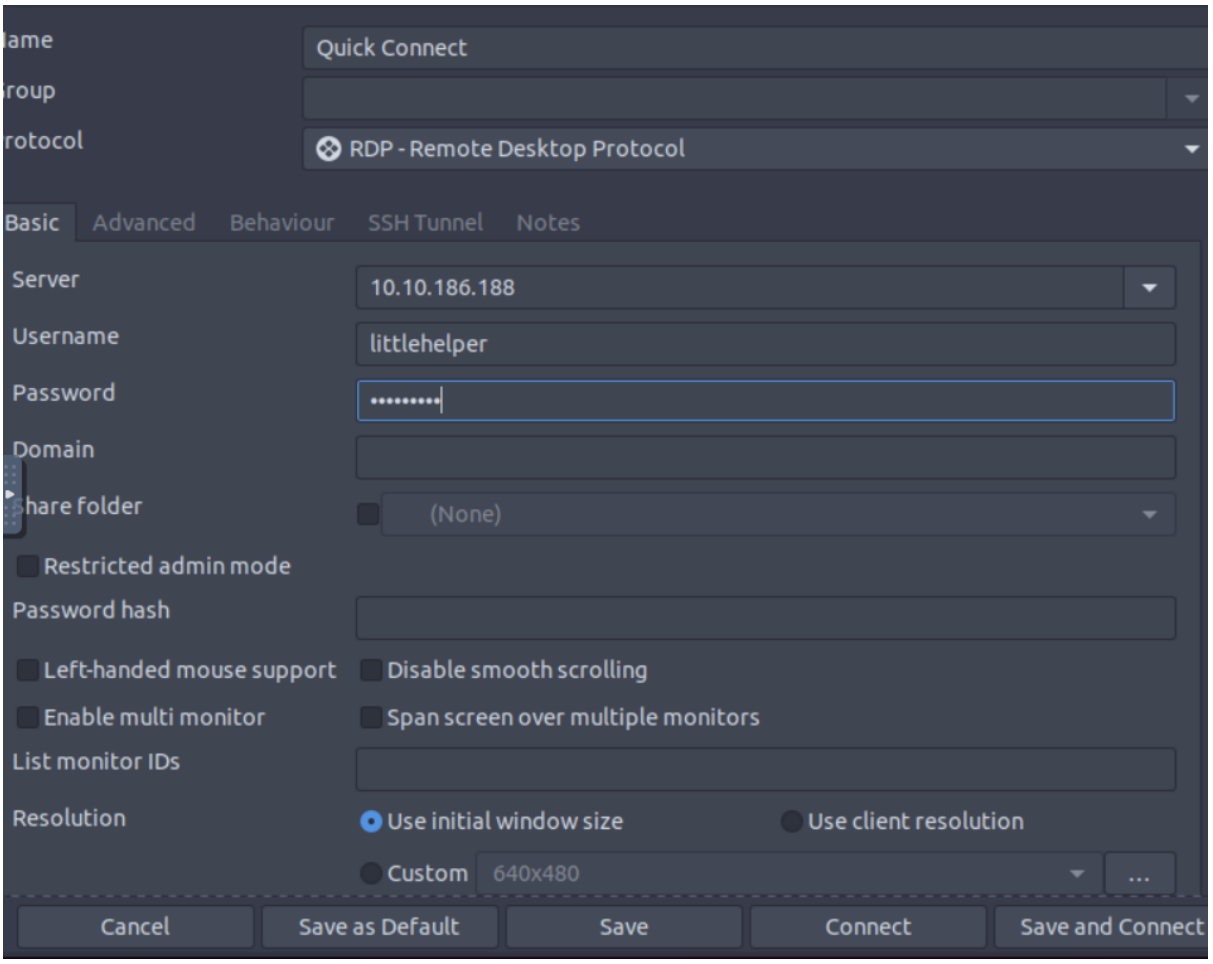
Tool used : Attackbox, Remmina

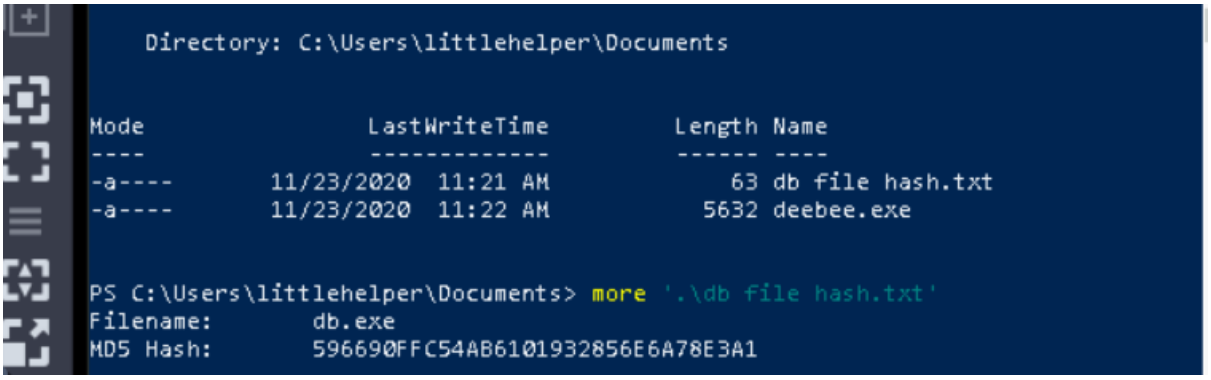
Solution / walkthrough :

<u>Question 1</u>

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

596690FFC54AB6101932856E6A78E3A1





Question 2

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

5F037501FB542AD2D9B06EB12AED09F0

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

Algorithm       Hash
---------       ----
MD5             5F037501FB542AD2D9B06EB12AED09F0


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

Question 3

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

F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED

```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm SHA256 .\deebee.exe

Algorithm       Hash
---------       ----
SHA256          F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED
```

Question 4

Using Strings find the hidden flag within the executable?

THM{f6187e6cbeb1214139ef313e108cb6f9}

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

```
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\littlehe
lper\Documents\db.exe).Path -ReadCount 0 -Encoding Byte) -Encoding Byte -Stream hi
dedb
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
z\V
WrapNonExceptionThrows
deebee
Copyright
```

Question 5

What is the powershell command used to view ADS?

Get-Item -Path file.exe -Stream *

The command to view ADS using Powershell:

```
Get-Item -Path file.exe -Stream *
```

Question 6

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

THM{088731ddc7b9fdeccaed982b07c297c}

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


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

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

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option:
```

Question 7

Which list is Sharika Spooner on?

Naughty List

```
C:\Users\littlehelper\Documents\deebee.exe:hidedb
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: 2
```

```
Jovan Hullett
Sherlene Loehr
Melisa Vanhoose
Sharika Spooner

Sucks for them .. Returning to the User Menu...
```

Question 8

Which list is Jaime Victoria on?

Nice List

```
C:\Users\littlehelper\Documents\deebee.exe:hidedb
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: 1
```

```
Frances Merkle
Thomasena Latimore
Laurena Gardea
Delphine Gossard
Jaime Victoria

Awesome .. Great! Returning to the User Menu...
```

Methodology : we booted up our target machine. We used remmina to connect to the machine with littlehelper and iLove5now! as the username and password. We started a Powershell and got into Documents directory with Set-Location.\Documents\. And list the contents with ls. To read the contents of the text time we used Get-Content '.\db file hash.txt' and the hash was revealed. To find the hash of the executable file, we used Get-FileHash -Algorithm MD5 .\deebee.exe. The SHA256 file hash of the mysterious executable within the Documents folder was revealed with Get-FileHash -Algorithm SHA256 .\deebee.exe. We used the strings command in order to find the hidden file. We used the C:\Tools\strings64.exe -accepteula .\deebee.exe and we found our flag as we scrolled down. The powershell that we used to view ADS was Get-Item -Path deebee.exe -Stream *. We ran the executable from this stream with the command wmic process call create $(Resolve-Path ./deebee.exe:hidedb) and the flag would be visible. We ran the program and found out that Sharika Spooner is on the Naughty list and Jaime Victoria is on the Nice list.

Day 22: Blue teaming - Elf McEager becomes Cyberelf

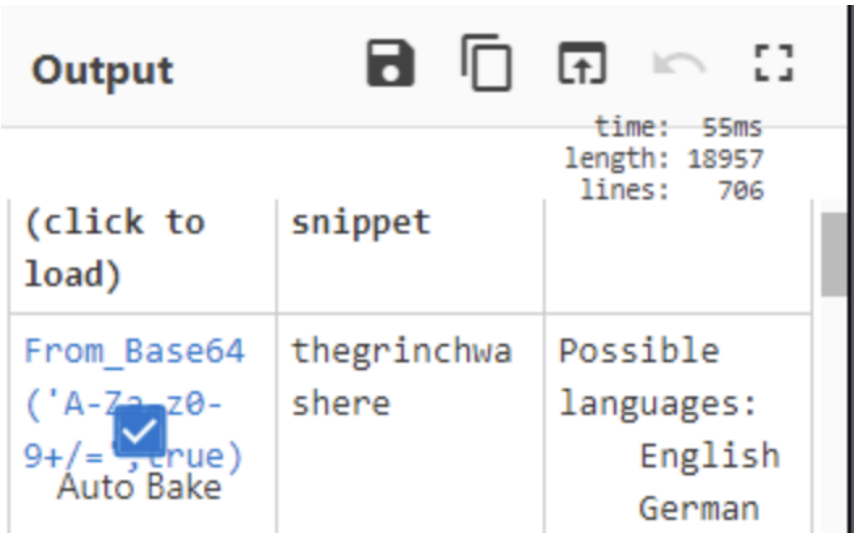
Tools used: Attackbox, Firefox, Remmina, Cyberchef

Solution:

Question 1

What is the password to the KeePass database?

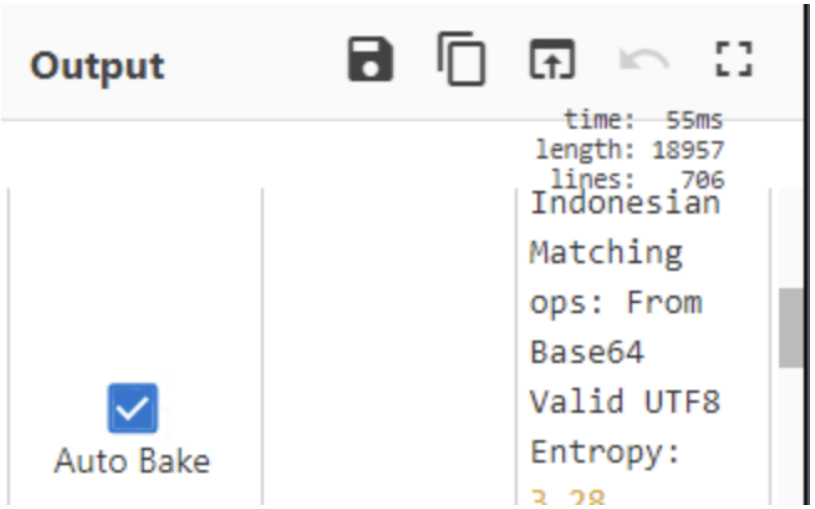
We used cyberchef to decode the name of the folder which was an encrypted value. We found out that the master password was **thegrinchwashere.**



Question 2

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

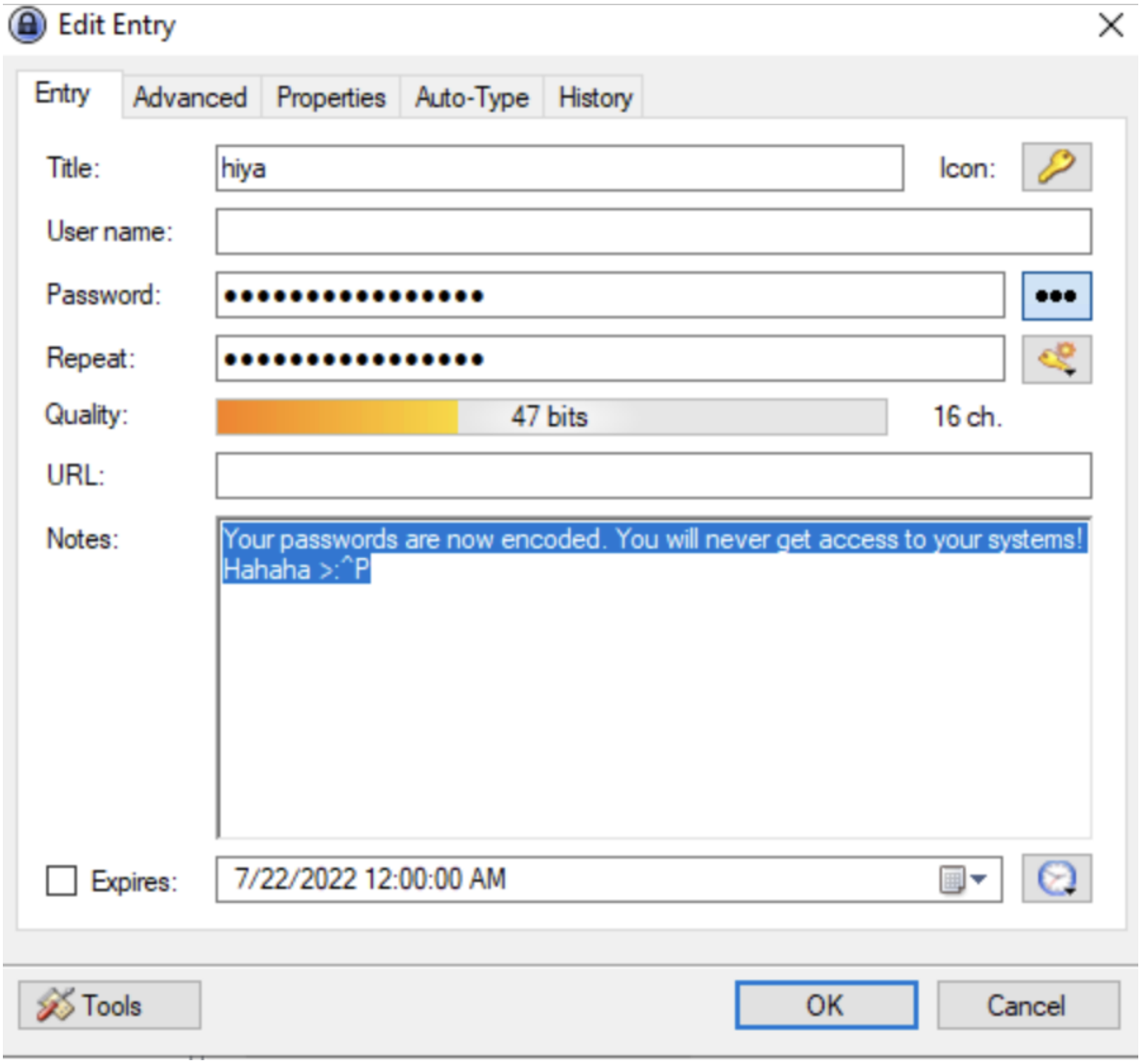
The encoding method was **base64**.



Question 3

What is the note on the hiya key?

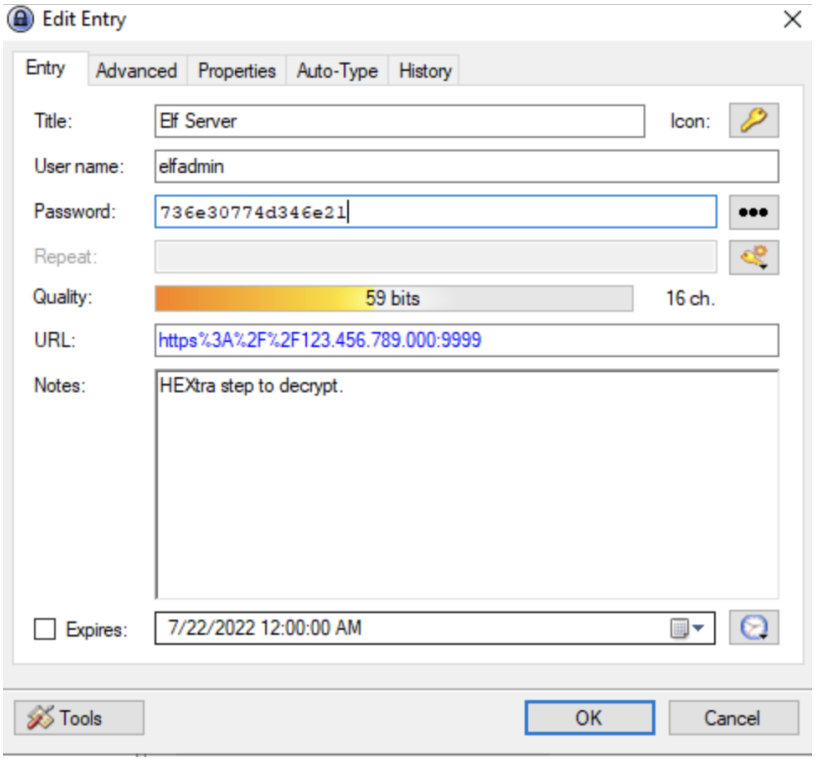
Revealed on the hiya key was the following message "**Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P**"

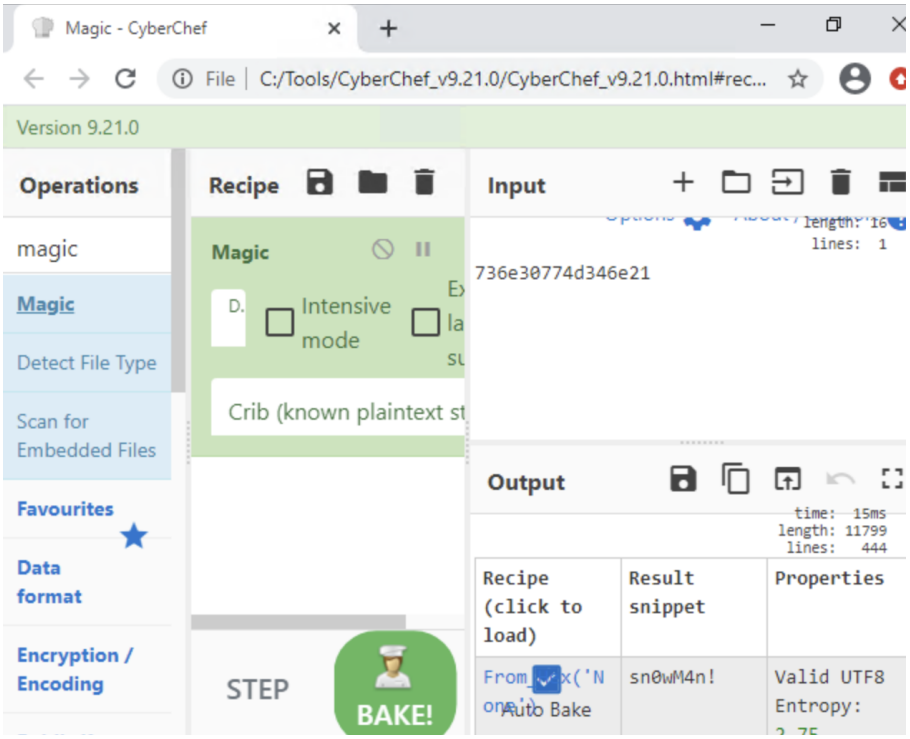


Question 4

What is the decoded password value of the Elf Server?

We'll use cyberchef to decrypt the password of the Elf server. The password is **sn0wM4n!**

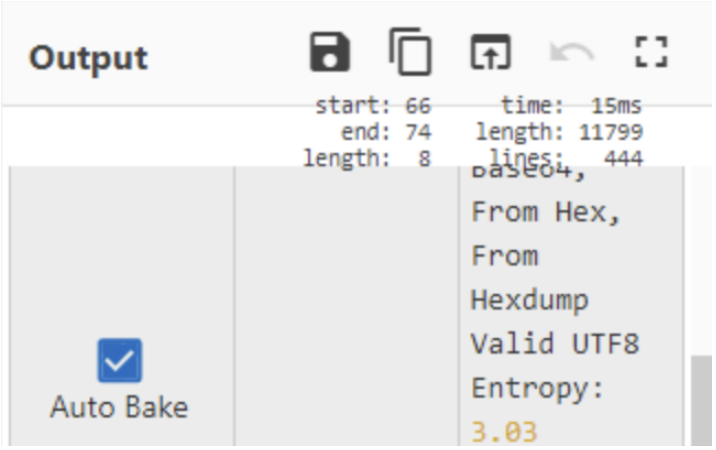




<u>Question 5</u>

What was the encoding used on the Elf Server password?

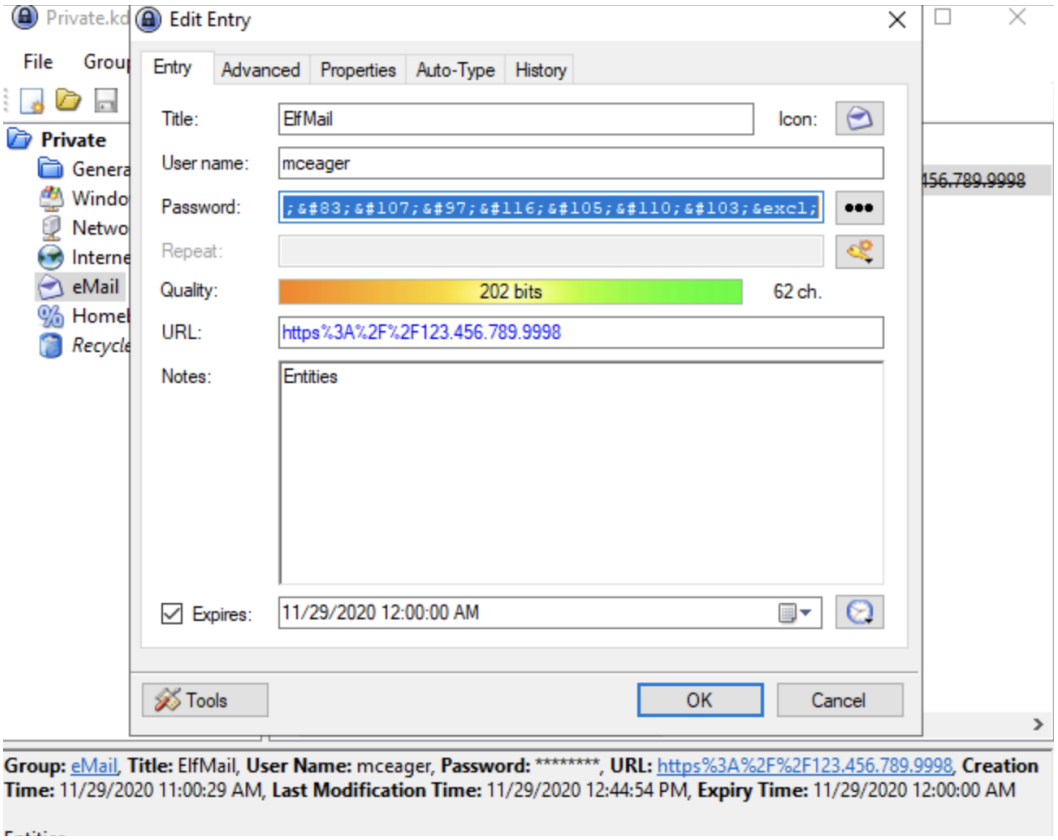
The encoding is **hex** based on the hint in the notes of the elf server as well as the matching ops stated by cyberchef.

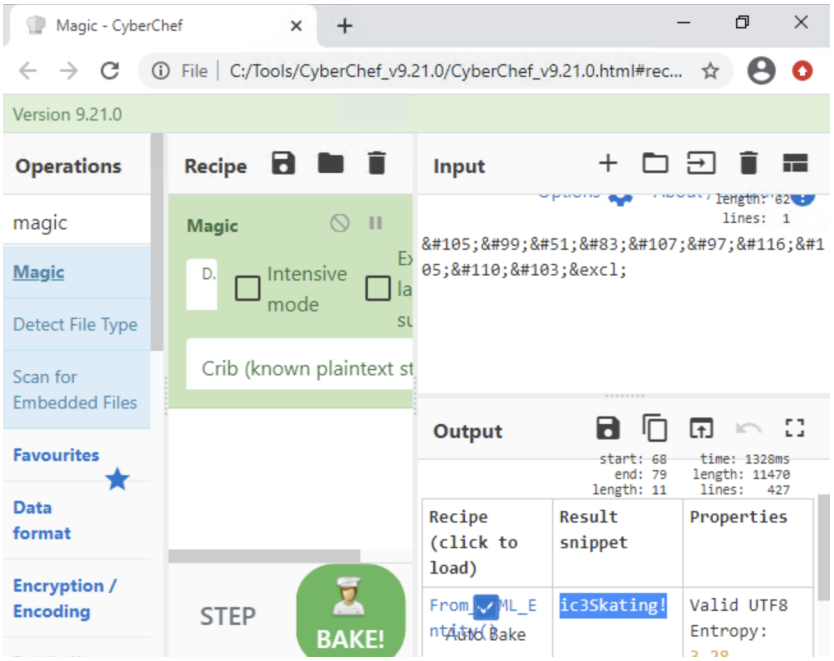


Question 6

What is the decoded password value for ElfMail?

Using cyberchef once again we were able to uncover the password using HTML entity decoding which we knew from the hint left by the note in the entry. The password is **ic3Skating!**.

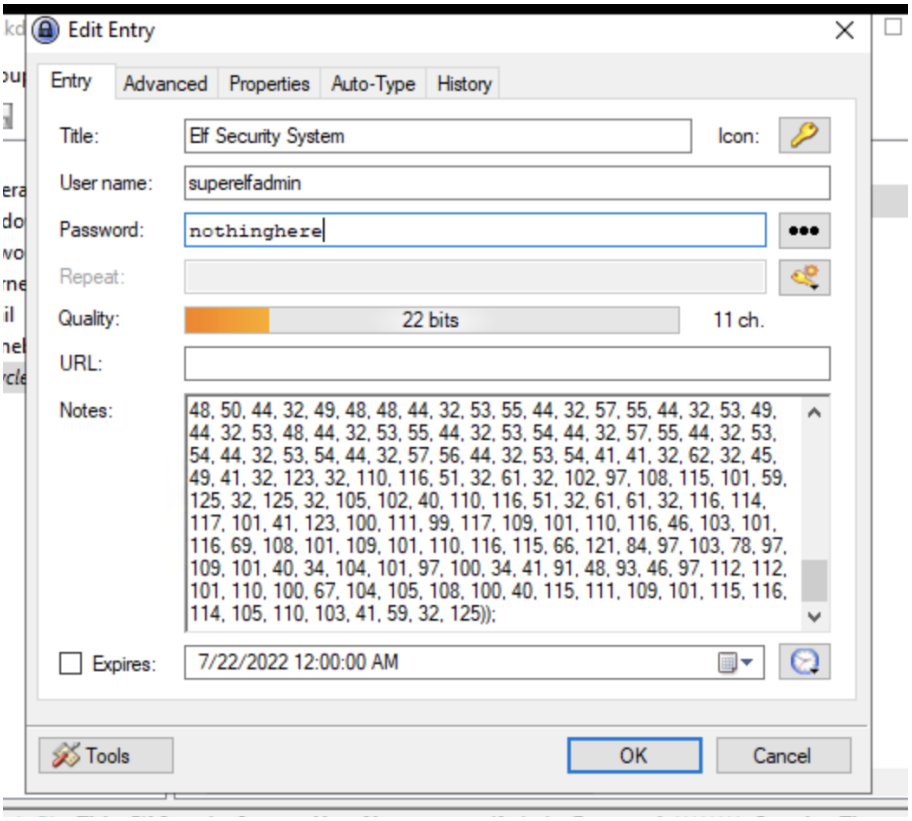




Question 7

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

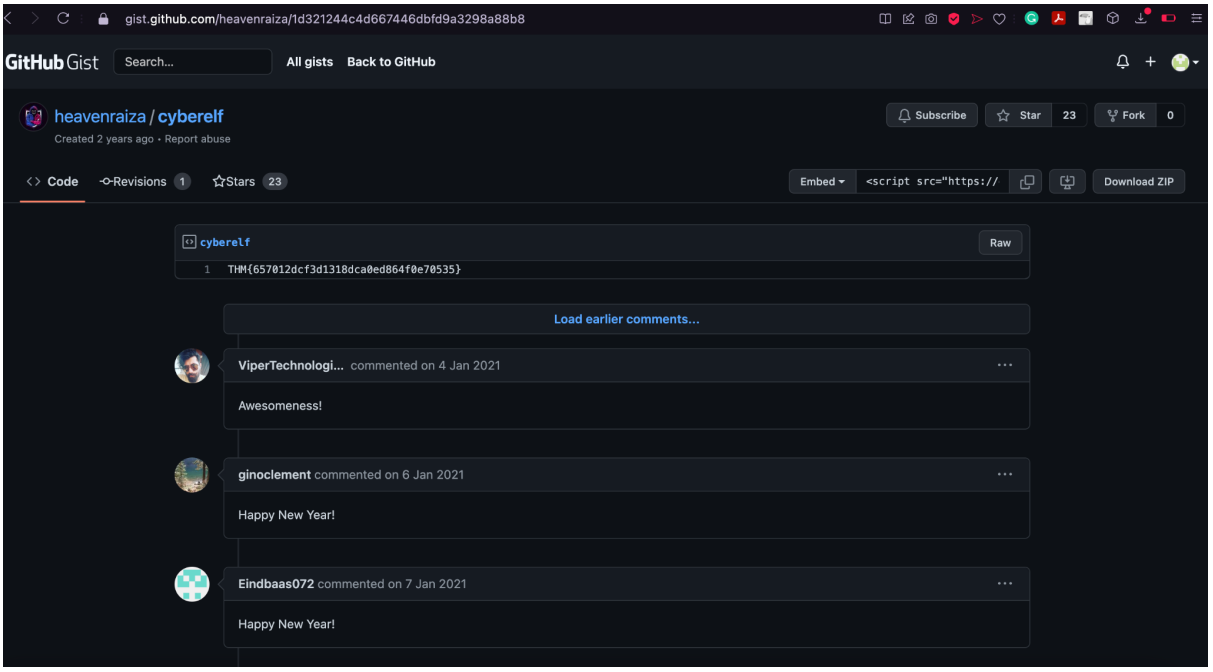
Viewing the entry we can see **superelfadmin:nothinghere**



Question 8

Decode the last encoded value. What is the flag?

We decrypt the code from the note of the entry of Elf Security System using character encoding with the delimiter set to comma and base 10. We repeat the procedure one more time and it revealed a link. When opening the link on the browser we were revealed the flag. `THM{657012dcf3d1318dca0ed864f0e70535}`



Methodology: We startup Remina and entered the proper information such as server, user name and password. Once the remote system is completely set up and booted we accessed a file with a random or abnormal name on the desktop. The folder seems to contain an app or programme called Keepass which we ran. We were prompted to enter the master key. We entered the master password **mceagerrockstar** but it failed. We investigated that the folder was oddly named with a cryptic value which was “dGhlZ3JpbmNod2FzaGVyZQ==” thus we speculated that it is encrypted. We grab the name of the folder and used cyberchef to decrypt or decode the value using the **magic** function. The decoded value was *thegrinchwashere*. We were able to gain access successfully. We looked through the tabs in Keepass and found elf server under the network’s tab. The password is apparently encrypted. Again we’ll use cyberchef to decrypt it. We gained the password which was *sn0wM4n!*. We then inspect the email option which contained ElfMail. The password for that was also encrypted. The entry also left us a note saying entity. We did some deductive work and found out that entity refers to HTML entity. The password was decrypted to be *ic3Skating!*. Next in the recycle bins tab, we found another entry

named Elf Security System. A note was left there and what seems to look like a javascript code. We try to avoid running this code for security reasons. Using character code encoding, we tried to decrypt this note. It returned us a github link which contains the flag.

Day 23 - [Blue Teaming] The Grinch strikes again!

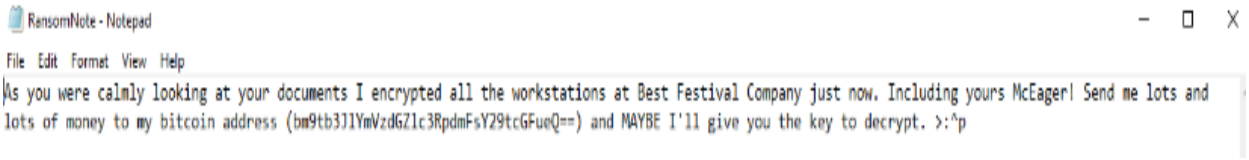
Tool used : Attackbox, Remmina, Google, Windows Task Scheduler

Solution / walkthrough :

Question 1

What does the wallpaper say?

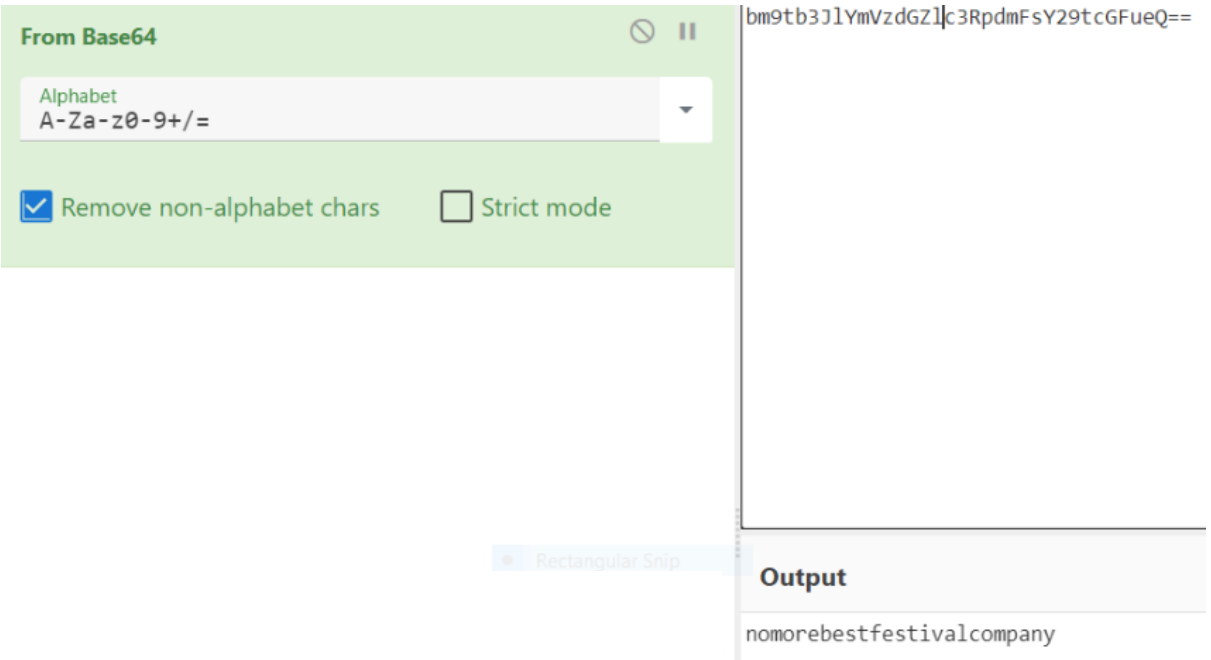
When we open the RDP connection, we can see a wallpaper that says ‘THIS IS FINE’ and a RansomeNote text document.



Question 2

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

We opened the ransom note located on the Desktop. According to the attacker, if we send him/her a large amount of bitcoin, he/she will give us the decryption key. However, the bitcoin’s address was a bit weird. It appears to be a base64-encoded fake address. We attempted to unravel it. Then we found out that it is indeed a fake address and it is Base64 encoding. The value we used was **bm9tb3JlYmVzdGZlc3RpdmFsY23tcGFueQ==** and the output was **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?

We looked in the Documents directory. There was a file named “master-password.txt**.grinch**”

Question 4

What is the name of the suspicious scheduled task?

There was some strange activity named “**opidsfsdf**” when we used the Task Scheduler app on Windows where you can schedule an activity. We opened the scheduled activity on the system and saw the suspicious scheduled task.

Question 5

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

By running an executable at that task, the activity will trigger an action to be taken at **C:\User\Administrator\Desktop\opidsfsdf.exe**

Question 6

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

There was another task scheduled named “ShadowCopyVolume”. We clicked on the task > actions tab > properties. The ID was in the “Add arguments”.
7a9eea15-0000-0000-0000-010000000000.

Question 7

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

The hidden folder name was “**confidential**”. We saw the partitions that are available in the system by opening the disk management. In addition to the C: partition, there is another one called Backup that is 1 GB in size. To use it, we must first give the Backup partition a letter, launch file manager, and list everything inside.

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?

Database and vStocking are the two folders found in Backup. We clicked the View Tab on the Windows file manager. Then, we checked the Hidden Items on Shows/hide section. Furthermore, there were 2 files ‘master-password.txt’ and ‘master-password.txt.grinch’ in the

“confidential” directory. The file before the ransom encryption is the non ‘.grinch’ file.,thus we can access the file. The password is **‘m33pa55w0rdlZseecure!’**.

Methodology: When we open the RDP connection, we can see a wallpaper that says ‘THIS IS FINE’ and a RansomeNote text document. Then, we opened the ransom note located on the Desktop. According to the attacker, if we send him/her a large amount of bitcoin, he/she will give us the decryption key. However, the bitcoin’s address was a bit weird. It appears to be a base64-encoded fake address. We attempted to unravel it. Then we found out that it is indeed a fake address and it is Base64 encoding. The value we used was **bm9tb3JlYmVzdGZlc3RpdmFsY23tcGFueQ==** and the output was **nomorebestfestivalcompany**. Next, we looked in the Documents directory. There was a file named “master-password.txt**.grinch”**. There was some strange activity named “**opidsfsdf**” when we used the Task Scheduler app on Windows where you can schedule an activity. We opened the scheduled activity on the system and saw the suspicious scheduled task. By running an executable at that task, the activity will trigger an action to be taken at **C:\User\Administrator\Desktop\opidsfsdf.exe.** There was another task scheduled named “ShadowCopyVolume”. We clicked on the task > actions tab > properties. The ID was in the “Add arguments”. **7a9eea15-0000-0000-0000-010000000000.** The hidden folder name was “**confidential**”. We saw the partitions that are available in the system by opening the disk management. In addition to the C: partition, there is another one called Backup that is 1 GB in size. To use it, we must first give the Backup partition a letter, launch file manager, and list everything inside. Finally, Database and vStocking are the two folders found in Backup. We clicked the View Tab on the Windows file manager. Then, we checked the Hidden Items on Shows/hide section. Furthermore, there were 2 files ‘master-password.txt’ and ‘master-password.txt.grinch’ in the “confidential” directory. The file before the ransom encryption is the non ‘.grinch’ file.,thus we can access the file. The password is **‘m33pa55w0rdlZseecure!’**.

Day 24 - [Final Challenge] The Trial Before Christmas

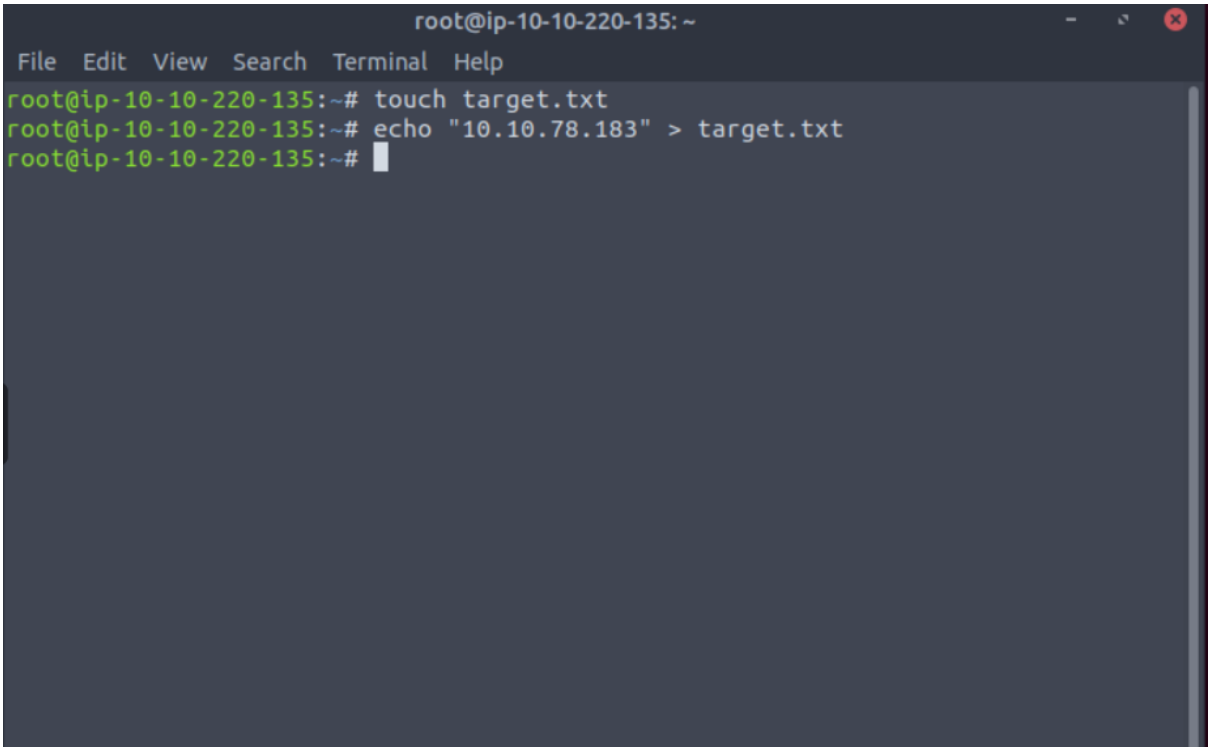
Tool used : attackbox

Solution/walkthrough :

<u>Question 1</u>

Scan the machine. What ports are open?

80, 65000



```
root@ip-10-10-220-135: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-220-135:~# cat target.txt
10.10.78.183
root@ip-10-10-220-135:~# nmap -p- -sCV -iL target.txt

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-21 04:47 BST
```

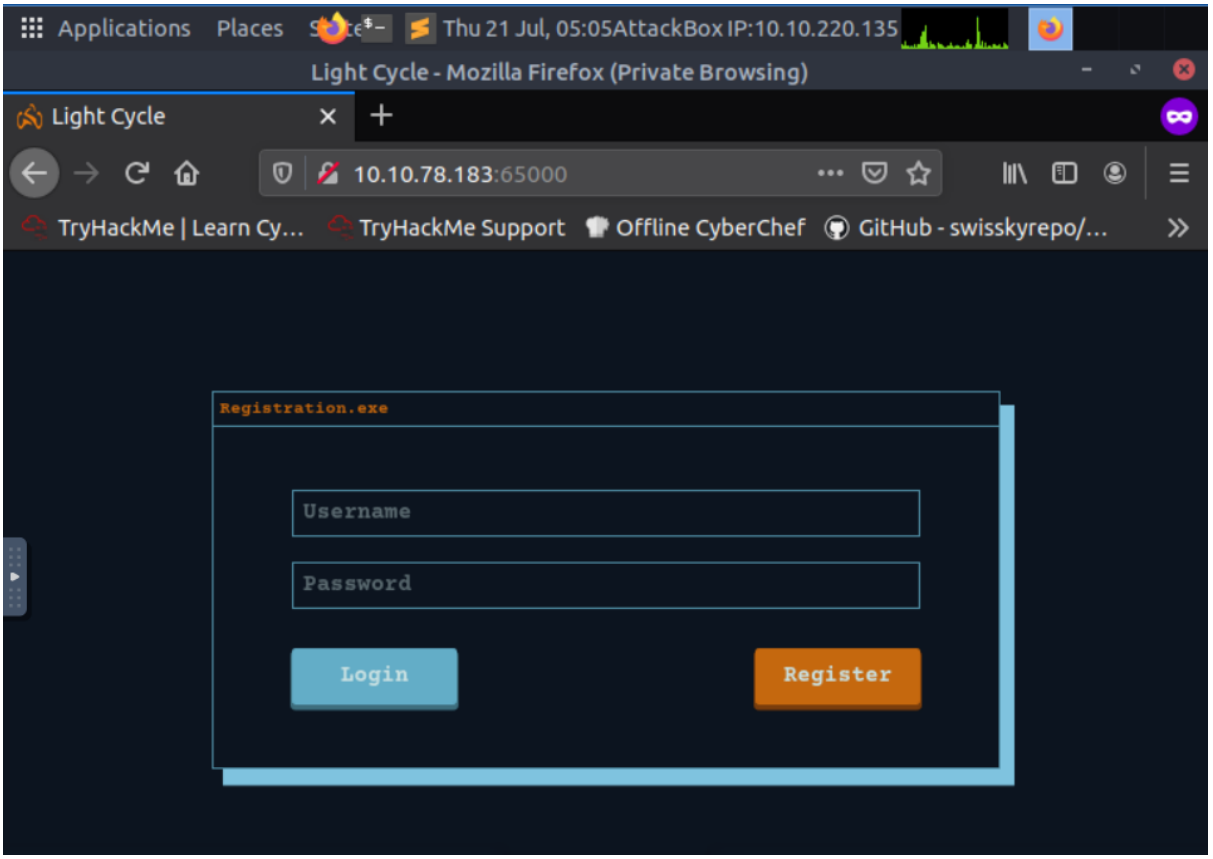
```
SYN Stealth Scan Timing: About 99.99% done; ETC: 05:00 (0:00:00 remaining)
Nmap scan report for ip-10-10-78-183.eu-west-1.compute.internal (10.10.78.183)
Host is up (0.00035s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
80/tcp    open  http
65000/tcp open  unknown
MAC Address: 02:A1:9E:F5:29:3D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 617.29 seconds
root@ip-10-10-220-135:~#
```

Question 2

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

Light Cycle



Question 3

What is the name of the hidden php page?

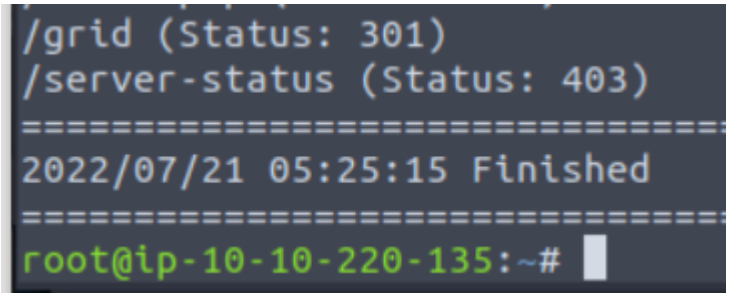
/uploads.php

```
===============================================================
2022/07/21 05:24:21 Starting gobuster
===============================================================
/uploads.php (Status: 200)
/assets (Status: 301)
/api (Status: 301)
/index.php (Status: 200)
/grid (Status: 301)
/server-status (Status: 403)
===============================================================
2022/07/21 05:25:15 Finished
===============================================================
root@ip-10-10-220-135:~#
```

Question 4

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

/grid



Question 5

What is the value of the web.txt flag?

THM{ENTER_THE_GRID}

Question 6

What lines are used to upgrade and stabilize your shell?

export TERM=xterm, python3 -c 'import pty;pty.spawn("/bin/bash")' and stty raw -echo; fg

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.

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**

tron:IFightForTheUsers

```
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($dbh->connect_error);
        }
?>
www-data@light-cycle:/var/www/TheGrid/includes$
```

Question 8

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

tron

```
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 |
+----+----------+----------------------------------+
```

Question 9

Crack the password. What is it?

@computer@

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

Free Password Hash Cracker

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

```
edc621628f6d19a13a00fd683f5e3ff7
```

I'm not a robot

reCAPTCHA
Privacy - Terms

Crack Hashes

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.

Question 10

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

flynn@light-cycle

```
flynn@light-cycle:
id
```

Question 11

What is the value of the user.txt flag?

THM{IDENTITY_DISC_RECOGNISED}

```
-r-------- 1 flynn flynn 30 Dec 19 16:42 user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
```

Question 12

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

lxd

```
flynn@light-cycle:~$ groups
flynn lxd
flynn@light-cycle:~$
```

Question 13

What is the value of the root.txt flag?

THM{FLYNN_LIVES}

```
total 4
-r--------    1 root     root           600 Dec 19 20:18 root.txt
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}
```

Methodology : To find out which ports are open, we used nmap to perform a scan. We discover that ports 80 and 65000 are open after doing a scan. We went to the web server at port 65000. When we arrive at the page, we notice a website called Light Cycle with the option to sign up or log in. To identify a hidden php file's name. Gobuster can help us accomplish this. We found a file named uploads.php after running this. The uploaded files are kept in a directory with the name "/grid," which is also visible. We used Burp Suite to get beyond the front end filter that limits the kind of files that may be submitted. Burp Suite should now be open. We went to the Proxy -> Options page. Intercept Client Requests' top line can be clicked, and then we can choose Edit. We removed js from the match condition once the menu had opened. We made sure Intercept requests based on the following rules were selected before closing this option. We forwarded requests in Burp Suite until we reached one with the /assets/js/filter.js URL. We started a netcat listener and navigated to the /grid directory. When we opened the file and went back to our netcat listener, our shell had started. We searched on /var/www/ directory. We accessed the contents with cat and the flag would be visible which is THM{ENTER_THE_GRID}. Lines we used to stabilise our shell are export TERM=xterm, python3 -c 'import pty;pty.spawn("/bin/bash")' and stty raw -echo; fg. We looked for a username and password combination in /var/www/TheGrid/includes/. We looked at dbauth.php and saw a database login with the username and password. We accessed the MySQL with the login information and entered the command mysql -utron -p and entered the password. After we entered MySQL, we used the command SHOW DATABASES and we saw a database named tron. The tron command can be used to choose the tron database, and the SELECT * FROM users command can be used to list the users table's contents. When we do this, two users' encrypted passwords are displayed. We cracked Flynn's password using https://crackstation.net/ and the password @computer@. The user we were switching to is flynn@light-cycle. We can use su to log in as Flynn now that we have his password. Now that we have access to Flynn's home directory, we can examine the information on the flag. Using cat, we can observe that the flag is THM.{IDENTITY DISC RECOGNISED}. Flynn is a member of the group lxd, which can be found by using the groups command. Because of a known vulnerability in lxd, we can build a root shell to see flag THM{FLYNN_LIVES}