

# PSP0201

## Week 6

# Writeup

GROUP NAME:Caustic Daddy

ID	NAME	ROLE
1211101658	Avinnaesh A/L G Baramesvaran	Member
1211103400	Rohit	Member
1211101977	ARVIND A/L KRISHNA KUMAR	Member
1211101778	Nevendra	Member

**DAY 21- Time for some elfforencics**

Tools used: Linux, Remmina

### Question 1

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

### Question 2

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

### Question 3

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

### Question 4

```
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
```

### Question 5

```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path .\deeb  
bee.exe:hidedb)
```

### Question 6

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

Choose an option:

- 1) Nice List
- 2) Naughty List
- 3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option:

### Question 7

```
Missy Stiner
Sanford Geesey
Jovan Hullett
letSherlene Loehr
Melisa Vanhoose
_PSharika Spooner
st
_
```

Thoughts: We used remmina to access the machine, then we used powershell to gain the hash and then we managed to recover the system.

## Day 22- Elf McEager becomes CyberElf

### Question 1

Output

time: 57ms  
length: 18957  
lines: 706

From\_Base6 thegrinchw Possible  
4('A-Z, ✓ ashere languages:  
z0- Auto Bake  
9+/' ,true English

### Question 3

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

### Question 4

Result snippet
sn0wM4n!
736e30774d346e21

### Question 5

HEXtra step to decrypt.

### Question 6

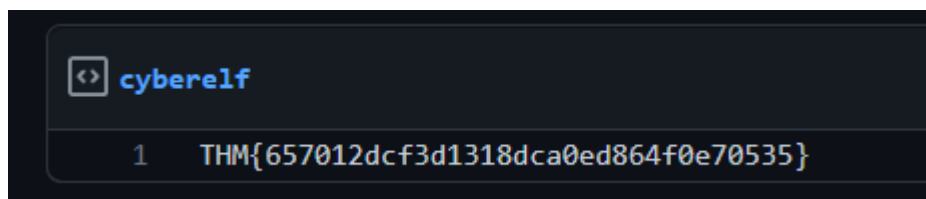
Recipe (click to load)	Result snippet	Properties
<code>From_HTML_Entity()</code>	<code>ic3Skating!</code>	Valid UTF8 Entropy: 3.28
	<code>&amp;#105;&amp;#99;&amp;#51;&amp;#83;&amp;#107;&amp;#97;&amp;#116;&amp;#105;&amp;#110;&amp;#103;&amp;excl;</code>	Matching ops: From Base85, From HTML Entity Valid UTF8 Entropy: 3.33

### Question 7

User name:

Password:

### Question 8

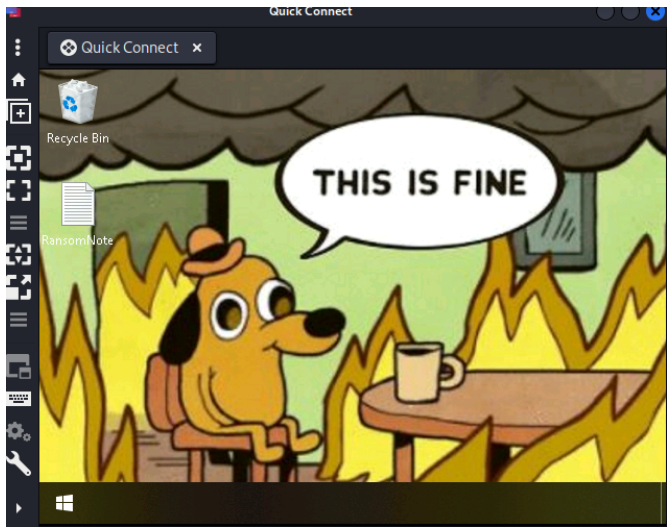


Thoughts: We accessed the machine and used remmina. Then we used cyberchef to decrypt the base 64 using cyberchef, and we decrypted every passwords using cyberchef.

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

**Tools Used: Linux, Remmina**

**Question 1**





**Question 2**




Recipe (click to load)	Result snippet	Properties
<code>From_Base64('A-Za-z0-9+/',true,false)</code>	<code>nomorebestfestivalcompany</code>	Possible languages: <ul style="list-style-type: none"><li>English</li><li>Spanish</li><li>Swedish</li><li>Danish</li><li>Slovak</li><li>Hungarian</li><li>Norwegian (Bokmål)</li><li>Norwegian (Nynorsk)</li><li>Catalan</li><li>French</li><li>Czech</li><li>...</li></ul>

**Question 3**

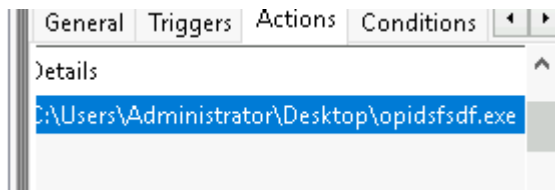
Name

-  elf1.txt.grinch
-  teeth.jpg.grinch

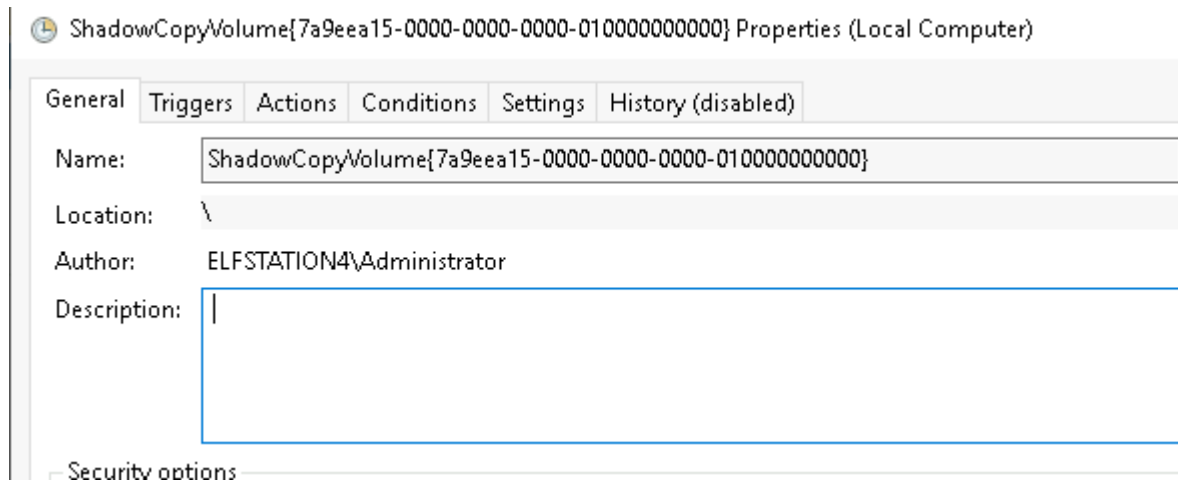
**Question 4**

Name	Status	Triggers
 GoogleUpda...	Disabled	At 5:05 AM every
 opidsfsdf	Ready	At log on of ELF
 ShadowCon	Ready	Multiple triggers

**Question 5**

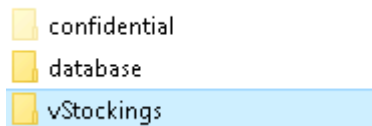


### Question 6

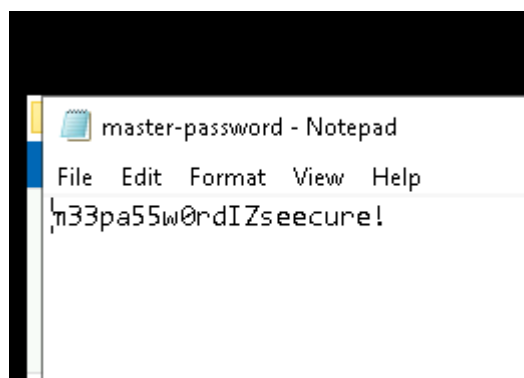


### Question 7

Name



### Question 8



### Thoughts:

We accessed the machine via remmina and used the scheduled task app to find the suspicious file and we used the view

button to see the confidential file,after that we restored the old file and got the password.

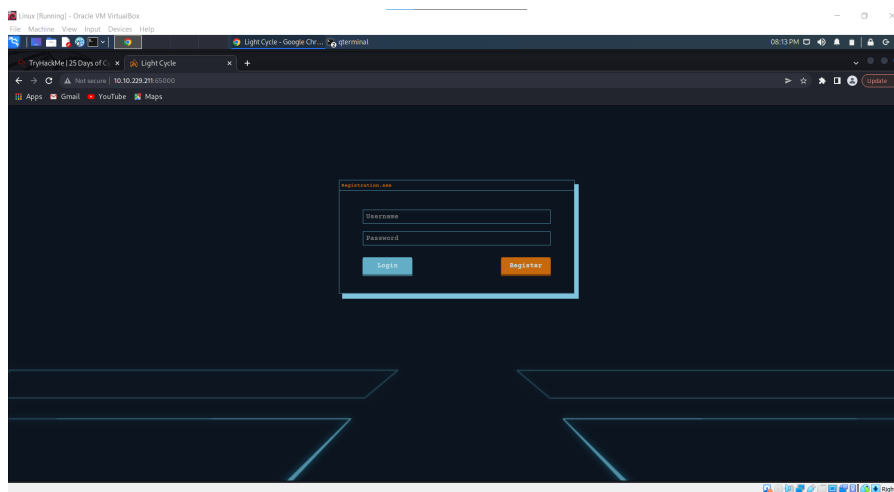
## Day 24 - [Final Challenge] The Trial Before Christmas

### Tools Used:Linux,Attackbox

### Question 1

```
PORT    STATE SERVICE
80/tcp  open  http
65000/tcp open  unknown
```

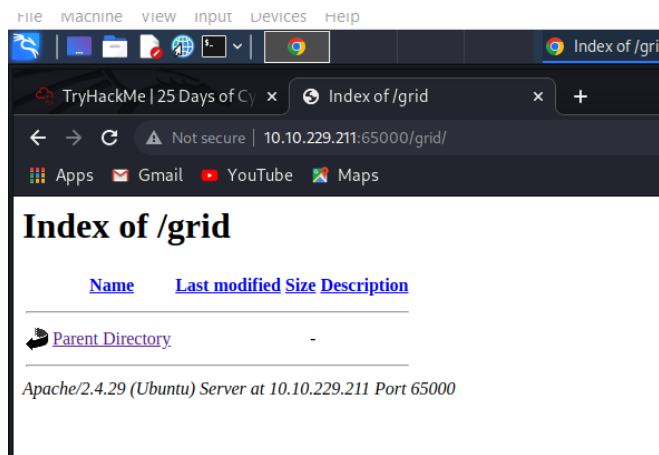
### Question 2



### Question 3



## Question 4



## Question 5

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

## Question 6

```
stty raw -echo; fg
```

## Question 7

```
$dbaddr = "localhost";  
$dbuser = "tron";  
$dbpass = "IFightForTheUsers";  
$database = "tron";
```

## Question 8

```
Database  
information_schema  
tron
```



id	username	password
1	flynn	edc621628f6d19a13a00fd683f5e3ff7

### Question 10

flynn
-------

```
flynn@light-cycle:~$ cat user.txt
cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ |
```

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

```
/mnt/root/root # cat root.txt  
cat root.txt  
THM{FLYNN_LIVES}
```

**Thoughts:** We accessed the machine, used nmap to find the ports and accessed the website, then we used burpsuite to intercept and we uploaded the reverse shell php file to the website and we used mysql to get the database.

