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
```

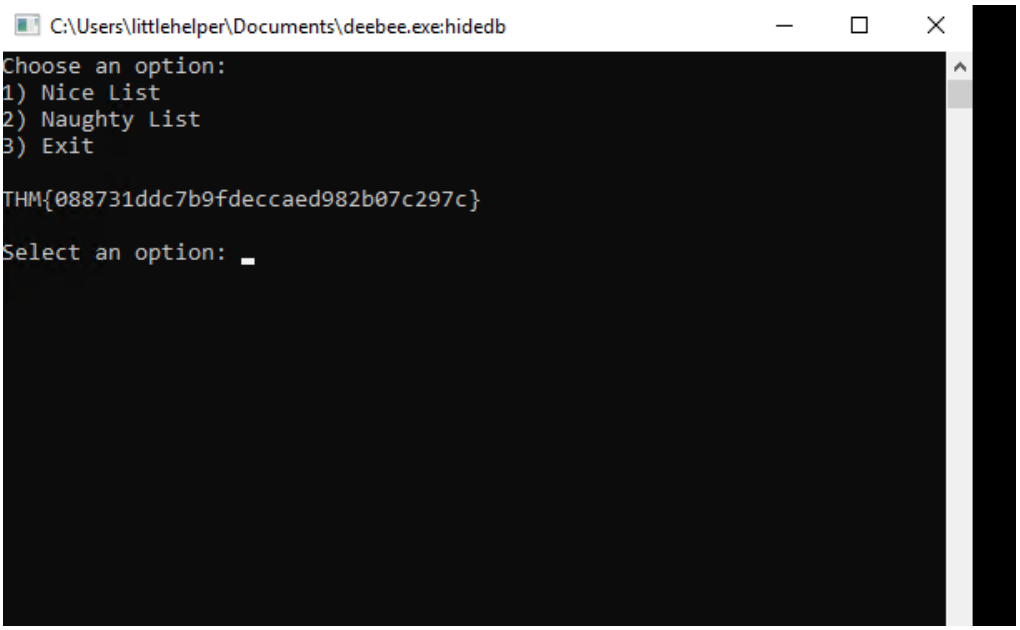
Question 4

```
THM{f6187e6cbeb1214139ef313e108cb6f9}
```

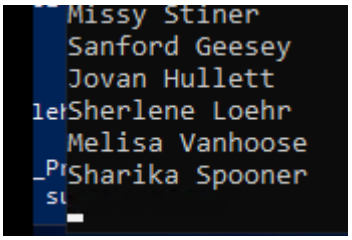
Question 5

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

Question 6



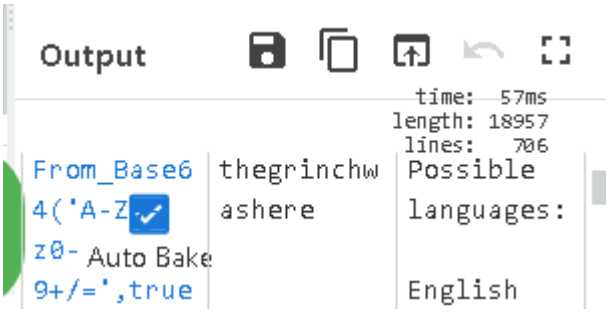
Question 7



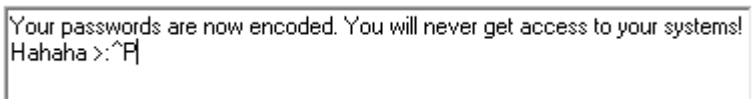
Thoughts: We used remmina to access the machine,then we used powershell to gain the hash and then we managed to recover the system.

Day 22- Elf McEager becomes CyberElf

Question 1



Question 3



Question 4

Result snippet
sn0wM4n!
736e30774d346e21

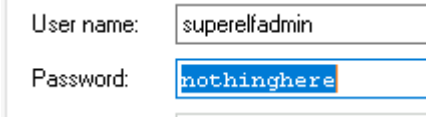
Question 5

HEXtra step to decrypt.

Question 6

Recipe (click to load)	Result snippet	Properties
From_HTML_Entity()	ic3Skating!	Valid UTF8 Entropy: 3.28
	ic3Skating!	Matching ops: From Base85, From HTML Entity Valid UTF8 Entropy: 3.33

Question 7



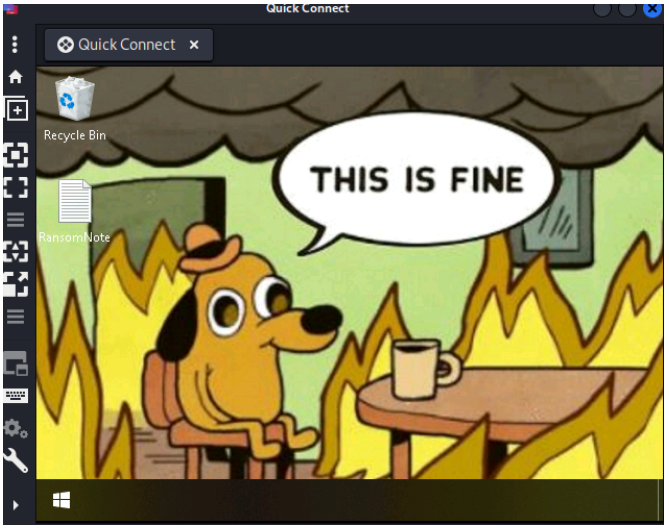
Question 8

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

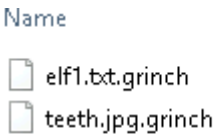
Question 1



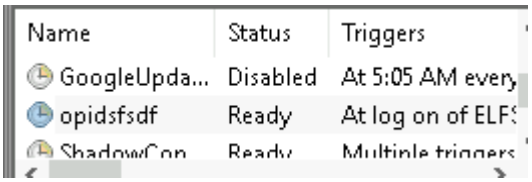
Question 2

Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/=',true,false)	nomorebestfestivalcompany	Possible languages: English Spanish Swedish Danish Slovak Hungarian Norwegian (Bokmål) Norwegian (Nynorsk) Catalan French Czech

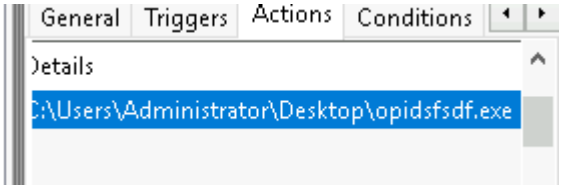
Question 3



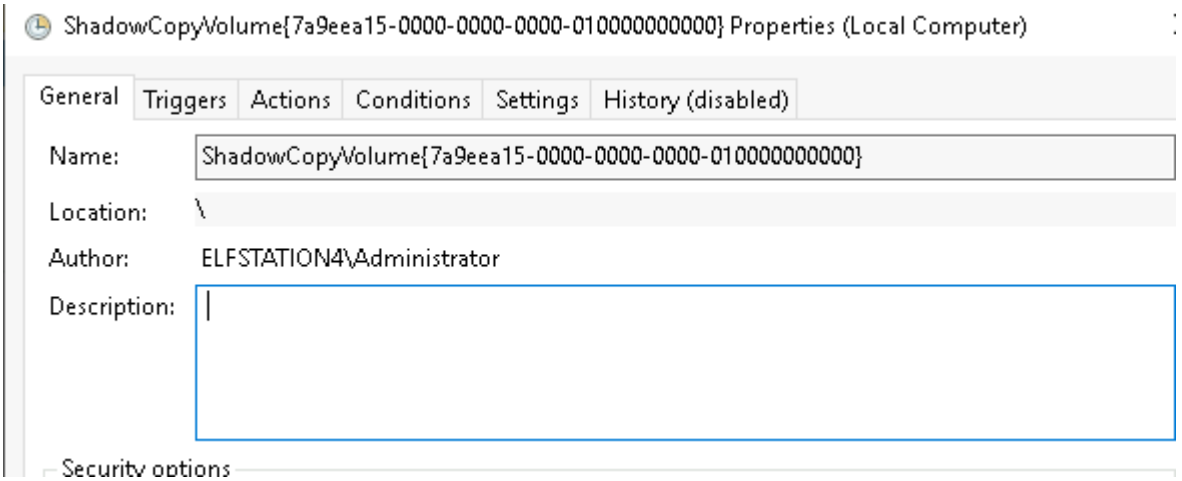
Question 4



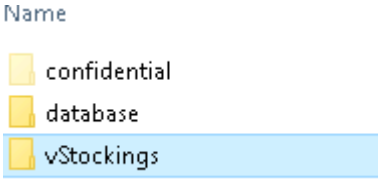
Question 5



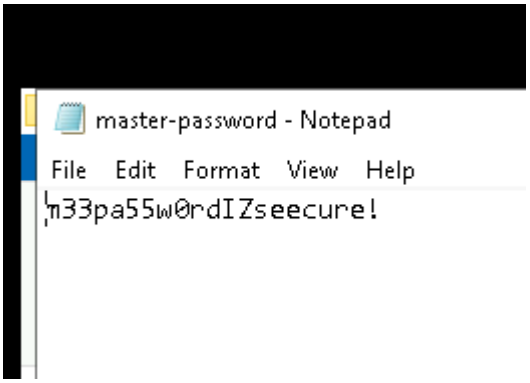
Question 6



Question 7



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

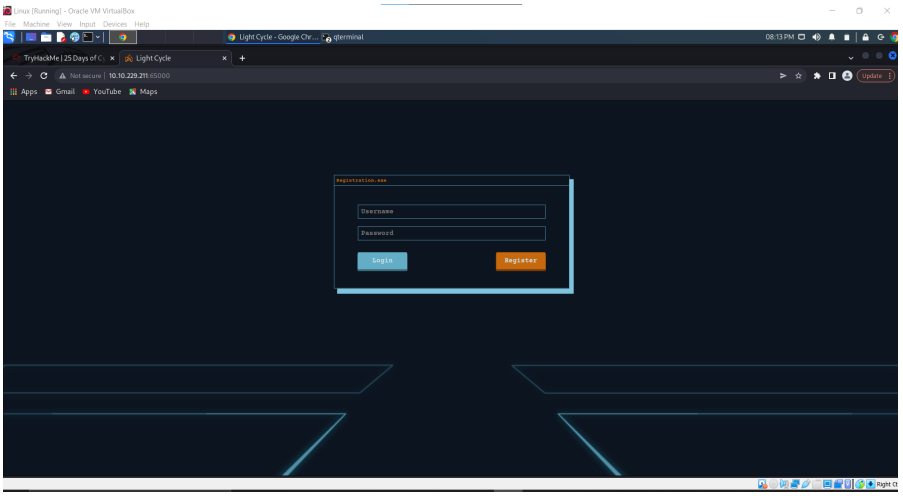
button to see the confidential file,after that we restored the old file and got the password.

Day 24 - [Final Challenge] The Trial Before Christmas
Tools Used:Linux,Attackbox

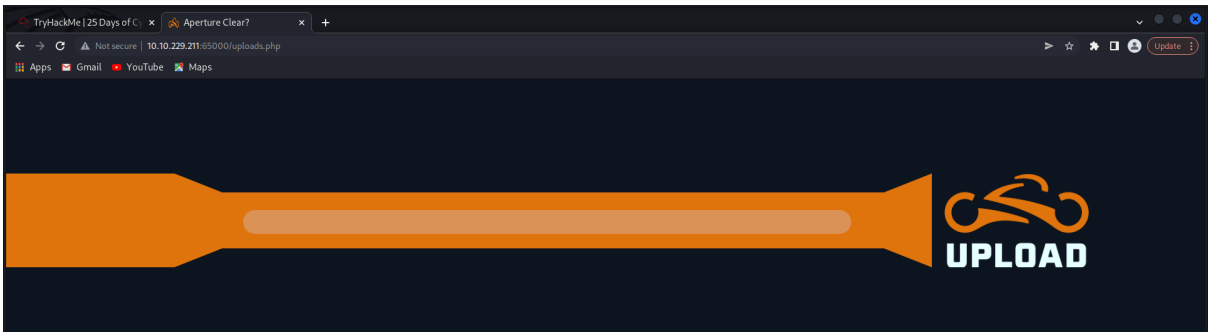
Question 1

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

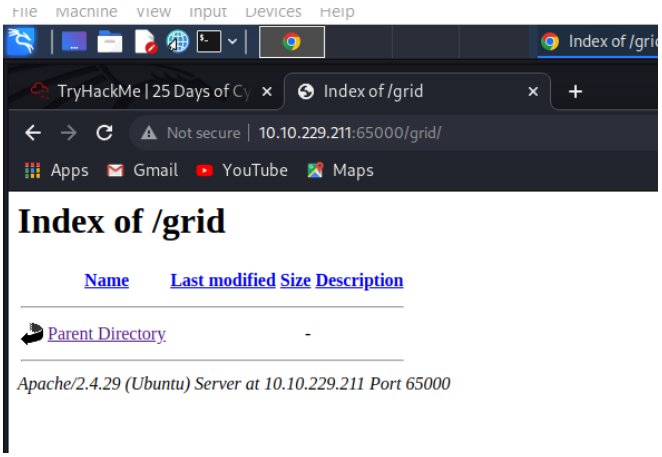
Question 2



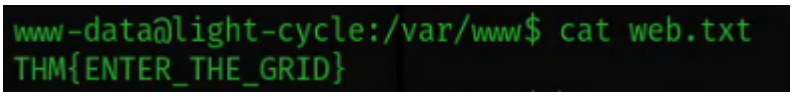
Question 3



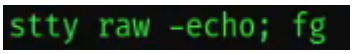
Question 4



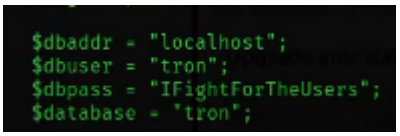
Question 5



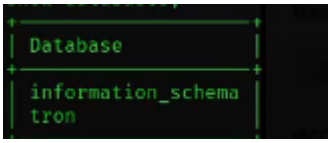
Question 6



Question 7

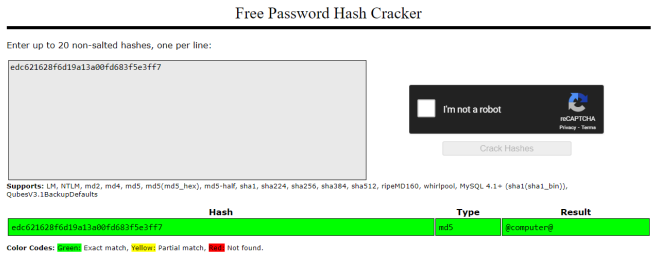


Question 8



Question 9

```
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
+----+----------+----------------------------------+
```



Question 10

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

Question 11

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

Question 12

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

Question 13

```
/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.