Faculty: Faculty of Computing & Informatics

Subject Code: PSP0201

Subject Name: MINI IT PROJECT

Section: TL7L

Assignment Name: Week 6 Tutorial Progress

Trimester: Trimester 3 2021/2022(T2120)

Lecturer: Mr Wong Ya Ping

STUDENT NAME	ID NUMBER
AZRYL SHAMIN BIN AZRIZAL	1211103145
TAN EASON	1211101844
JERRELL SU MING JIE	1211103690

Day 21: Blue Teaming – Time for some ELForensics

Tools used: Kali Linux, Firefox, Remmina

Solution/walkthrough:

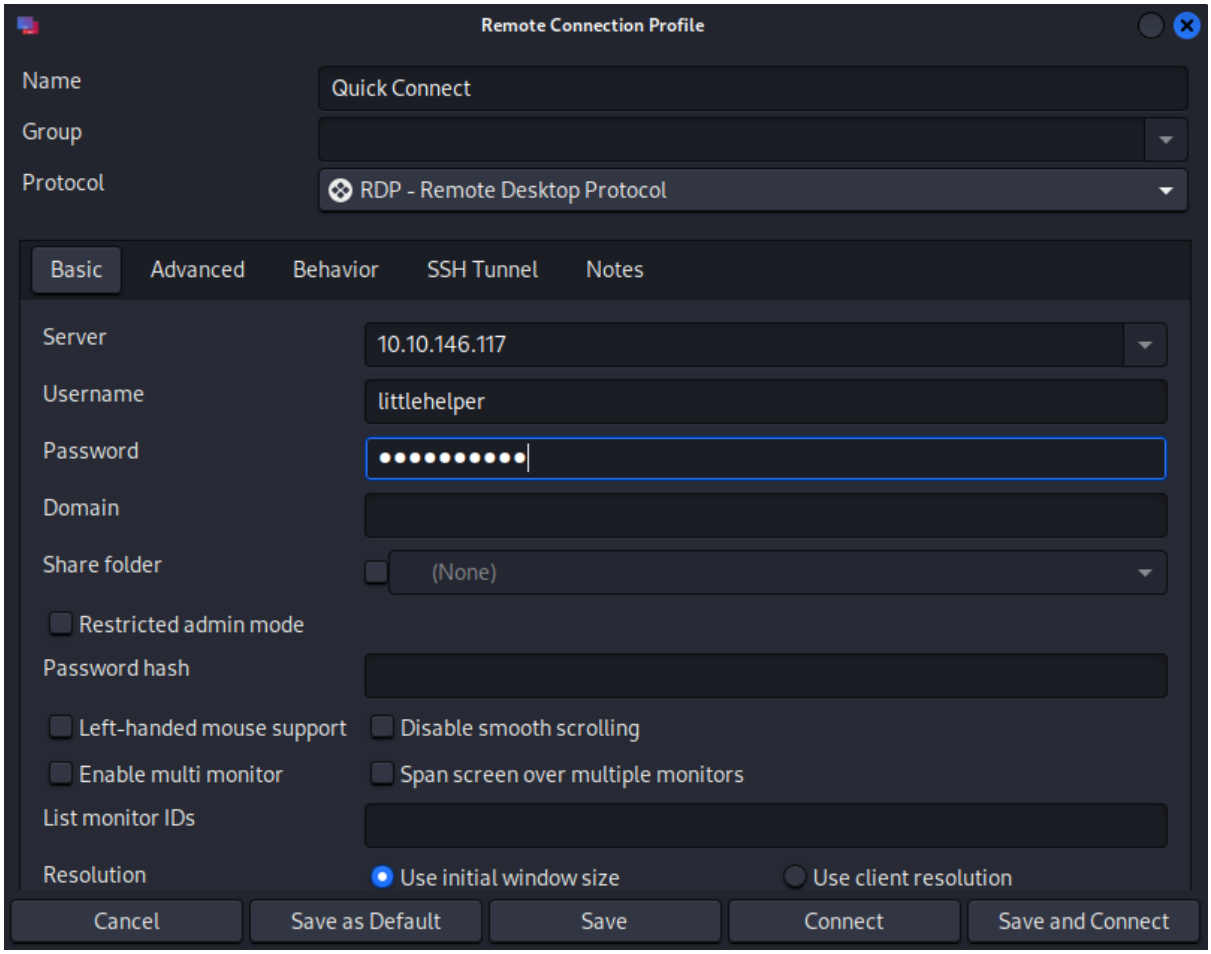
Question 1

We are provided with the credentials for the user account.

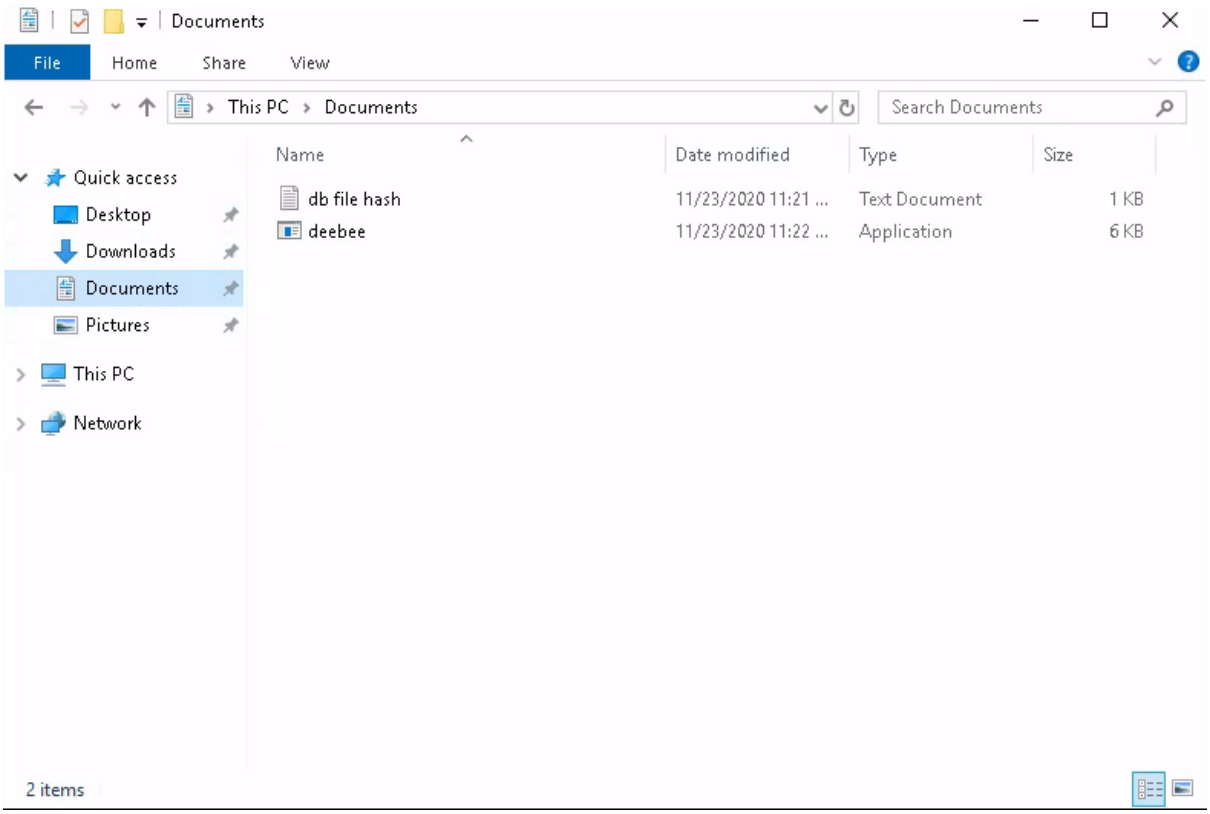
For **Server** provide (`MACHINE_IP`) as the IP address provided to you for the remote machine. The credentials for the user account is:

- User name: `littlehelper`
- User password: `iLove5now!`

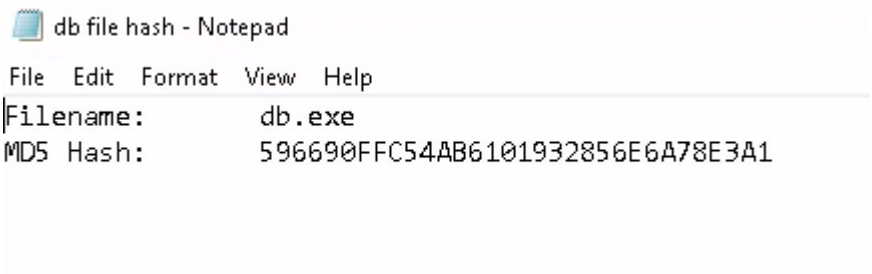
With that, we are setting up our remmina.



Once inside, we noticed it is a windows and we decided to look at the file on the machine. It turns out that the machine has 2 files (an executable and its file hash).



Once we open up the file hash we can see the file name of the executable and its original MD5 hash.



Question 2

In order to check whether the executable file is tampered or not, we decided to run a command to check its MD5 hash. It has different value than given in the hash file.

Question 3

We also check SHA256 type of hash using the command.

```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm SHA256 deebee.exe

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED       C:\Users\littlehelper\Documen...
```

Question 4

Next, we run a strings scan on the exe file.

```
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
```

The output shows the flag for today.

```
Accessing the Best Festival Company Database...
Done.
Using SSO to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\Documents
 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
```

Question 5

The instruction above gave us a command to run the hidden executable.

The command to run to launch the hidden executable hiding within ADS: `wmic process call create $(Resolve-Path file.exe:streamname)`

Note: You must replace **file.exe** with the actual name of the file which contains the ADS, and **streamname** is the actual name of the stream displayed in the output.

Question 6

We run the hidden executable by replacing some part with the information we get on the strings scan.

```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path .\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 3252;
        ReturnValue = 0;
};
```

The command opens up a terminal application which also contain the flag.

Question 7

Once we open the naughty list, **Sharika Spoon** is there.

Question 8

We also open the nice list and **Jamie Victoria** is on there.

Thought Process/Methodology:

We are provided with the credentials for the user account. With that, we are setting up our remmina. Once inside, we noticed it is on Windows and we decided to look at the file on the machine. It turns out that the machine has 2 files (an executable and its file hash). Once we open up the file hash, we can see the file name of the executable and its original MD5 hash. In order to check whether the executable file is tampered or not, we decided to run a command to check its MD5 hash. It has different value than given in the hash file. Next, we run a strings scan on the exe file. We run a command to open the hidden executable by replacing some part with the information we get on the strings scan. The command opens up a terminal application which also contain the flag.

Day 22: Blue Teaming – Elf McEager becomes CyberElf

Tools used: Kali Linux, Firefox, Remmina

Solution/walkthrough:

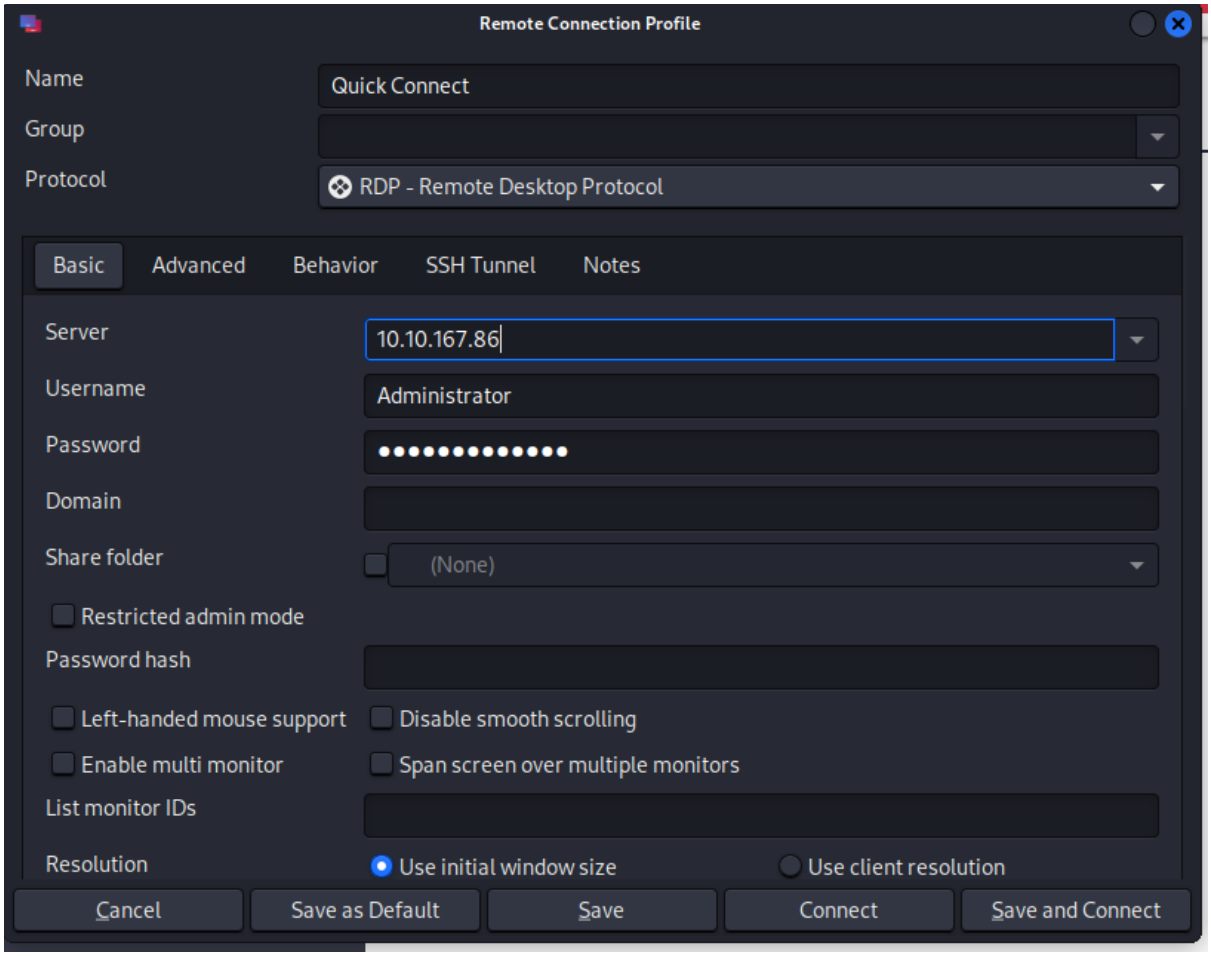
Question 1

When we started the task, we were given an IP address of a remote machine with the credentials for the user account.

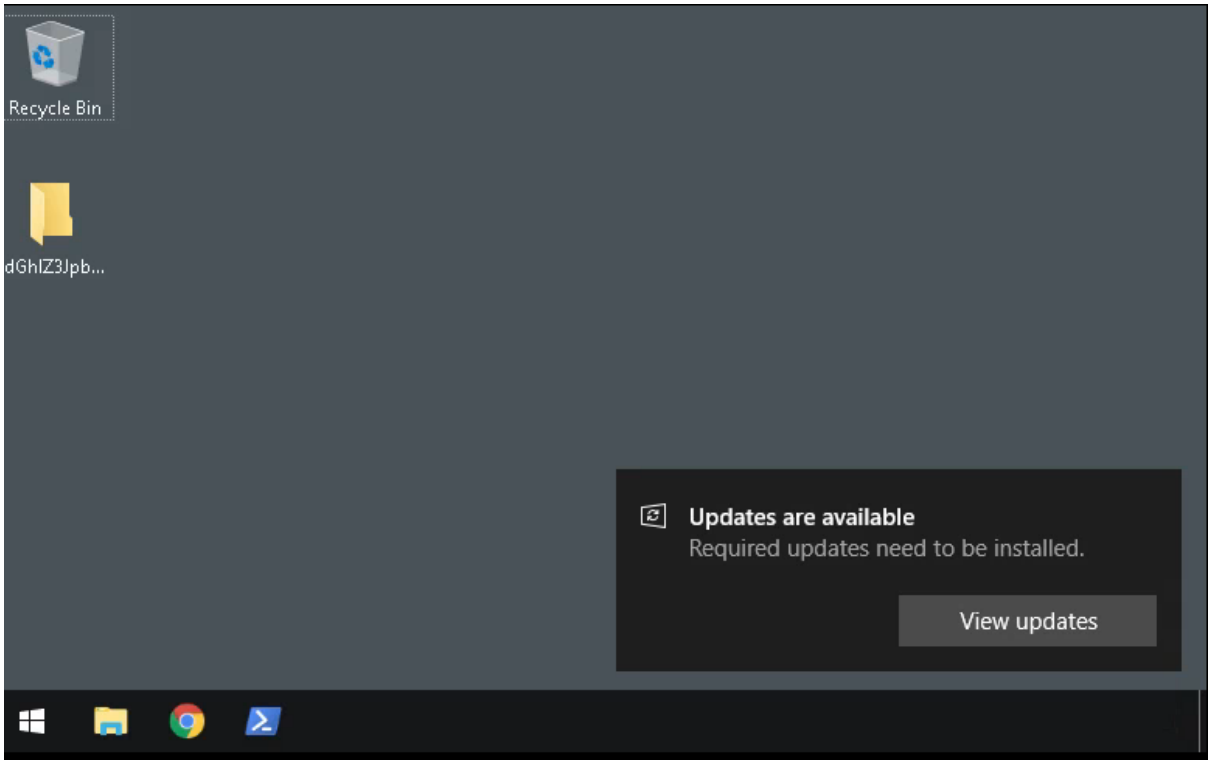
For **Server** provide (`10.10.167.86`) as the IP address provided to you for the remote machine. The credentials for the user account is:

- User name: `Administrator`
- User password: `sn0wF!akes!!!`

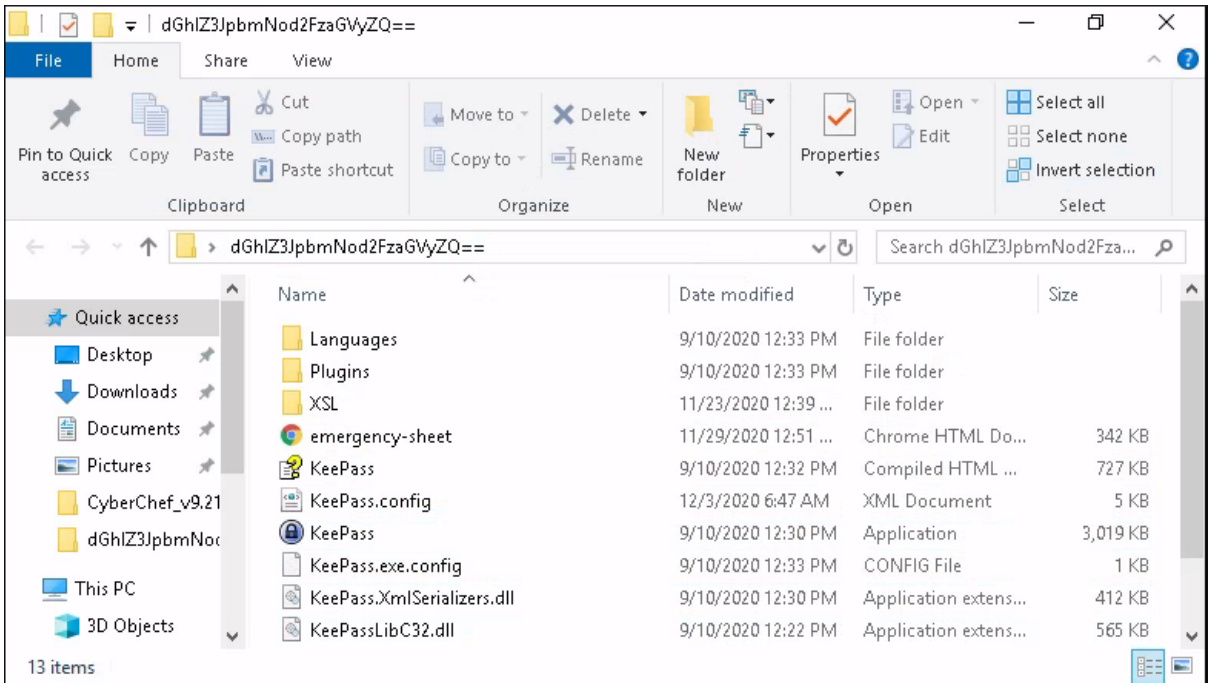
We then setting up remmina with the credentials given.



Once we are in the server, the machine was a windows machine and got a folder with folder name which seems like an encrypted text



Inside we found the files for KeePass application.



Based on the task details, we need to decrypt the file name using “magic” in order to get the new KeePass password

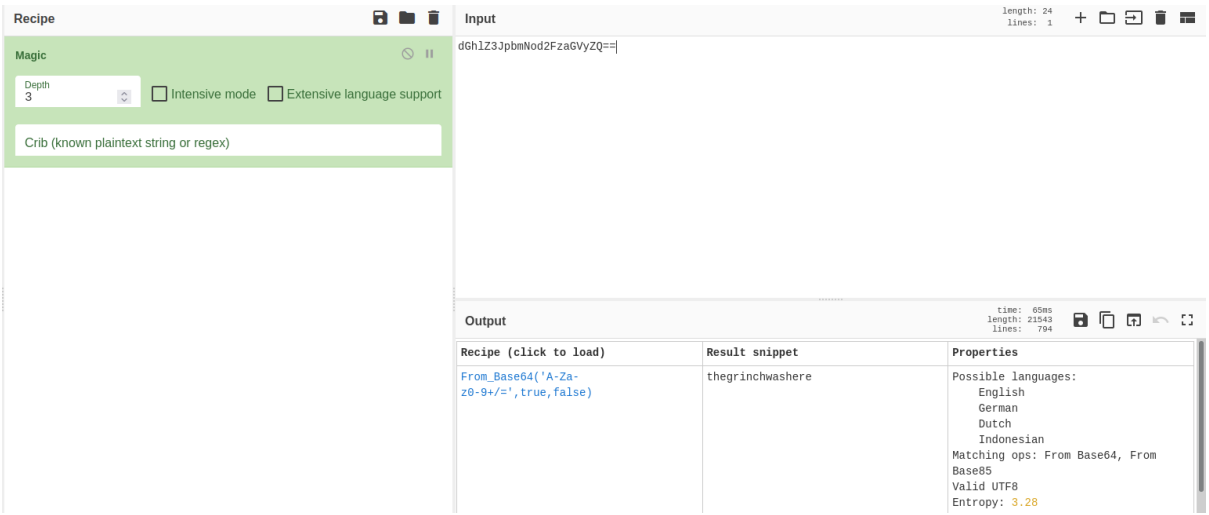
Now with that out of the way, open the strange-looking folder name on the desktop and run KeePass. You will be prompted to enter the master password. If you enter the phrase **mceagerrockstar** you will see a message stating that the key is invalid.

Looking back at the folder name it looks cryptic, like some sort of encoding. Encryption and encoding are familiar techniques used in IT, especially within Computer Security. Malware writers use some of these encoding techniques to hide their malicious code. Some encodings are quickly identifiable and some are not.

You can use **CyberChef** to decrypt/decode the encrypted/encoded values that you will encounter within this endpoint. CyberChef is the self-purported 'Cyber Swiss-Army Knife' created by GCHQ. It's a fantastic tool for data transformation, extraction & manipulation in your web-browser. CyberChef uses recipes to perform this magic.

Speaking of 'magic', you can use the `Magic` recipe to decode the folder name. There is a local copy of CyberChef (`C:\Tools`) on the endpoint.

Done decrypting, we know that the new password is “thegrinchwashere”.

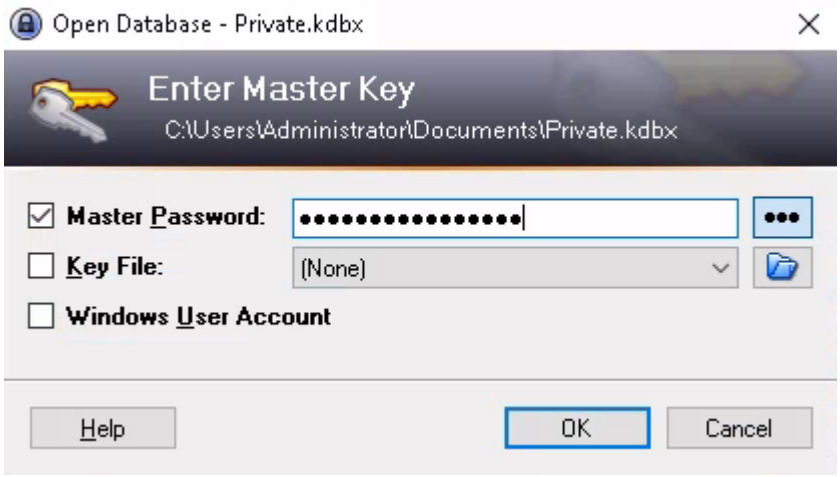


Question 2

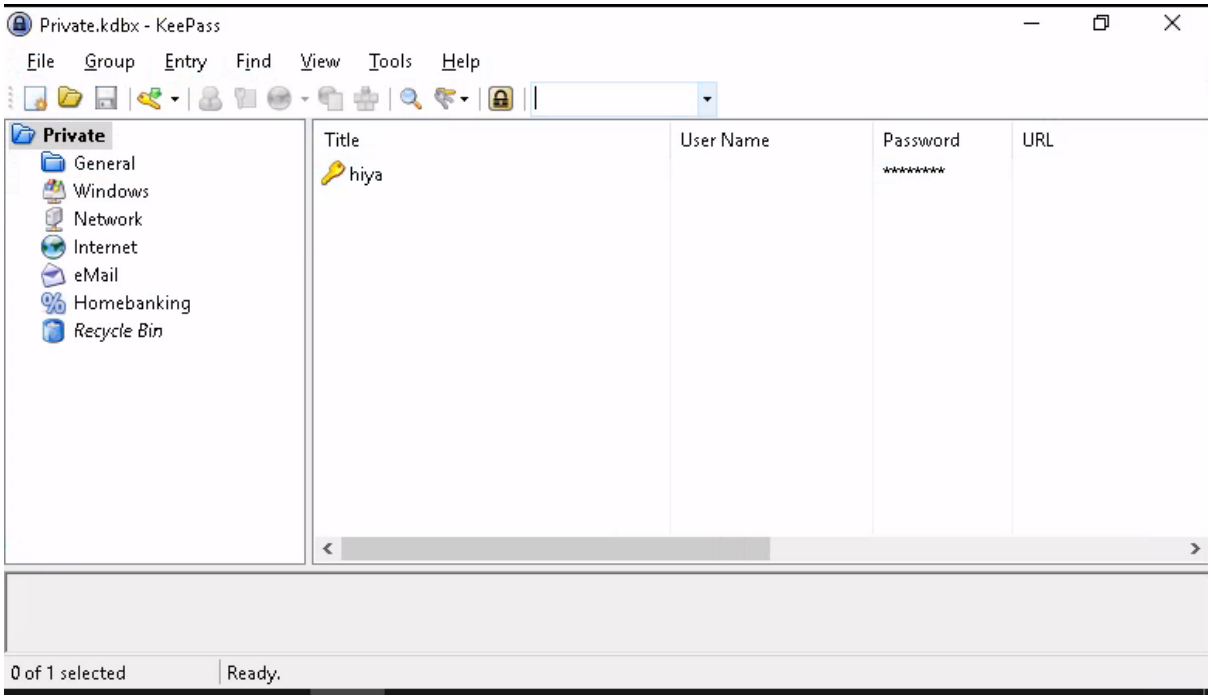
The CyberChef also stated that the encoding method listed as the “matching ops” is base64

Question 3

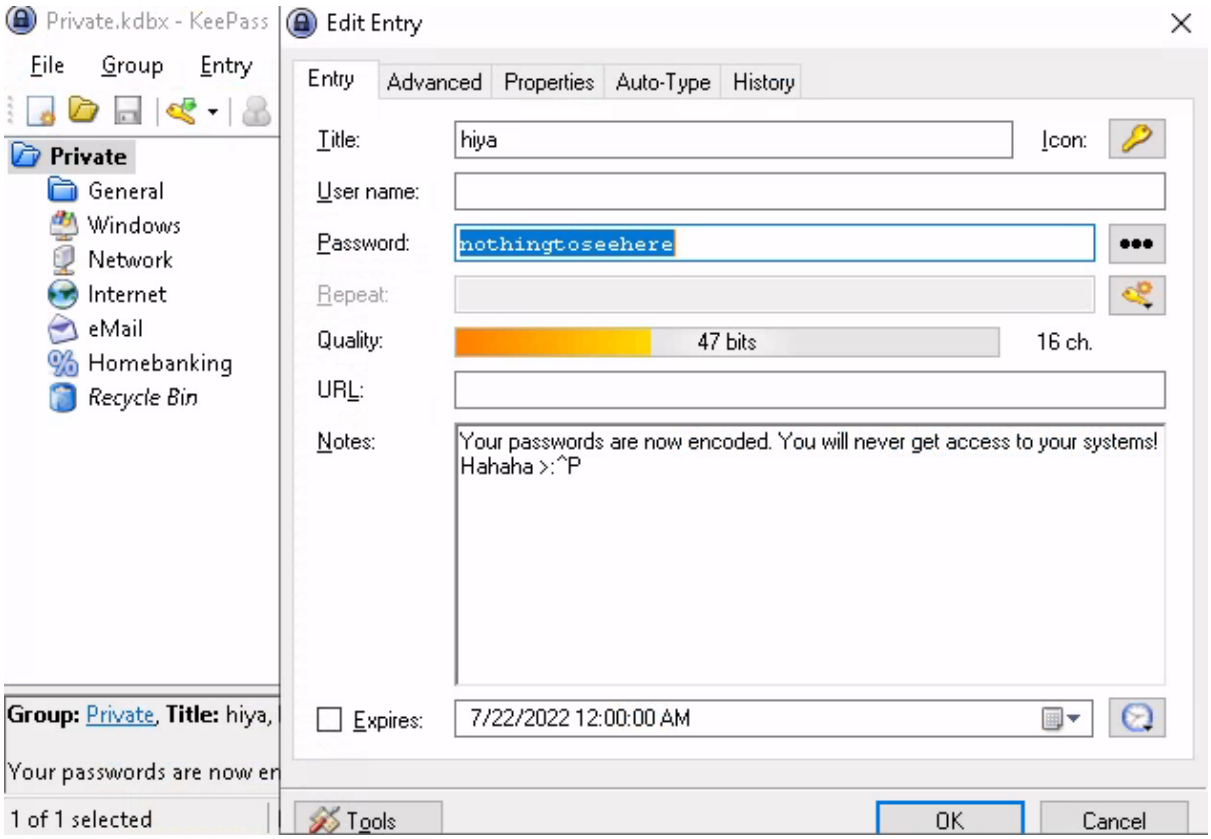
With the password to the KeePass we got earlier, we then try to access the password manager and it was a success.



On the private password section, we got a key named hiya.

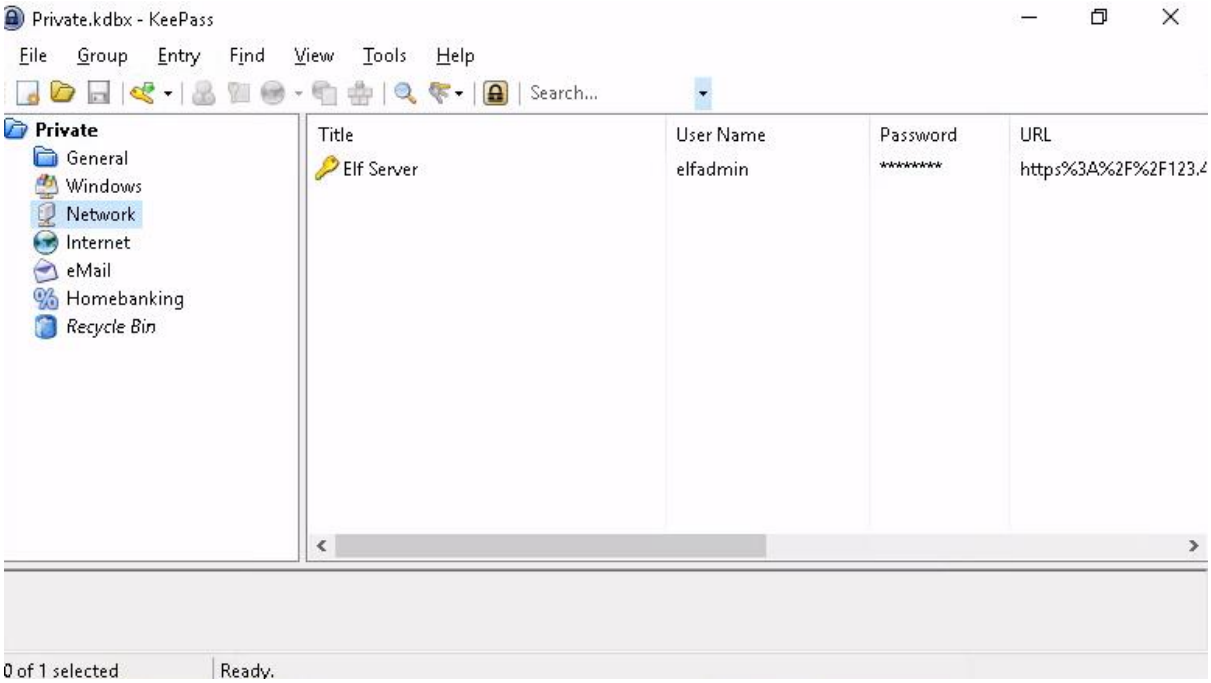


The password for hiya key is “nothingtoseehere”.

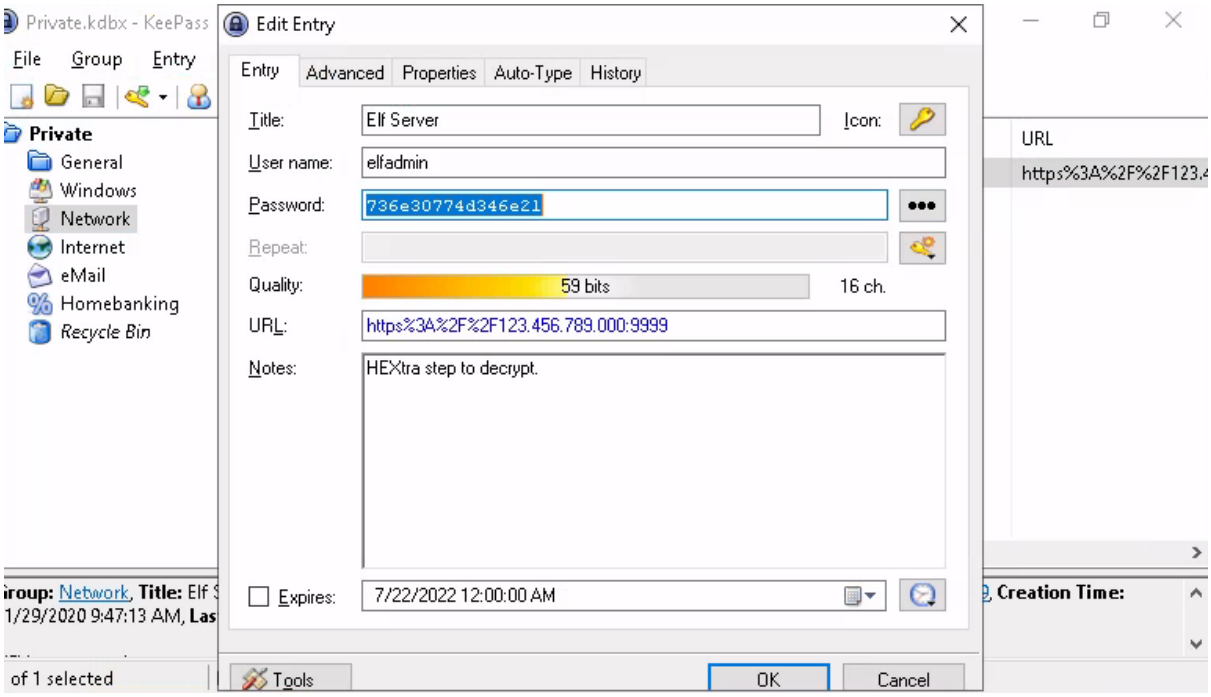


Question 4

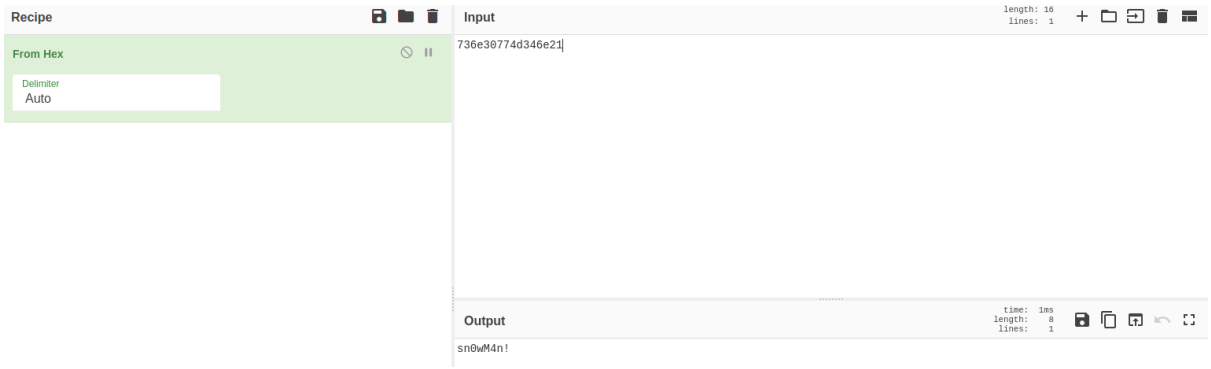
On the network password section, we got the password to the Elf Server.



But it seems that the password needed the extra step to decrypt it.



The decryption got us the password which is “sn0wM4n!”

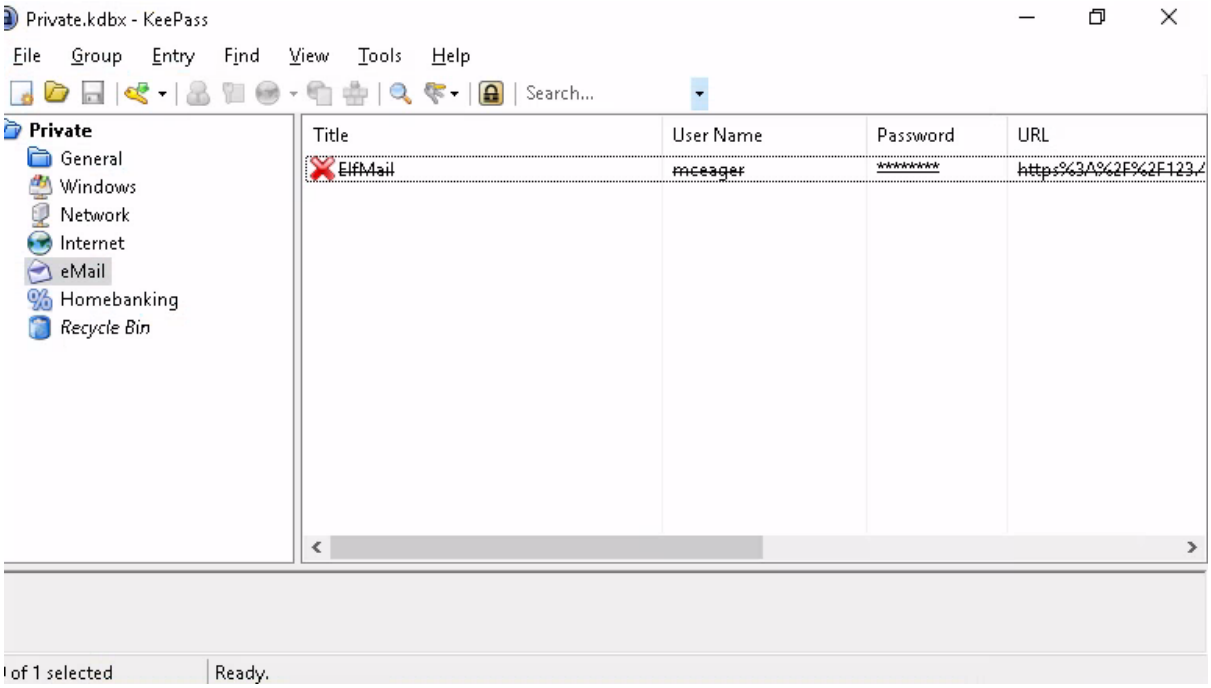


Question 5

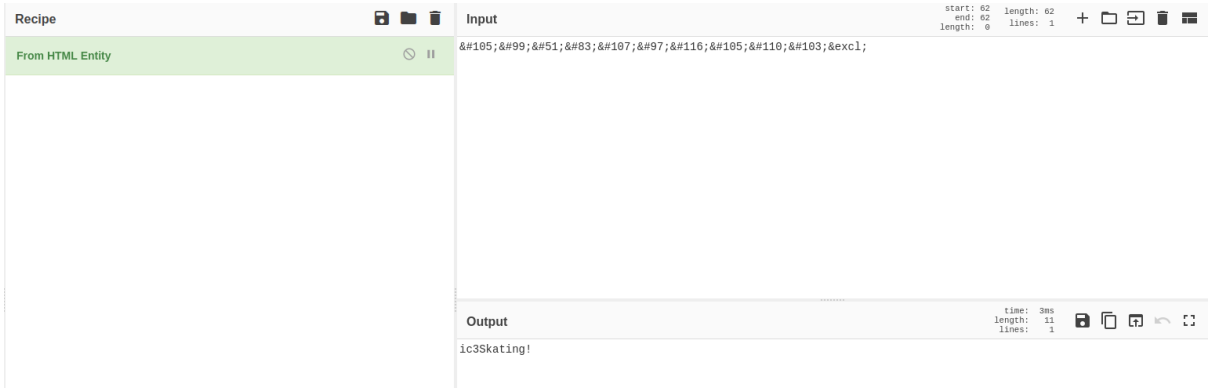
Also, based on the pun given on the notes, we know that the encoding we needed is hex.

Question 6

On the email section there's the password to the ElfMail.

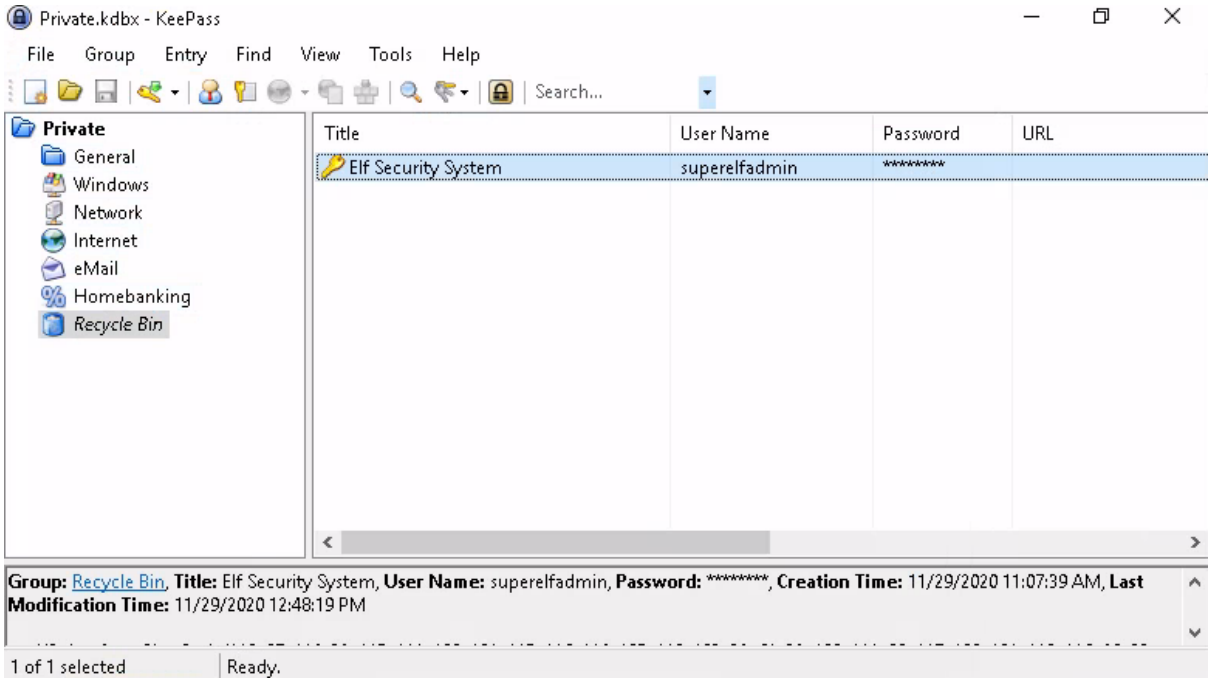


After decrypting, we know that the password is ic3Skating!.

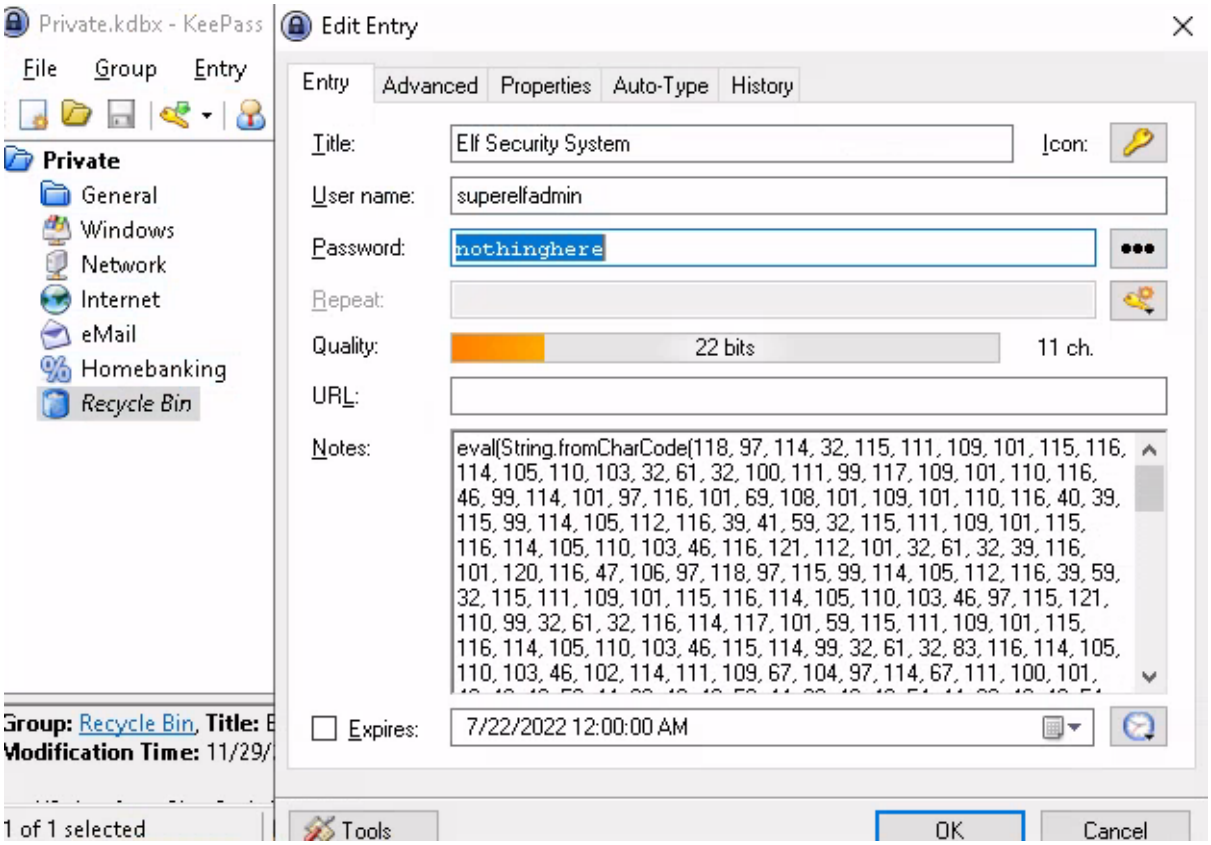


Question 7

When we check the recycle bin, There's a password to the Elf Security System

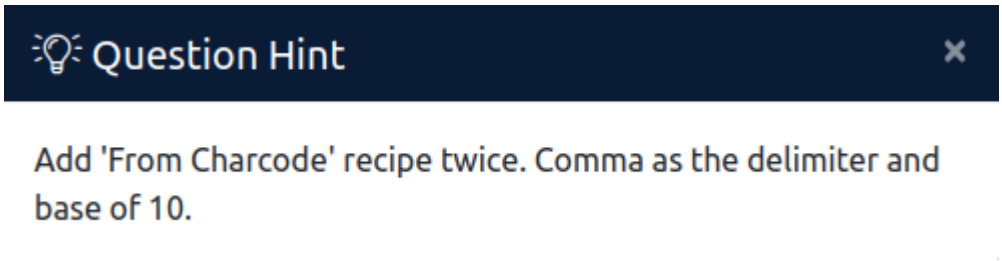


There we can see the username and password for the system.

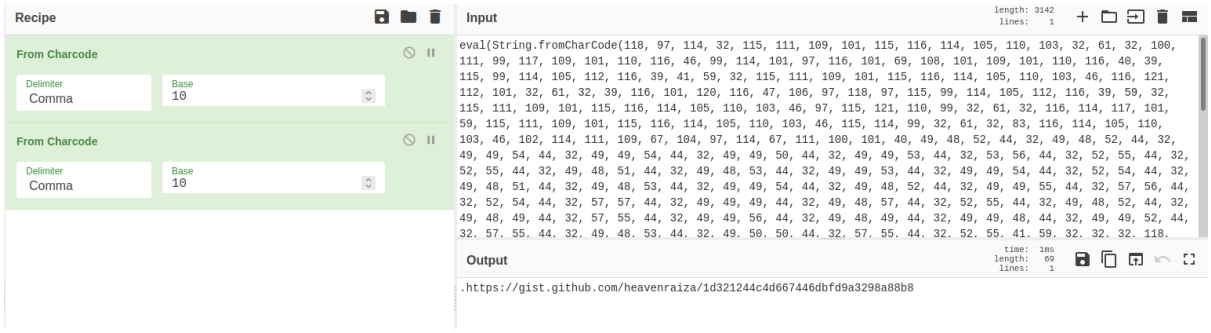


Question 8

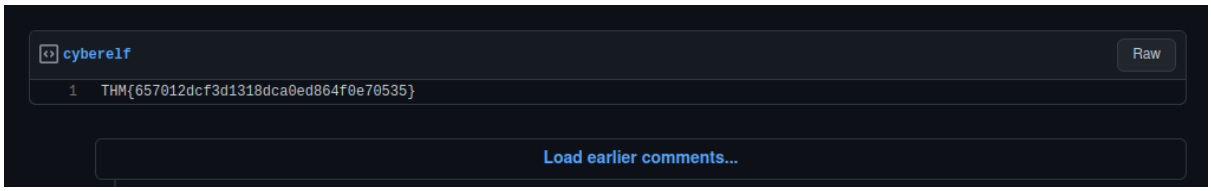
On the notes of the Elf Security System, we can see texts stating that it is from CharCode. But since we can't decrypt it, we decided on looking at the hint and we know that we need to decrypt it twice.



Once we done decrypting it twice, it gives us a link.



The link leads us to the flag for today.



Thought Process/Methodology:

When we started the task, we were given an IP address of a remote machine with the credentials for the user account. We then setting up remmina with the credentials given. Once we are in the server, the machine was a windows machine and got a folder with folder name which seems like an encrypted text. Inside we found the files for KeePass application. Based on the task details, we need to decrypt the file name using "magic" in order to get the new KeePass password. With the password to the KeePass we got earlier, we then try to access the password manager and it was a success. When we check the recycle bin, There's a password to the Elf Security System. Once we done decrypting the text on the notes, it gives us a link. The link leads us to the flag for today.

Day 22: Blue Teaming – The Grinch strikes again!

Tools used: Kali Linux, Firefox, Remmina

Solution/walkthrough:

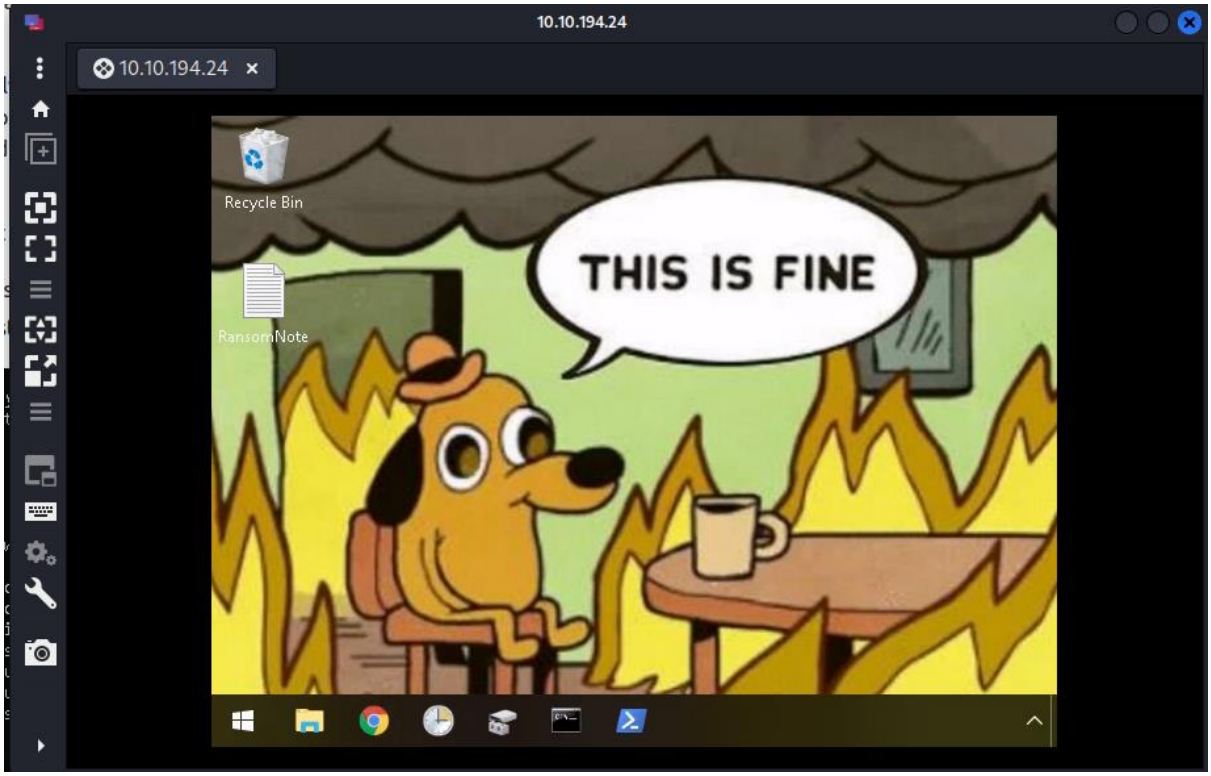
Question 1

Starting the task, we are given an IP address to a remote machine with the credentials for the user account.

For **Server** provide (`10.10.194.24`) as the IP address provided to you for the remote machine. The credentials for the user account is:

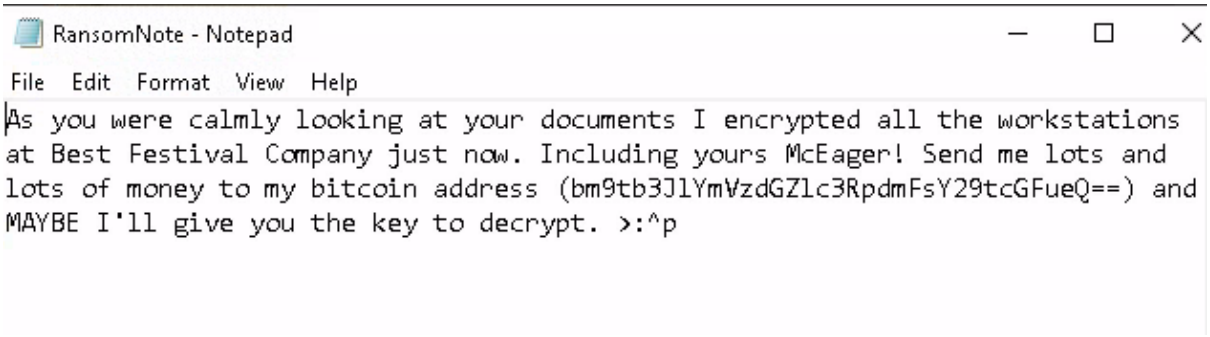
- User name: `administrator`
- User password: `sn0wF!akes!!!`

The wallpaper of the machine can be seen.

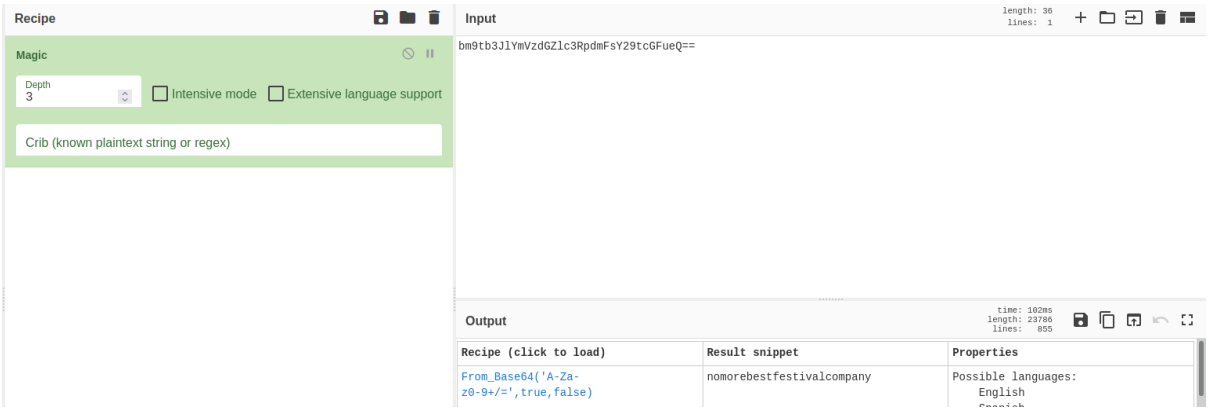


Question 2

Once in the machine, there was a text file named Ransom Note with an bitcoin address on it

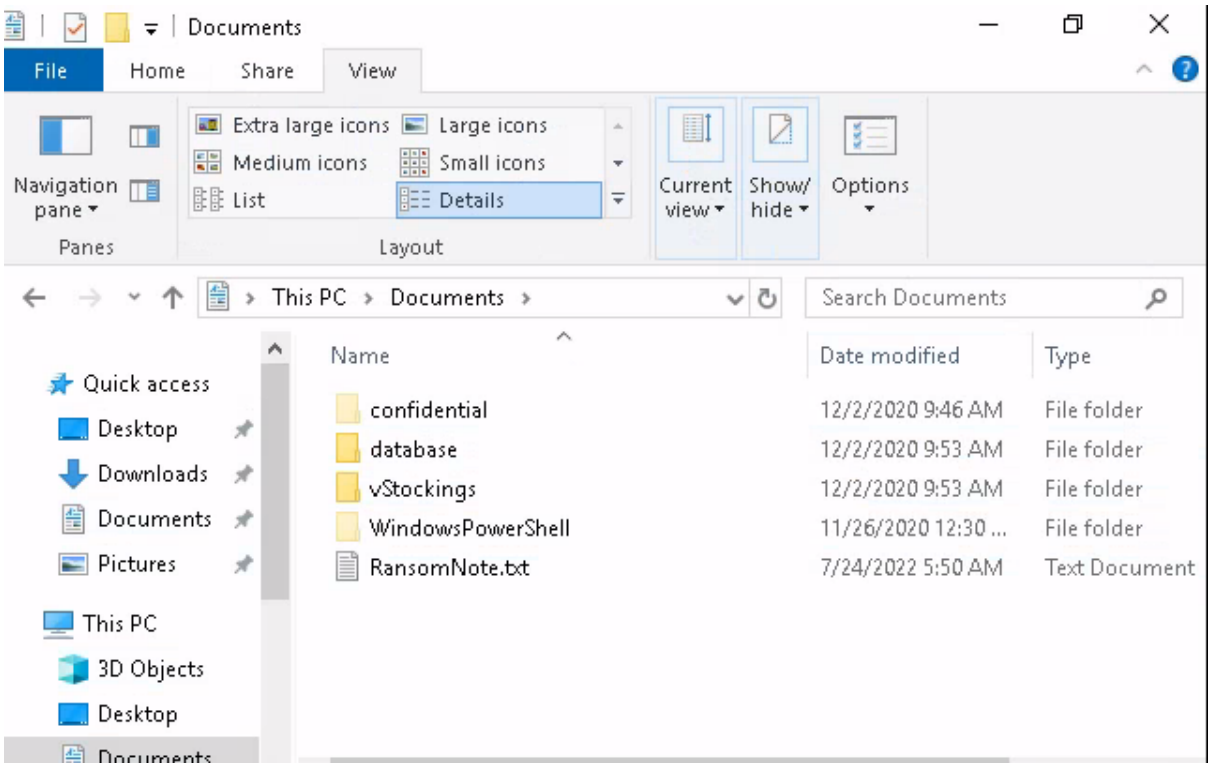


Using the CyberChef, we decrypt the bitcoin address and it reveals the real message which is “nomorebestfestivalcompany”.

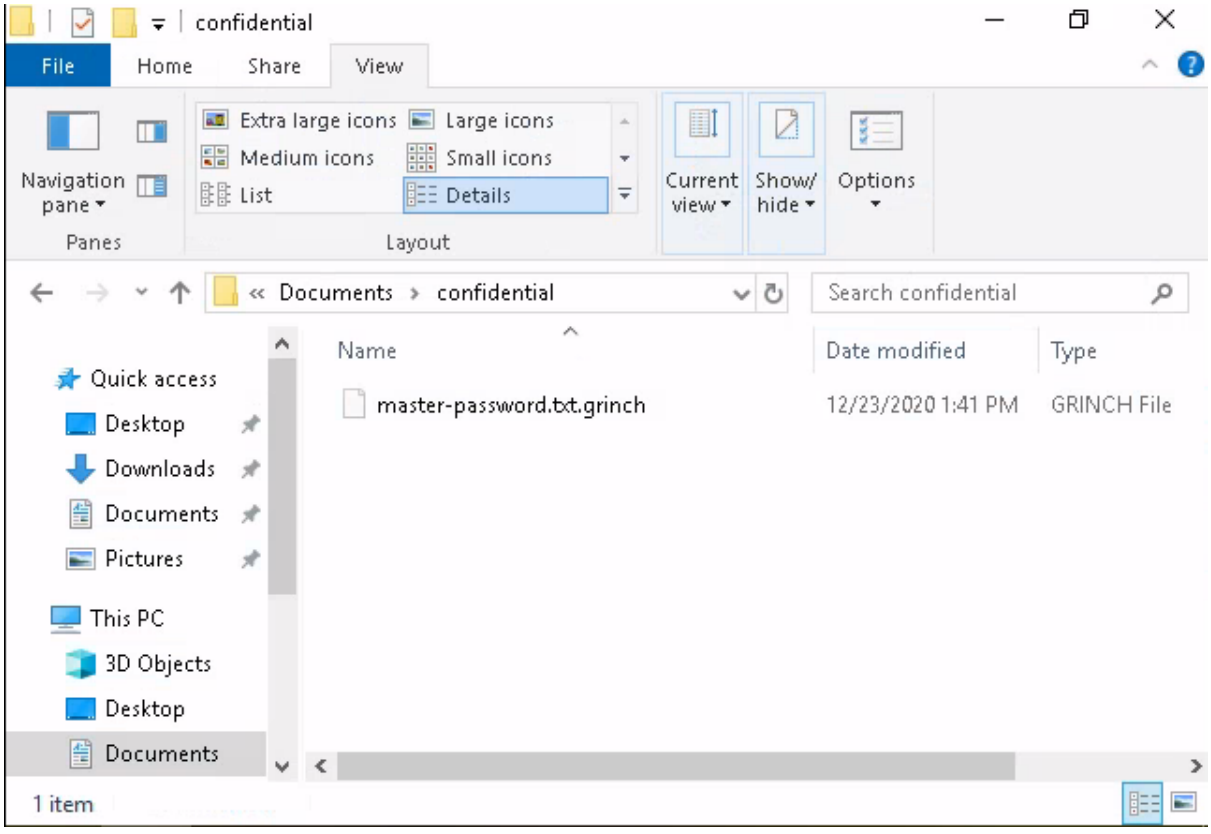


Question 3

We accidently found a secret folder when trying to check for the file extension of the note.

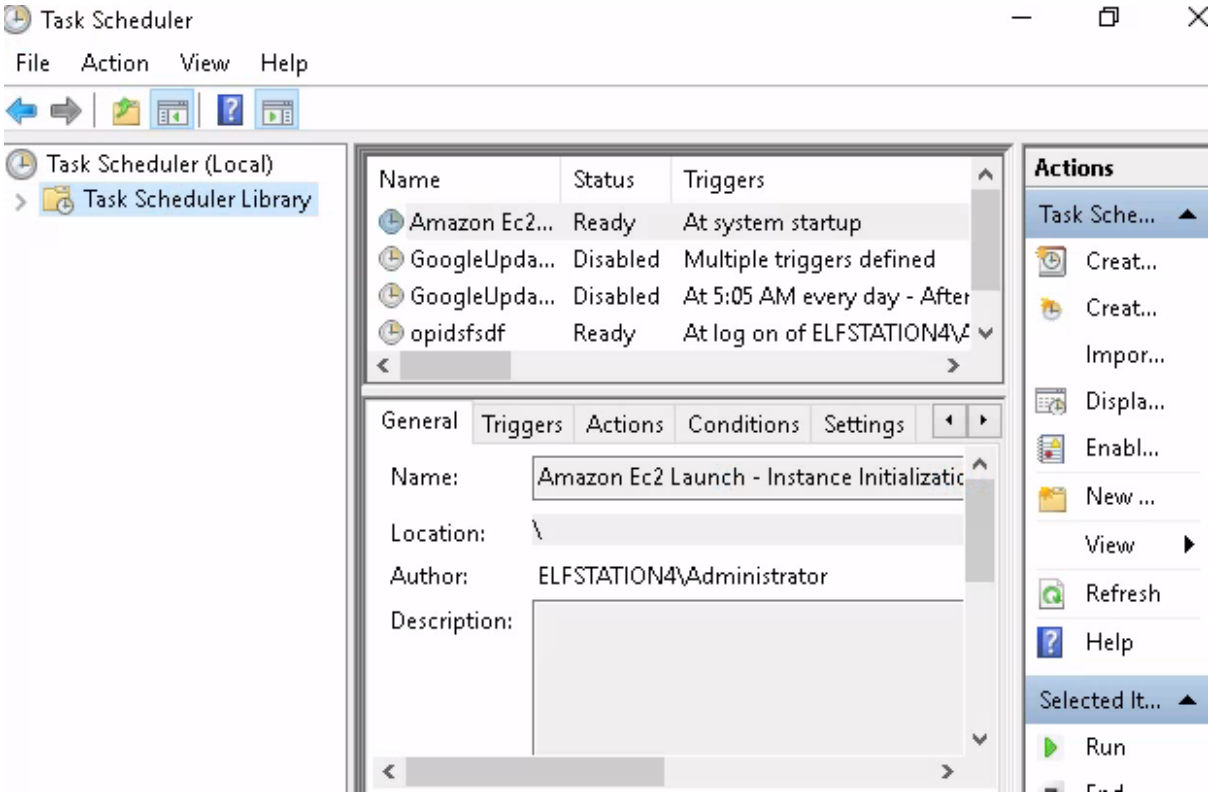


The text file in the hidden folder has the ".grinch" extension on it.



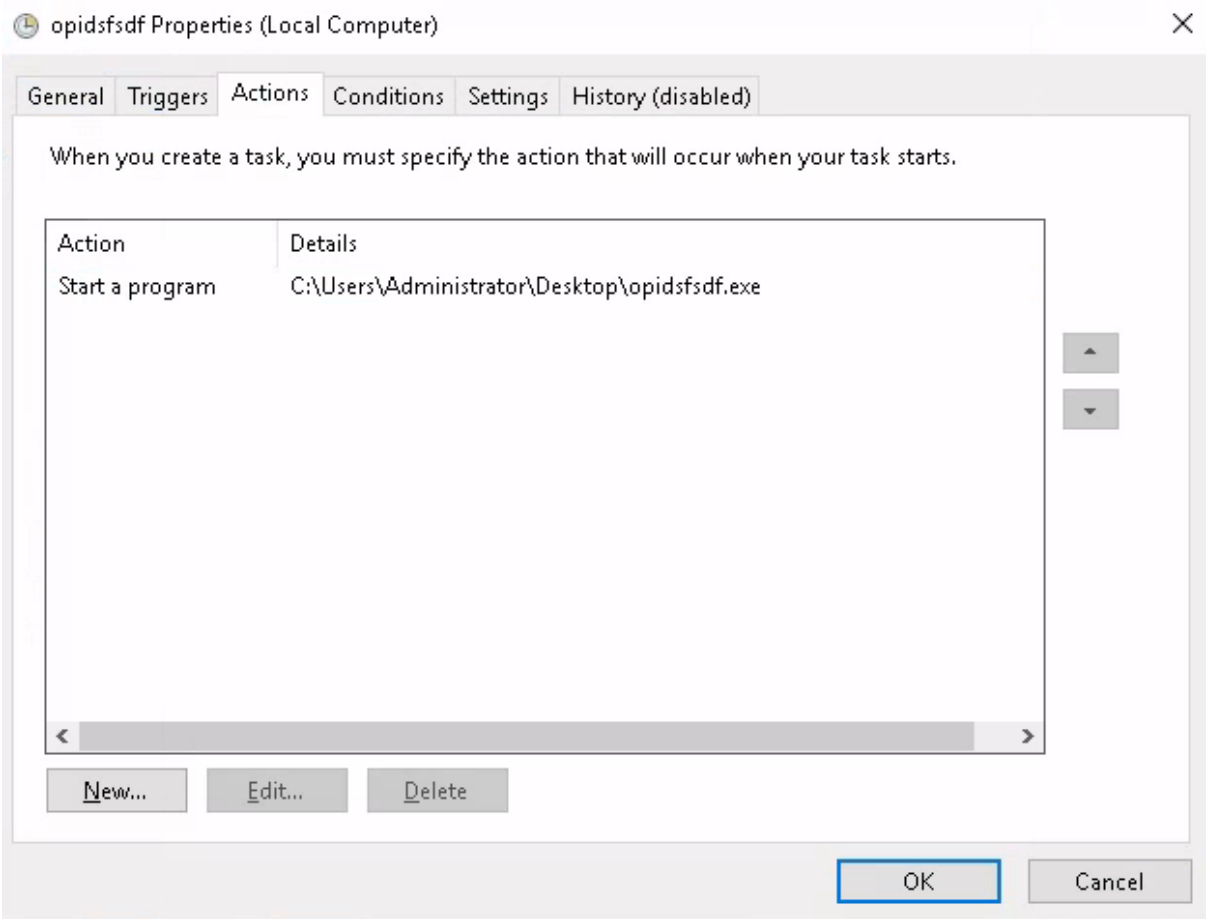
Question 4

The suspicious scheduled task that can be seen on the task scheduler is opidsfsdf.



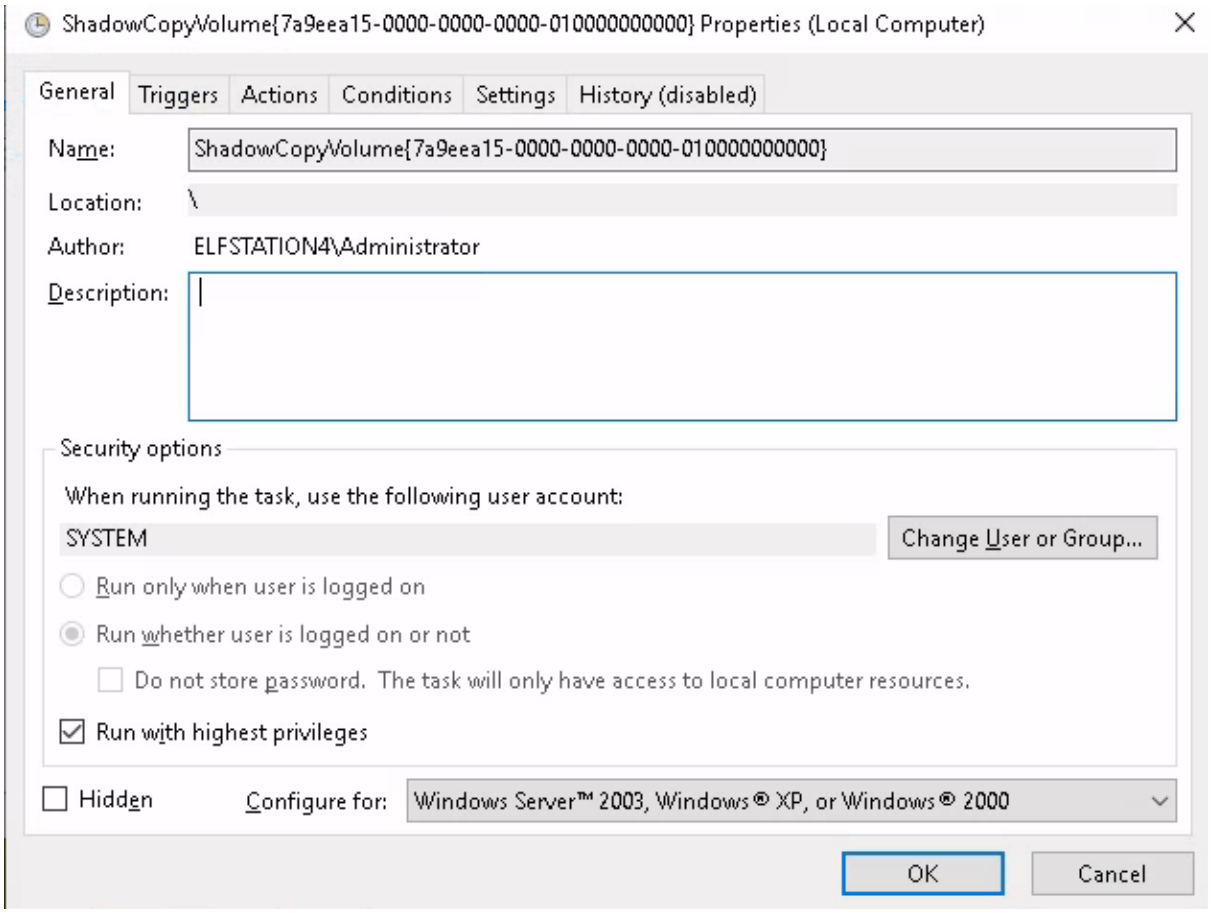
Question 5

By checking the actions property, we can see the path of the executable.



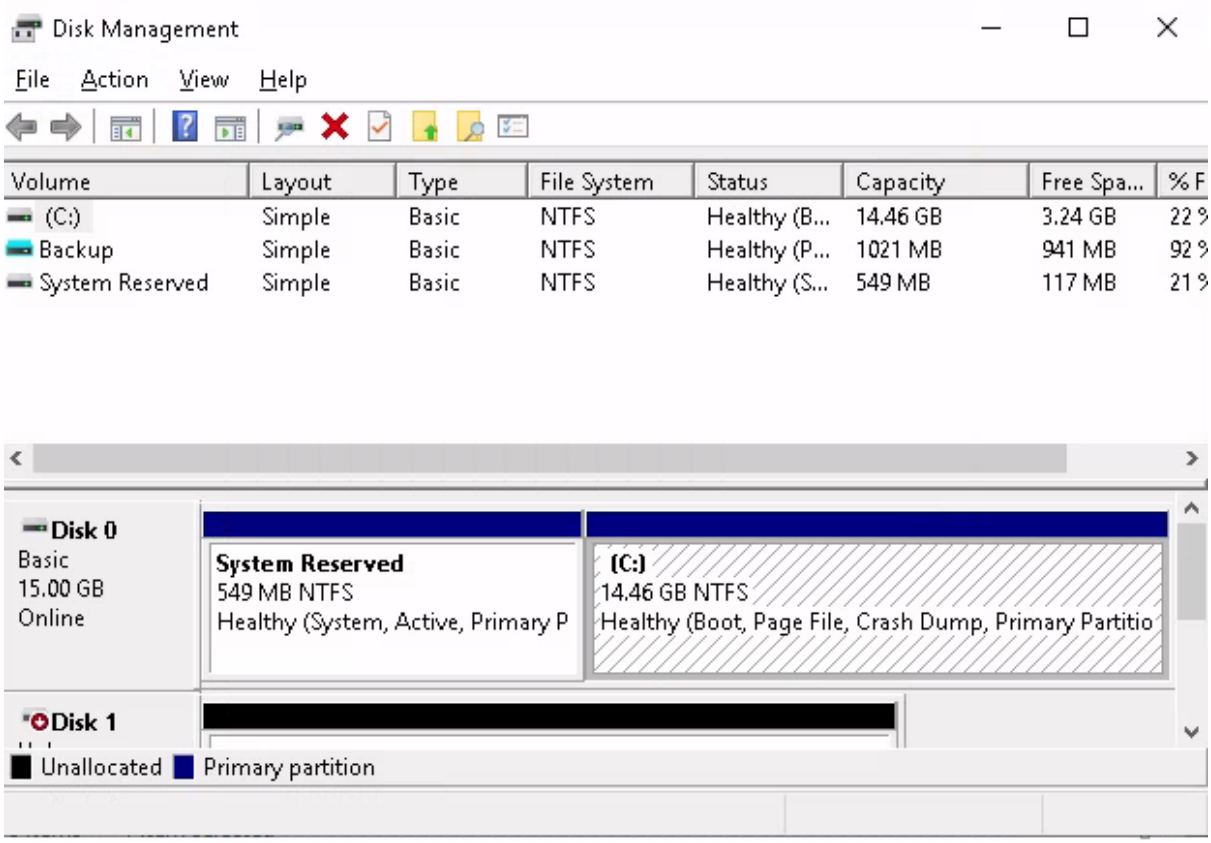
Question 6

The other scheduled task that is related to VSS is ShadowCopyVolume.

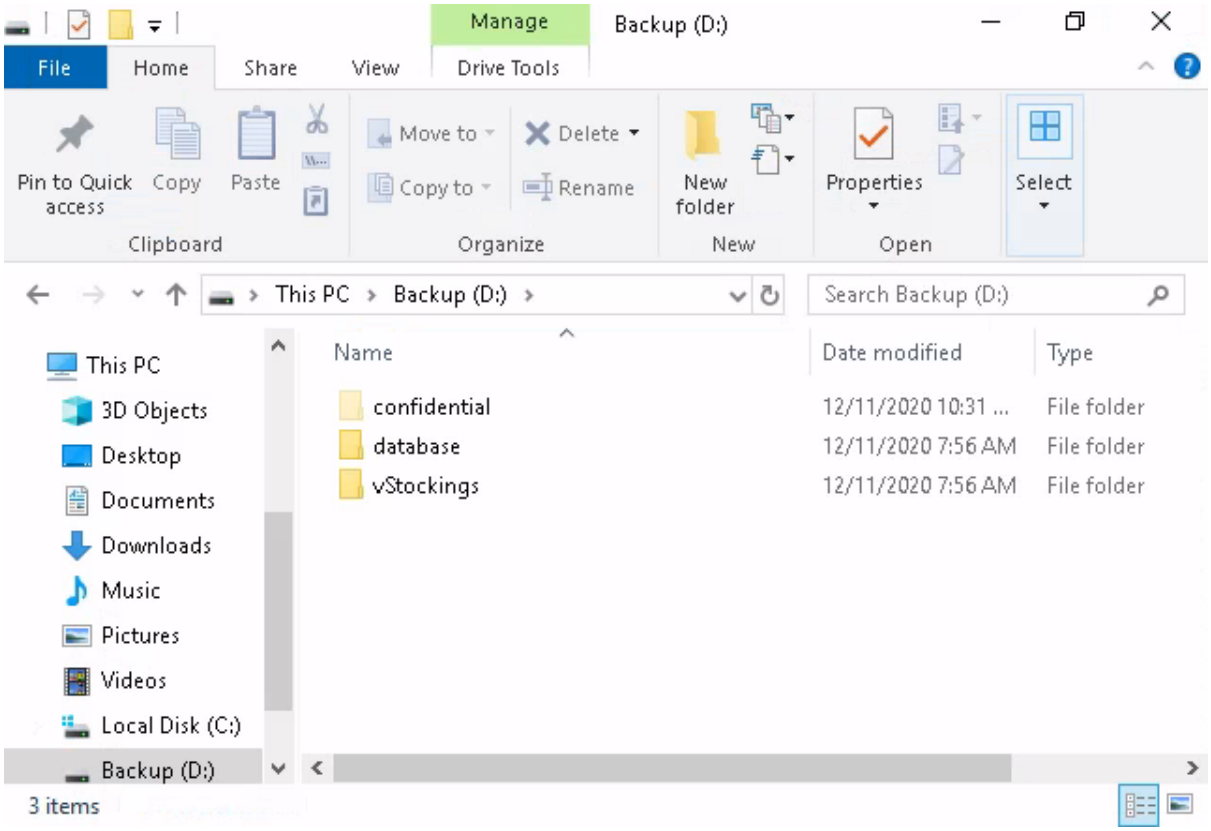


Question 7

Once we checked the disk management, we realized that there is a backup disk partition.

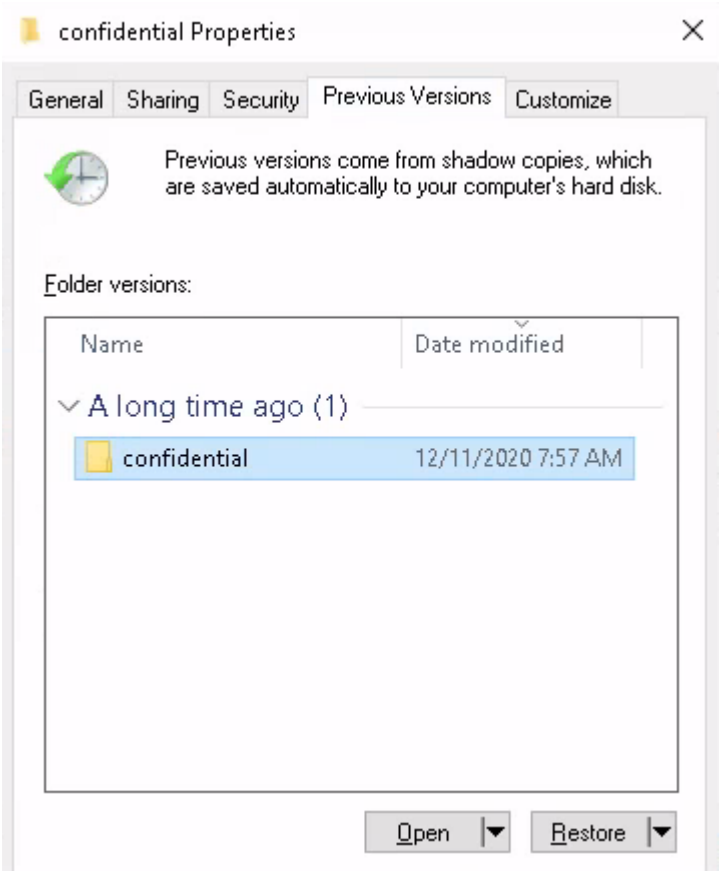


We open it and find that there is another hidden folder named “confidential”.

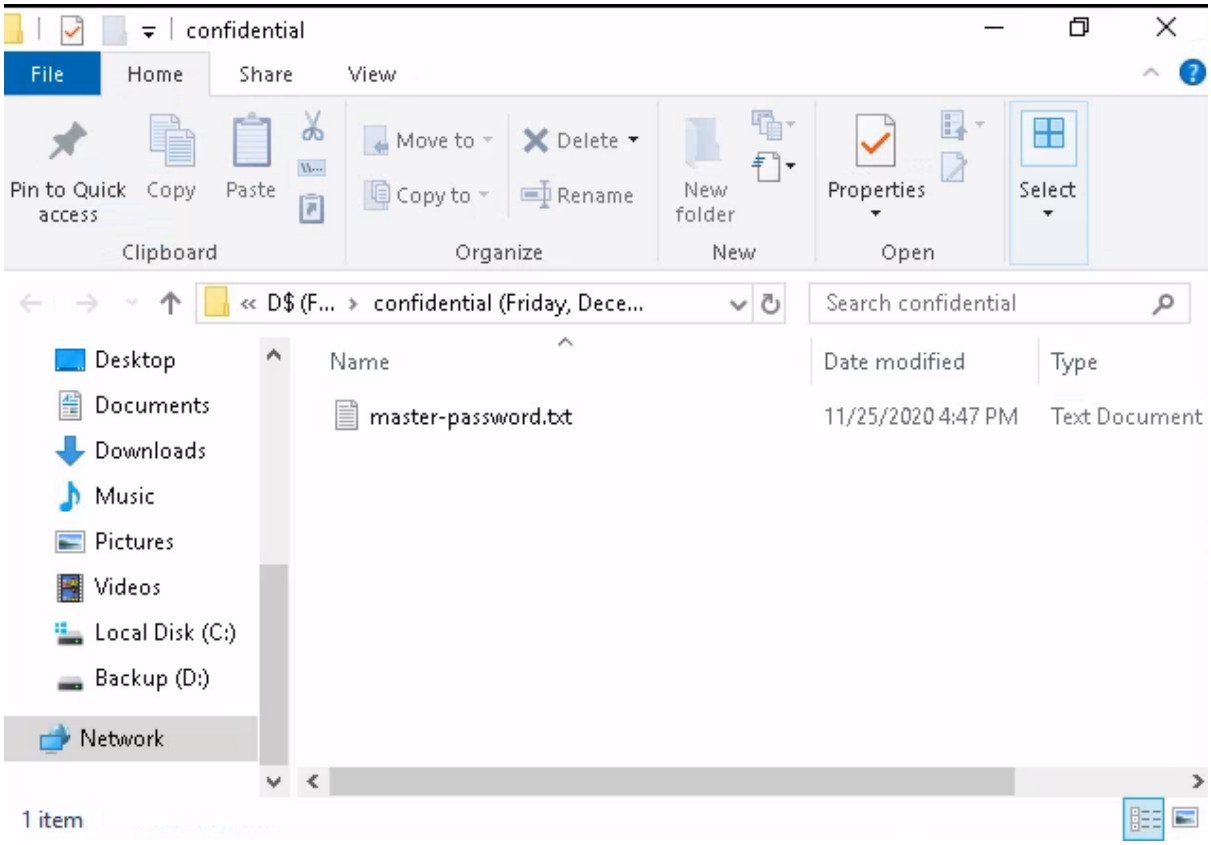


Question 8

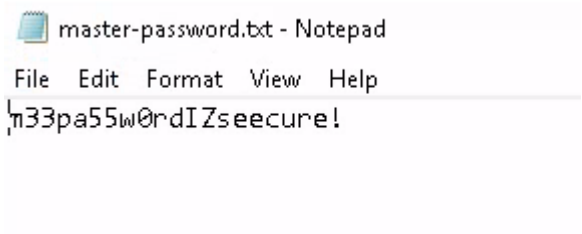
We check the properties and return it to the previous version.



Inside there, we can find a master password text file.



It gives us the password for the ransomware.



Thought Process/Methodology:

Starting the task, we are given an IP address to a remote machine with the credentials for the user account. Once in the machine, there was a text file named Ransom Note with an bitcoin address on it. We accidently found a secret folder when trying to check for the file extension of the note. Once we checked the disk management, we realized that there is a backup disk partition. We open it and find that there is another hidden folder named “confidential”. We check the properties and return it to the previous version. Inside there, we can find a master password text file. It gives us the password for the ransomware.