PSP0201 Week 6 Writeup

Group Name: Undecided

Members:

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

Day 22 : Blue Teaming – Elf McEafer becomes CyberElf

Tools used: Kali Linux, Remmina, Firefox

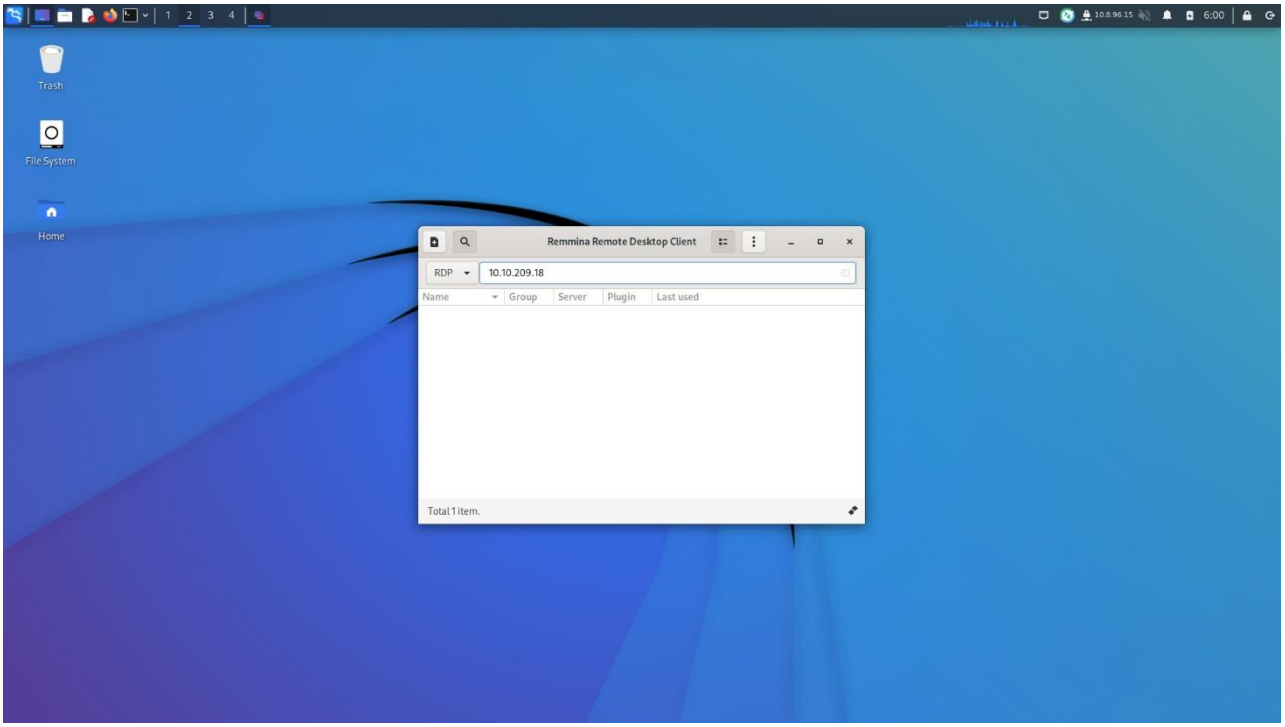
Solution/walkthrough:

Question 1

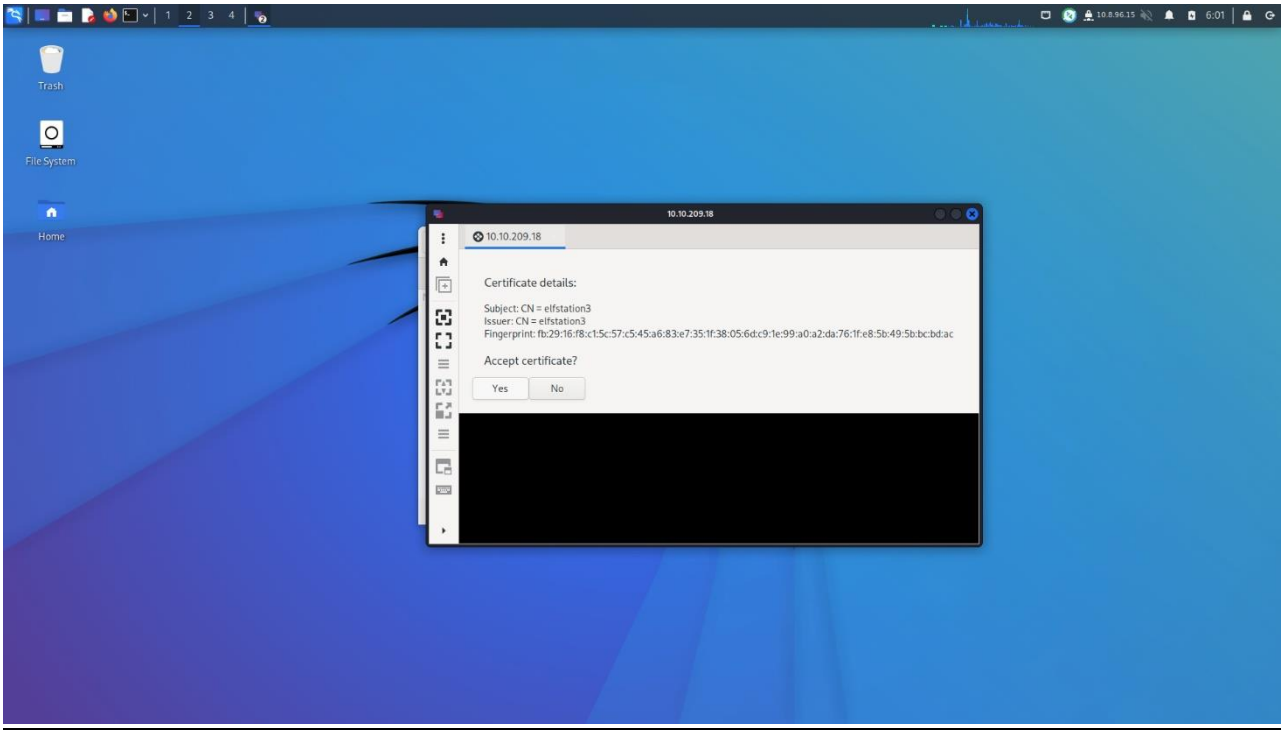
To start the task, we first connected to the server provided with the credentials for the user account.

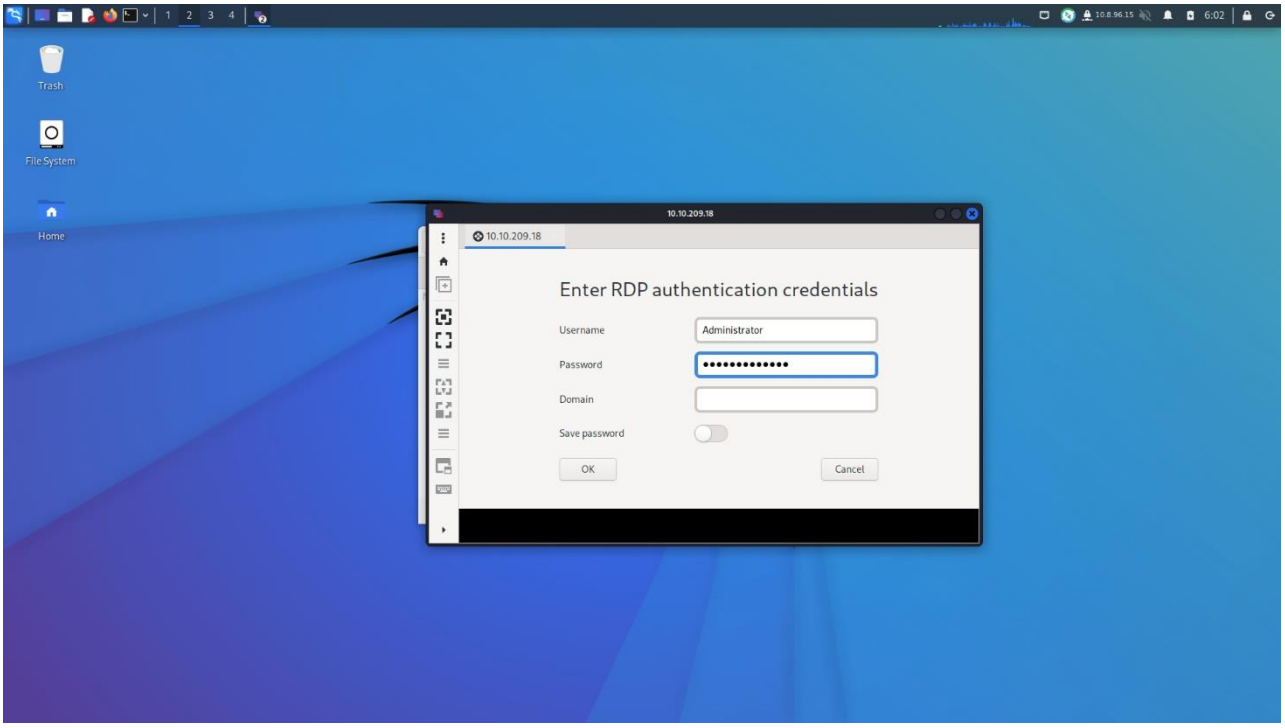
User name: Administrator

User password: sn0wF!akes!!!

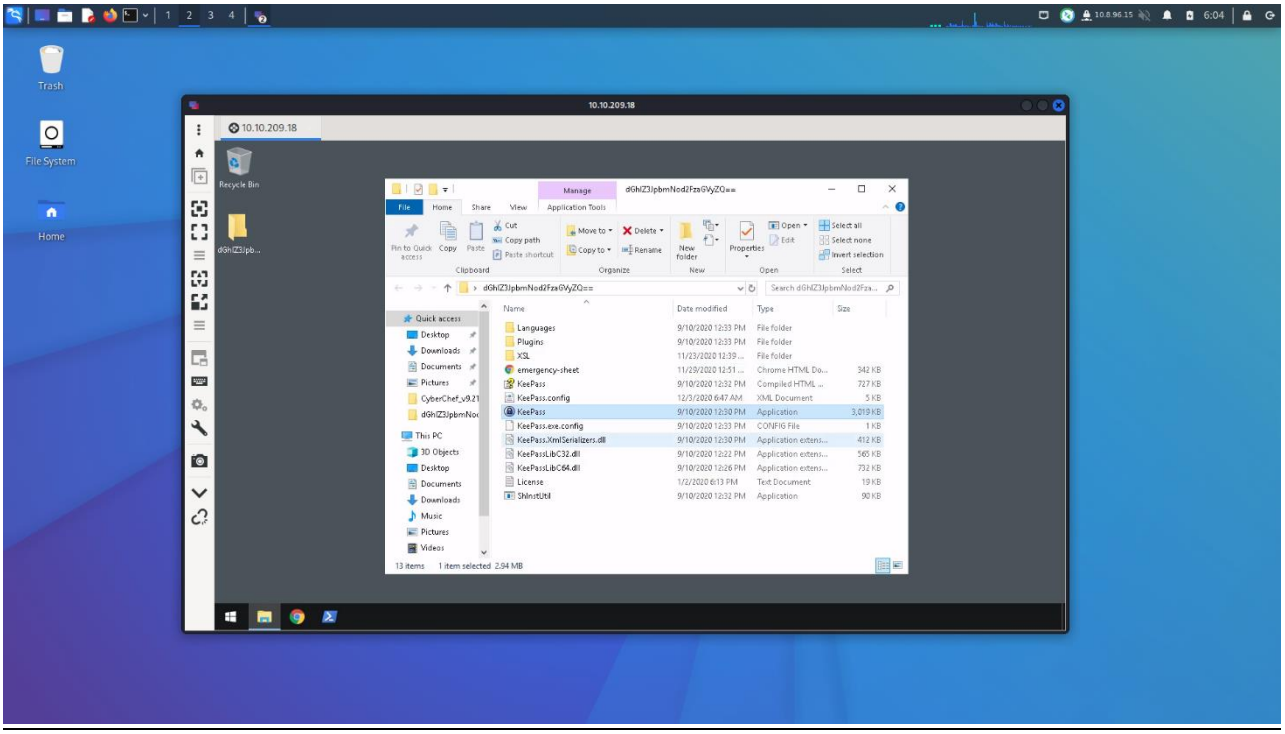


We accepted the certificate and logged into the remote system.

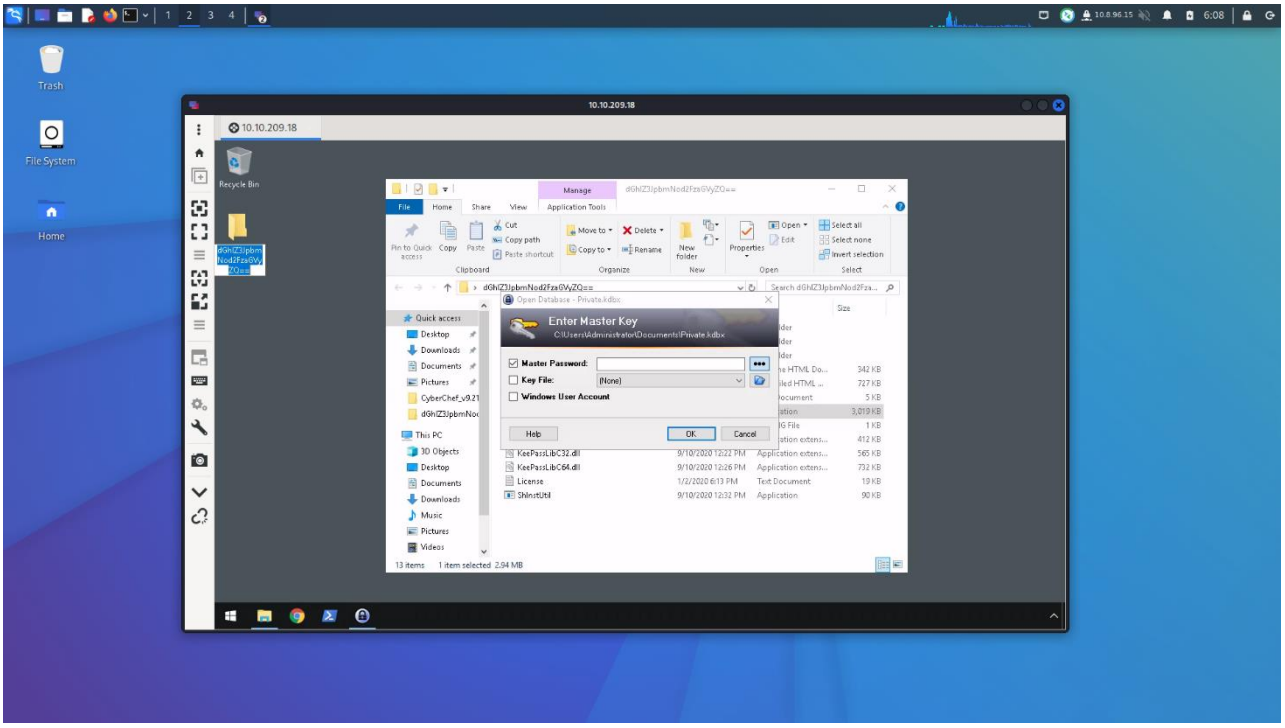




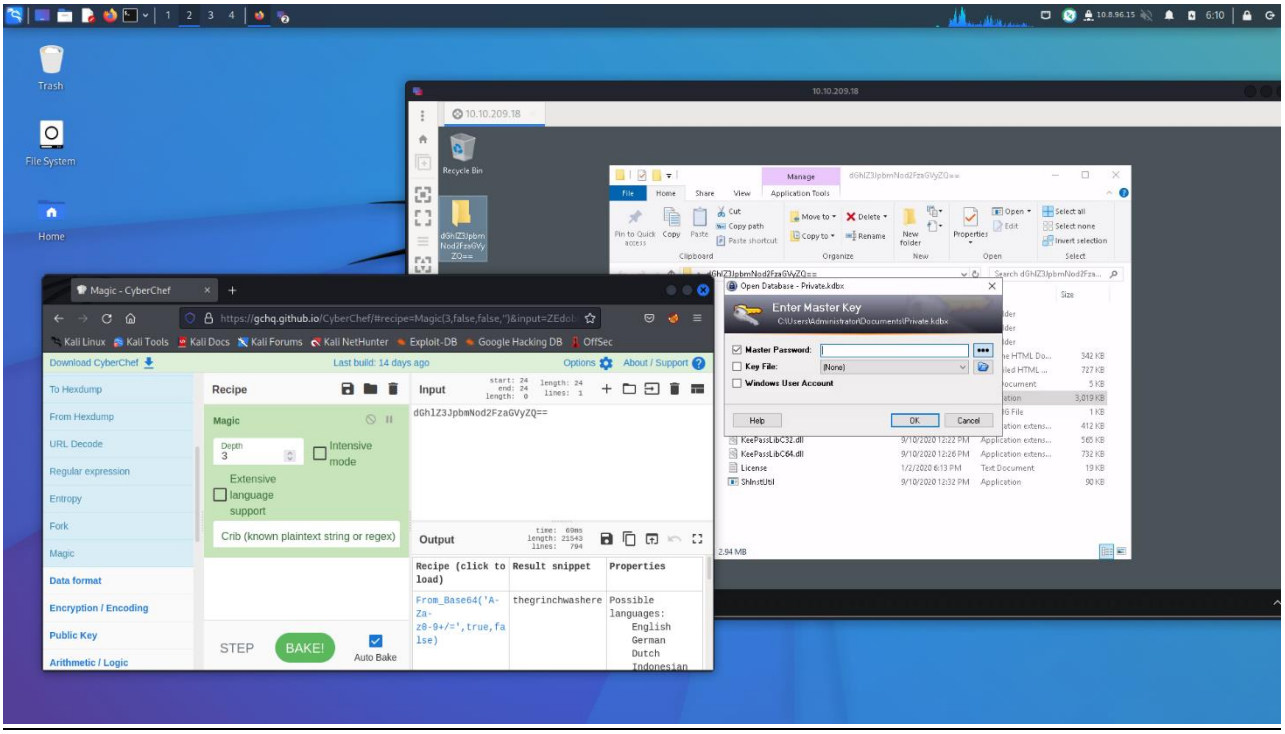
Once connected, we opened the strange looking folder name on the desktop. In there, we found an application KeePass which store all types of data, including password.



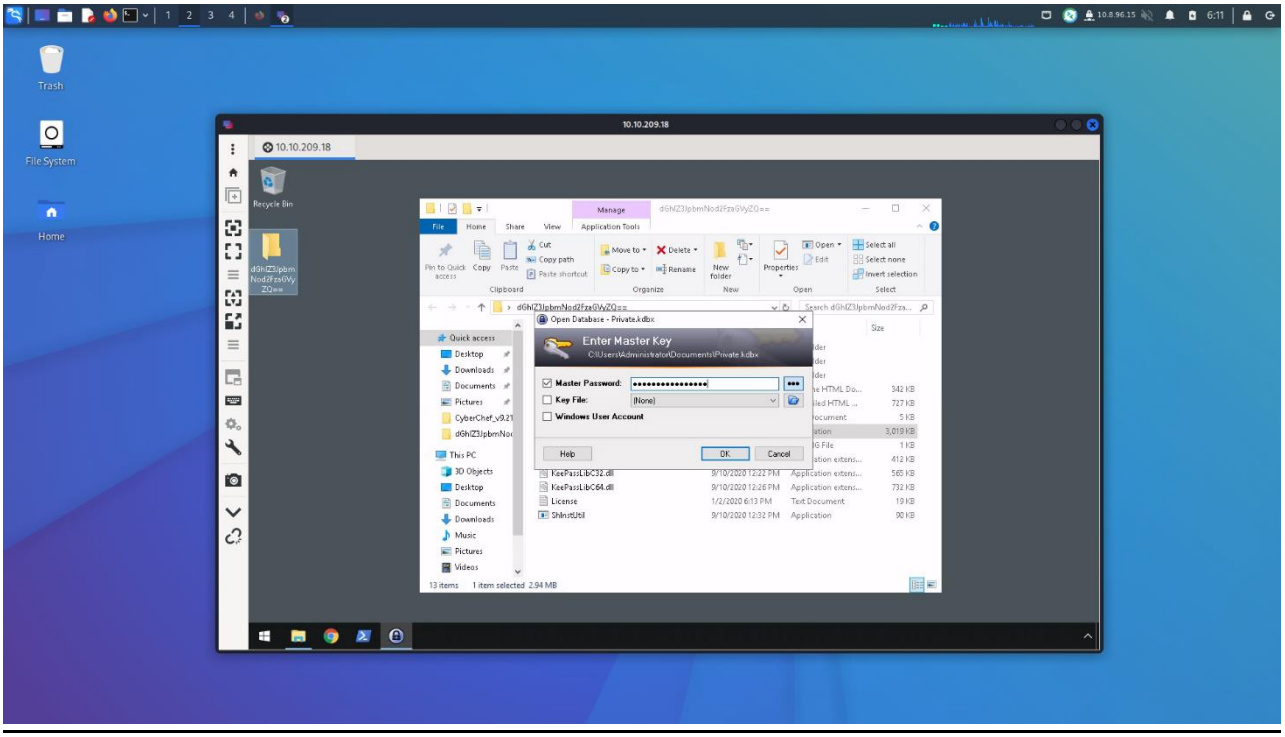
The strange file name looked like it was encoded into something, so we decided to try decoding it.



We headed to Cyberchef and enter the strange file name in the input. We picked the ‘Magic’ recipe to decode it.



The result output showed us what we suspected to be the Master Key password. We entered the output into the Master Password and gained access into the application.



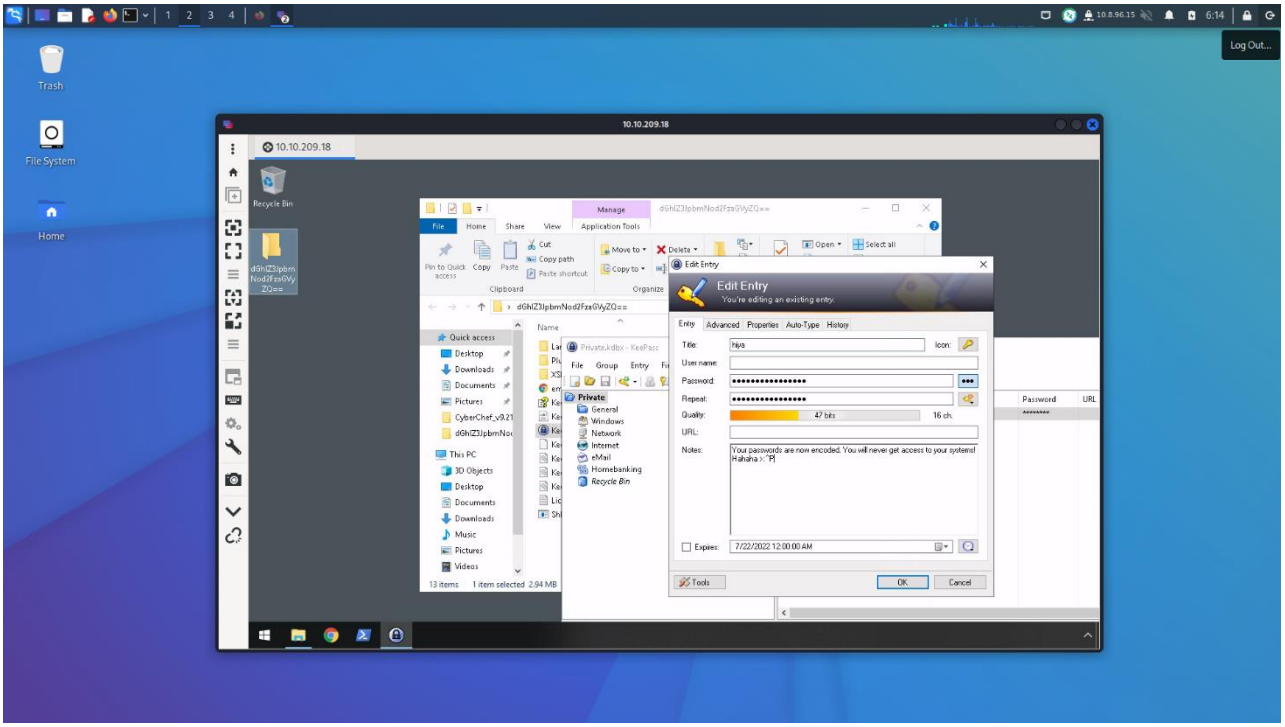
Question 2

Under the properties section, we found that the encoding method is Base64.

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

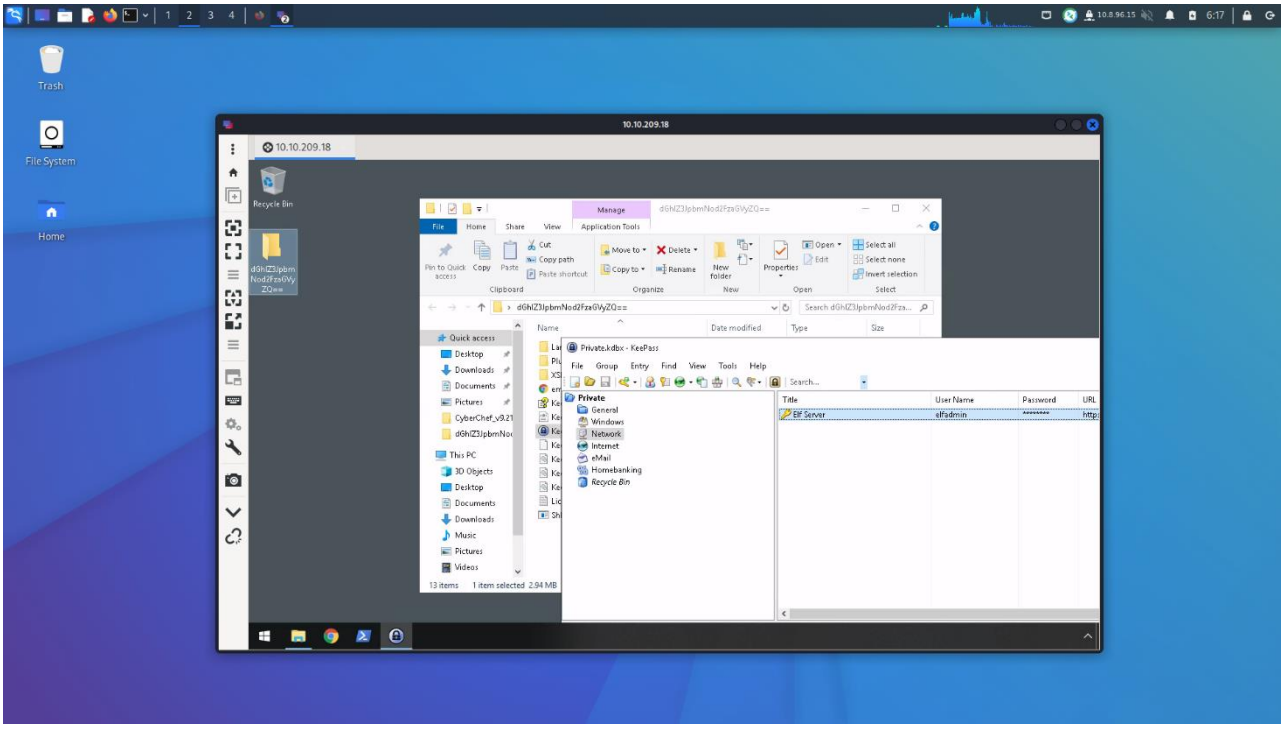
Question 3

Once we gained access, we notice the hiya key under the private folder. We opened it and found a note left behind.

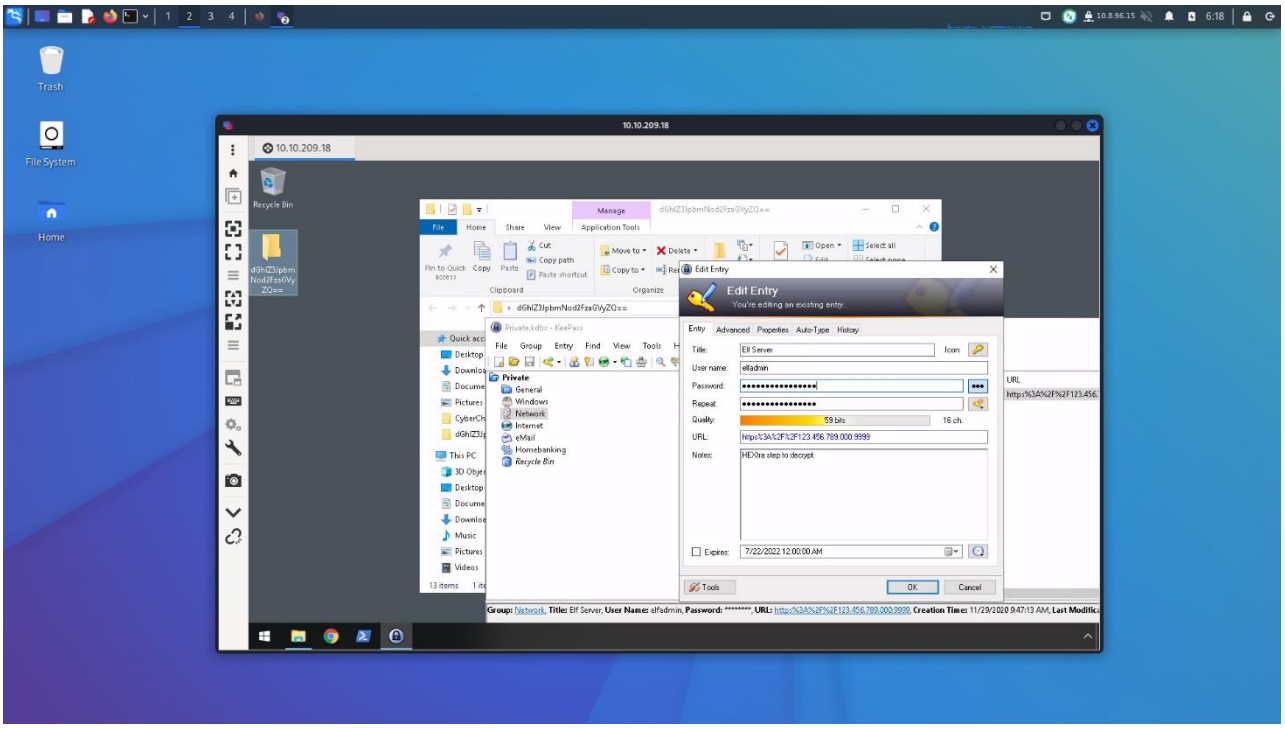


Question 4

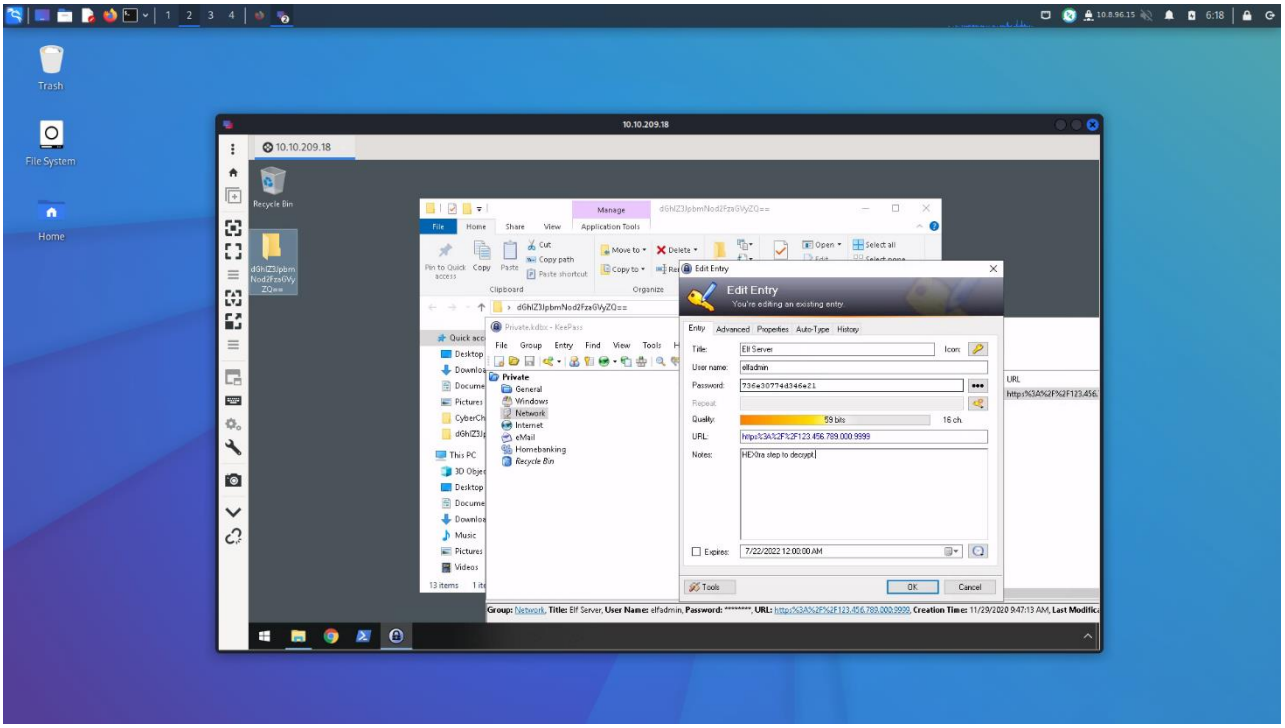
We navigate to the network folder and discover the Elf Server key.



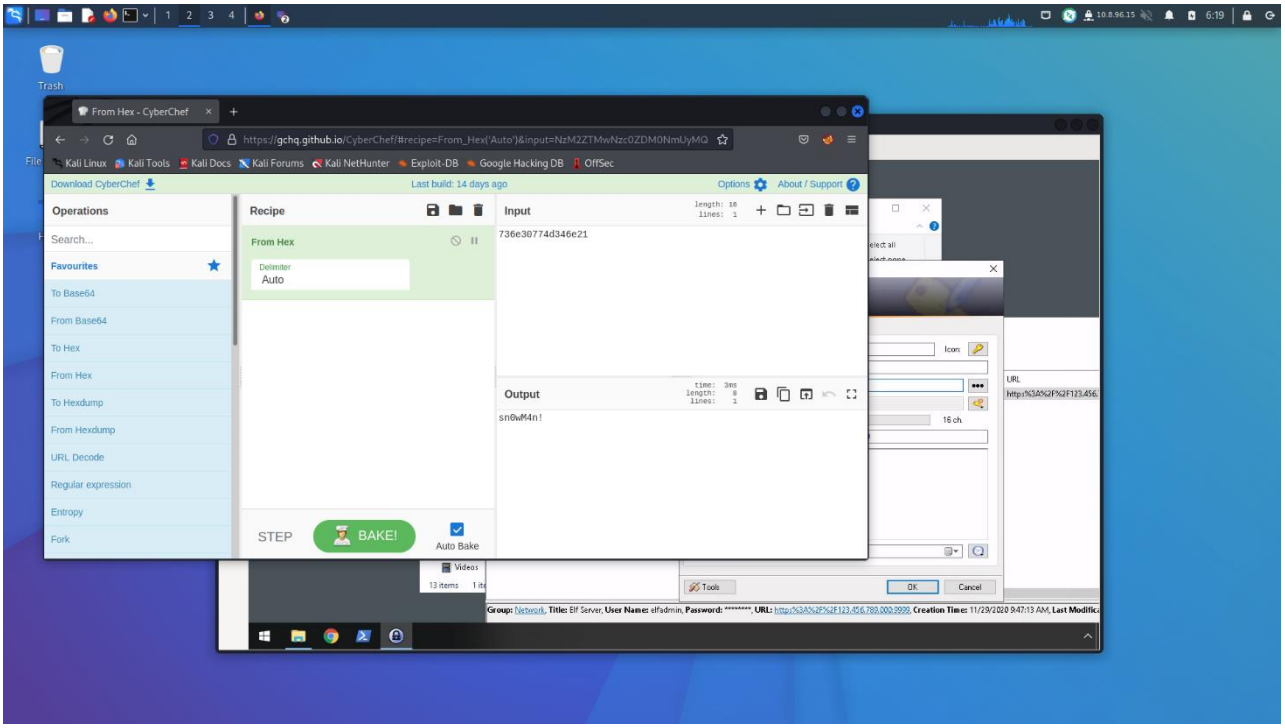
We opened the key.



We clicked the three dot next to the password to reveal the Elf Server password.

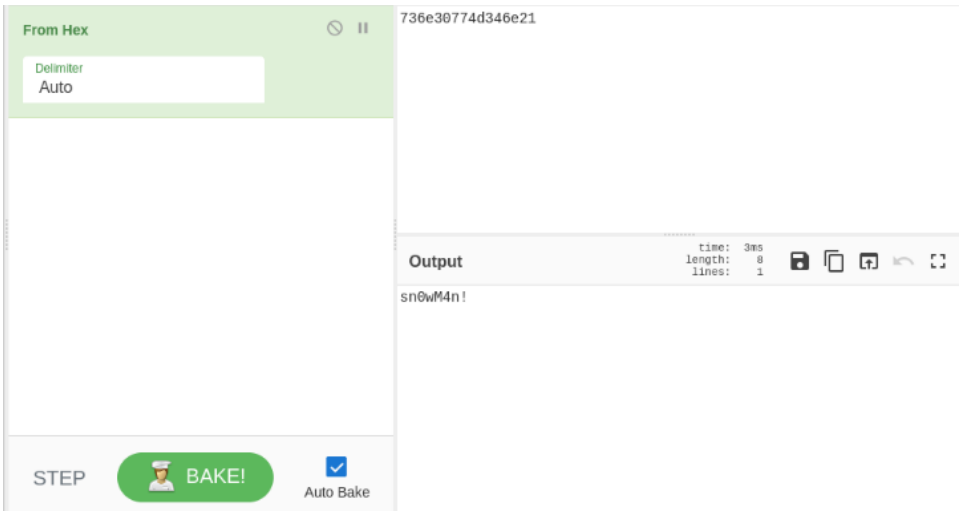


The password was encoded in what looked like hex. We went back to Cyberchef to decode it and obtain the decoded password value.



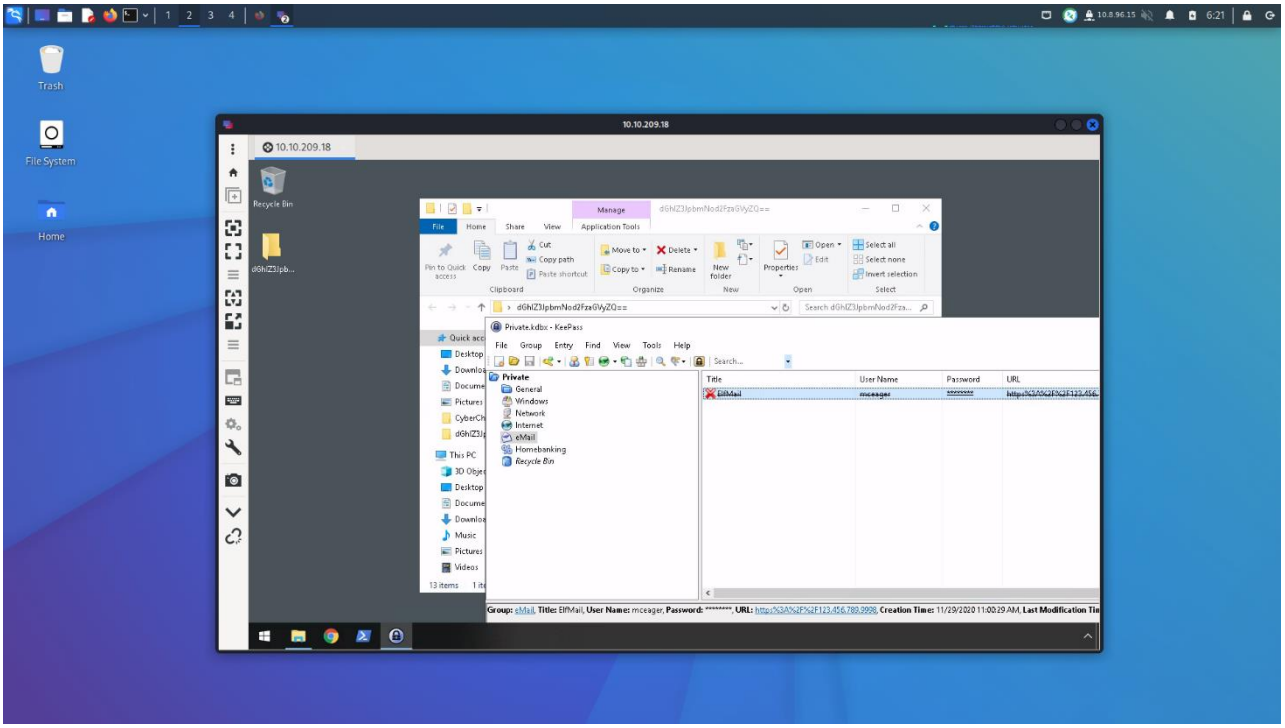
Question 5

Using From Hex recipe and retrieving the decoded password meant that the Elf Server password was encoded using hex.

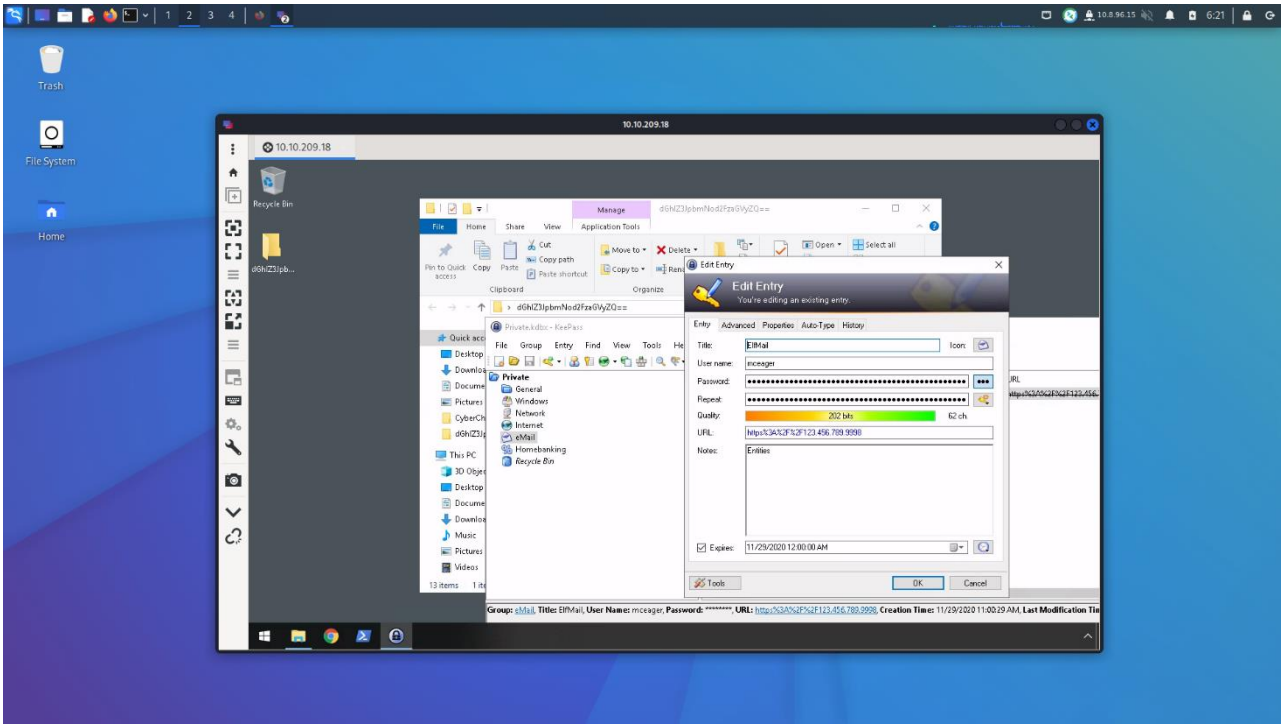


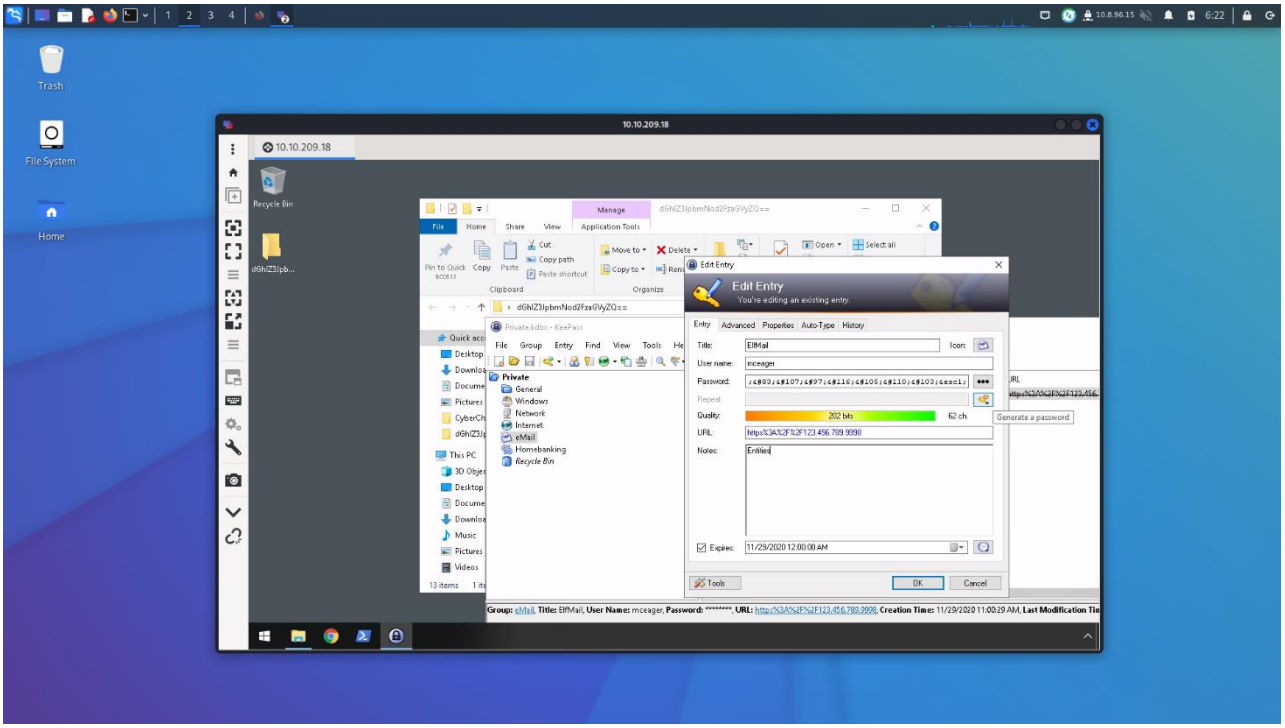
Question 6

We continued exploring other folder and found another key under eMail folder.

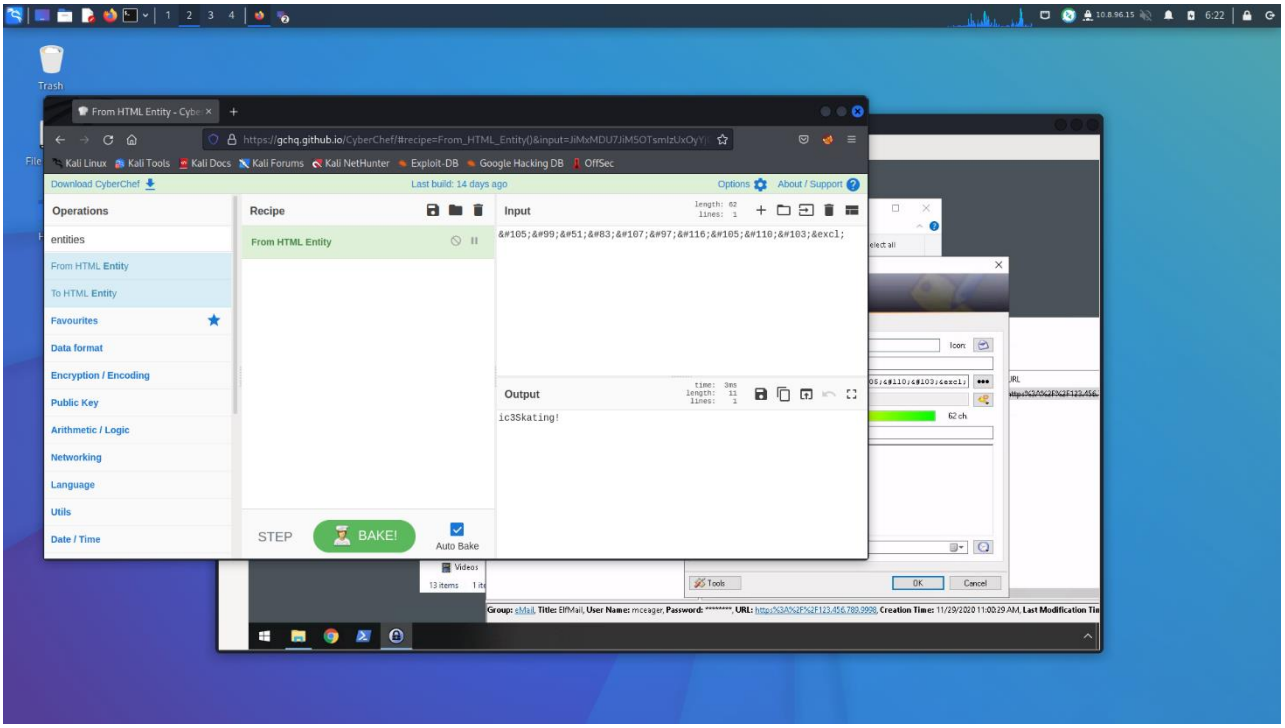


We opened the ElfMail key and revealed the password.



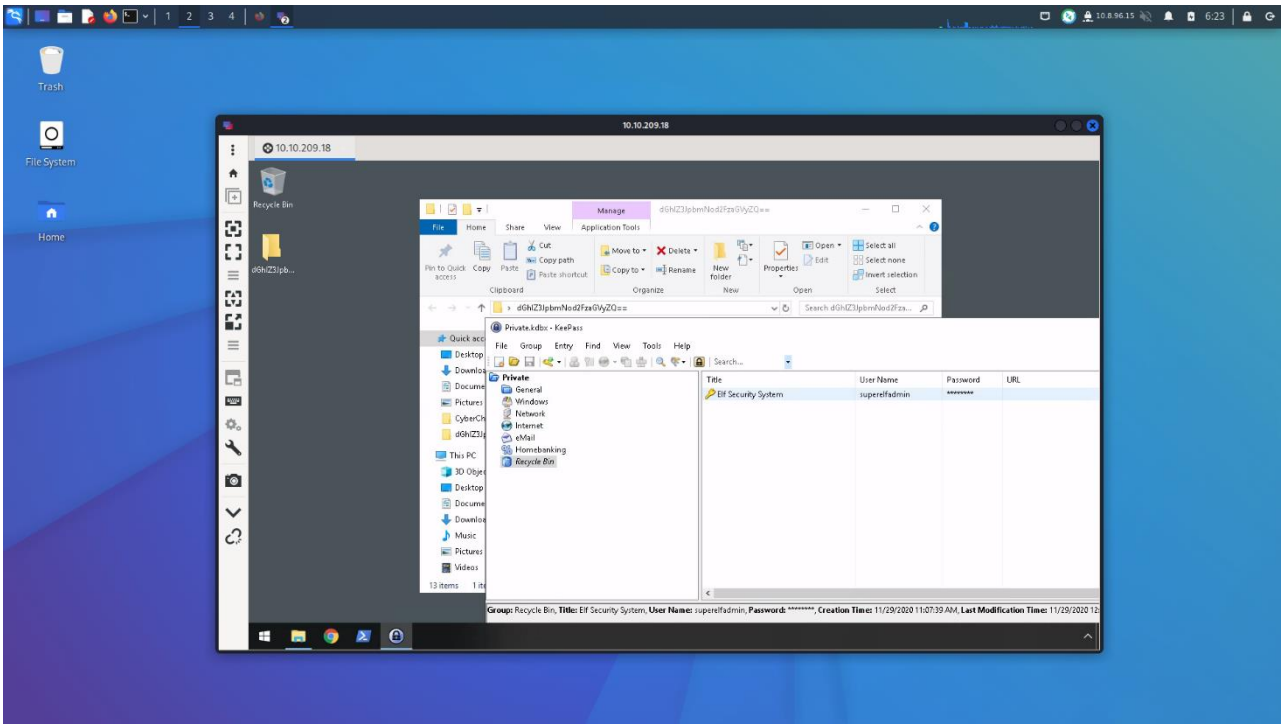


The password was encoded once again. Hence, we went back to Cyberchef. We deduced that it was encoded from HTML Entity after reading the notes left. Once we enter the input, we received the decoded password value in the output.

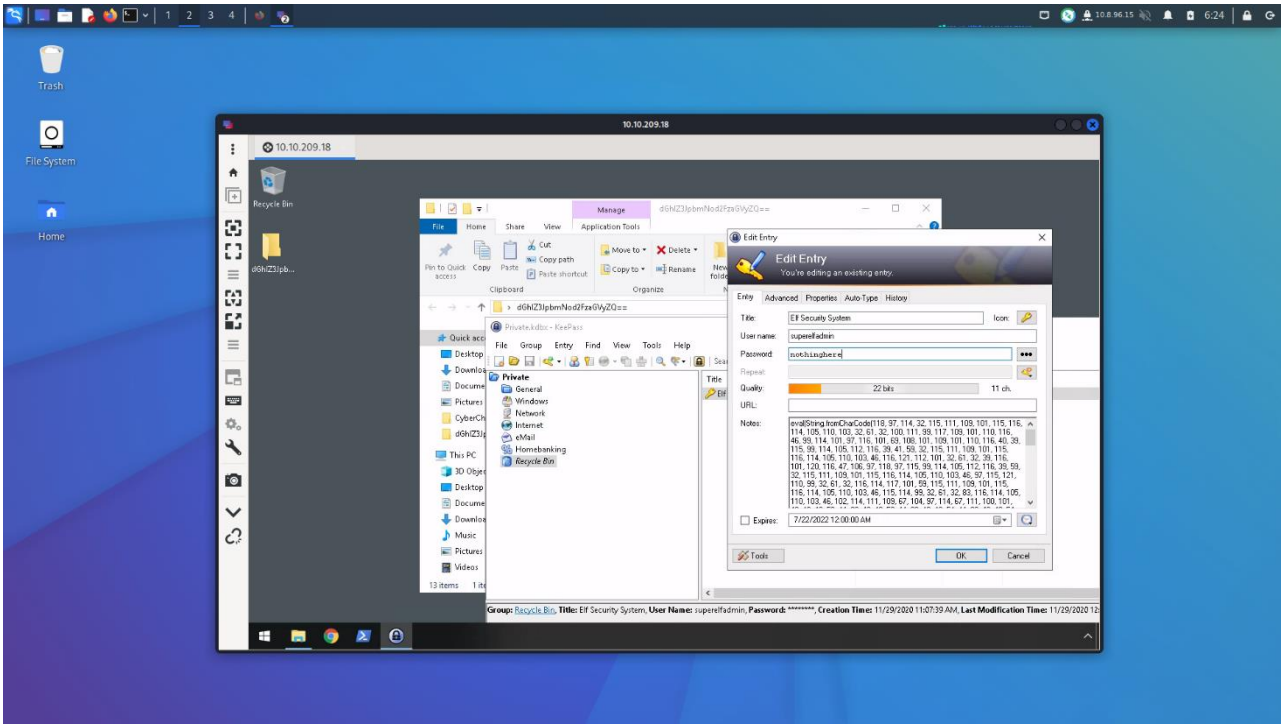


Question 7

We went back to exploring the other folder when we found the Elf Security System key in the Recycle Bin.

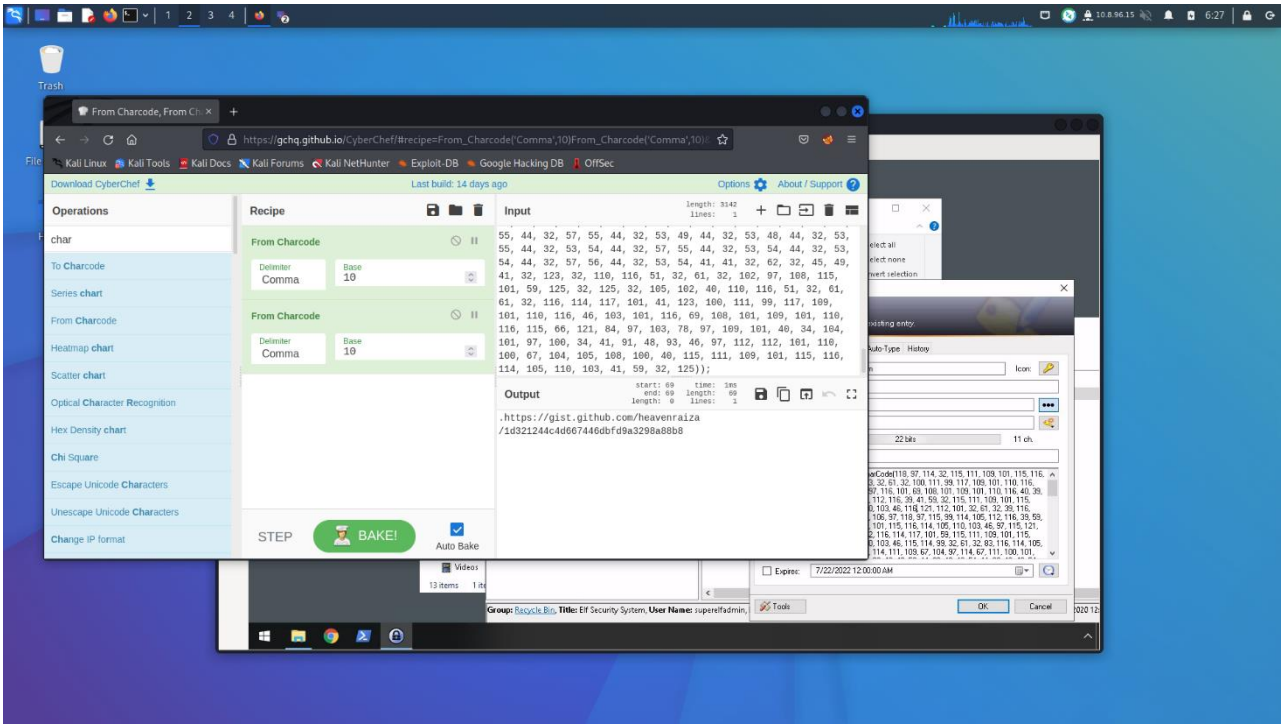


We opened the key, and we found the username and password easily.

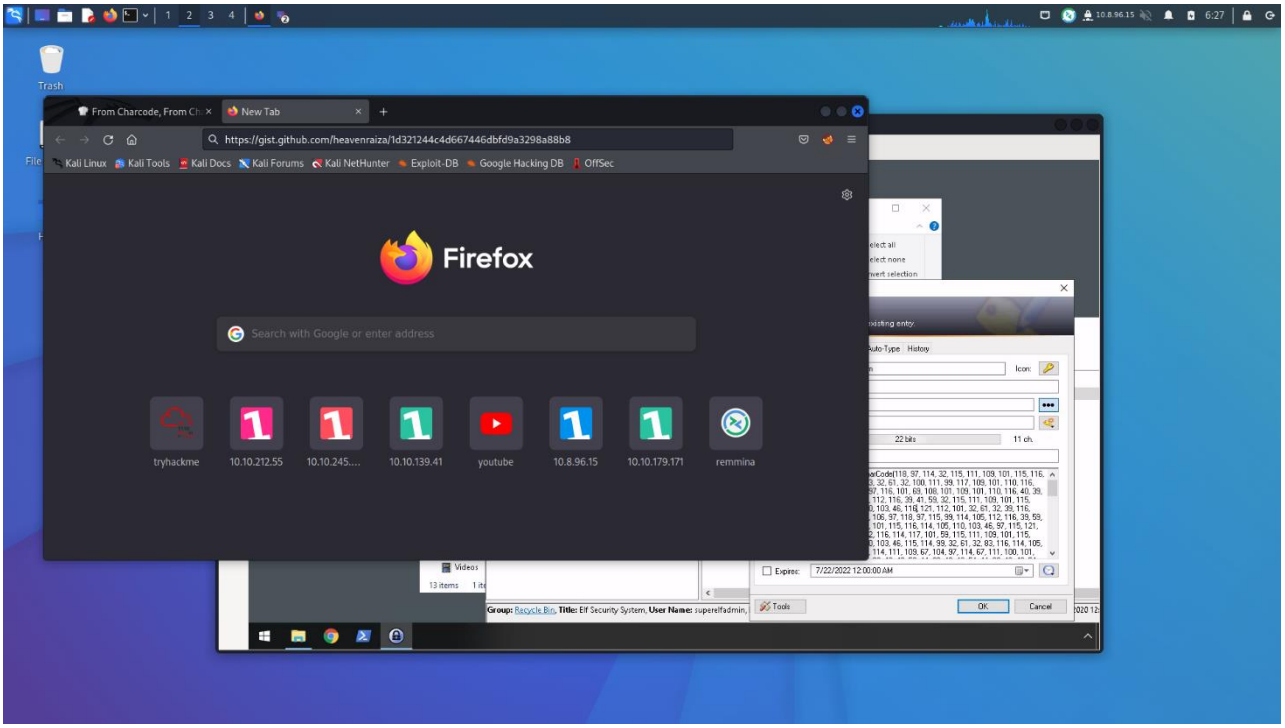


Question 8

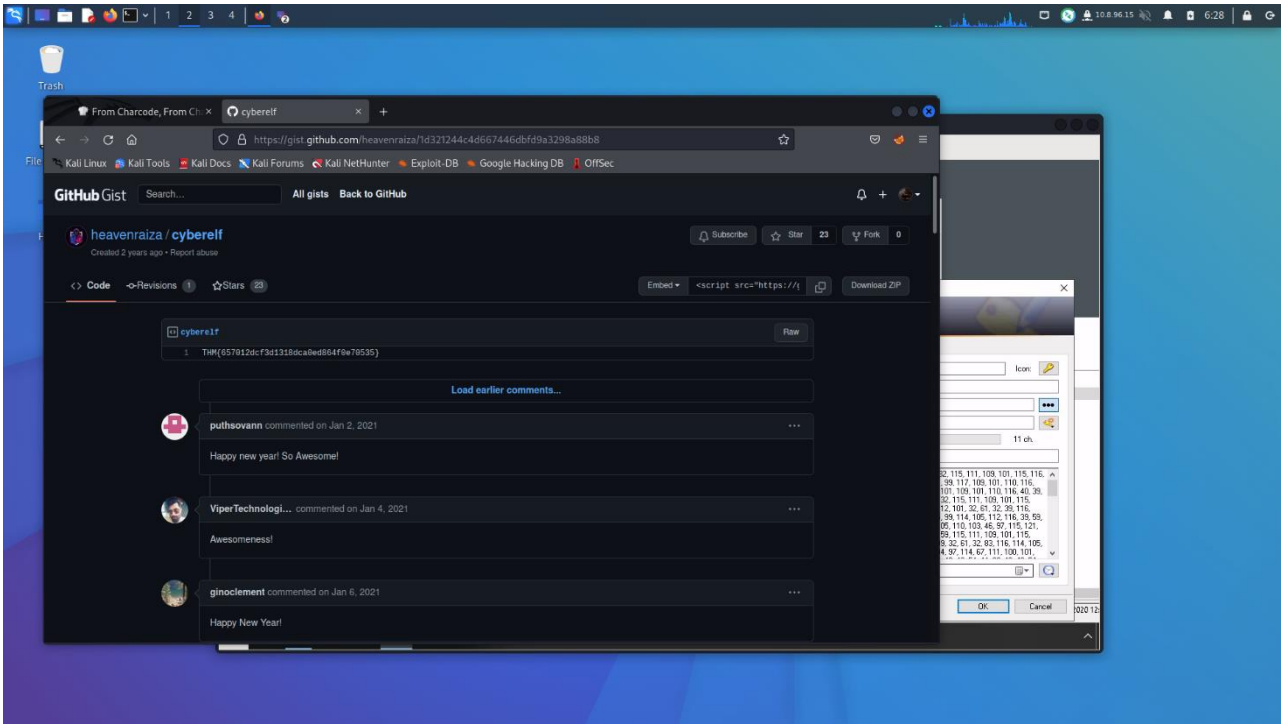
In the notes, we noticed the long numbers stored in it. Once again, we browsed Cyberchef and paste the value into the input. As for the recipe, we add two From Charcode, changed the Delimiter to comma and set the base to base 10.



The output gave us a link.



We opened the link and found the flag.



Thought Process/Methodology:

To start the task, we first connected to the server provided with the credentials for the user account. We accepted the certificate and logged into the remote system. Once connected, we opened the strange looking folder name on the desktop. In there, we found an application named KeePass which store all types of data, including password. However, to access the data within KeePass, we needed the master key password. We took a look at the strange looking file name and decided to try decoding it as it might be a hint to finding the master key password. We browsed Cyberchef to decode the file name. Since we are unsure what the name was encoded into, we picked Magic as the recipe. The output result shows us what we suspected to be the Master Key password. Thus, we entered the output into the Master Password, and we were proven right. We have gained access into the application. We looked at the file name that we have decoded. Under the properties section, we understood that it was encoded with Base64. We went back to KeePass now having access inside. In the Private folder, there was a key named hiya. We opened the key and found a note inside. It gave us no further valuable data, so we continued exploring other folders. In the Network folder, we discover the Elf Server Key. We opened the key and retrieved the password by clicking the three-dot next to the password. We have obtained the password, but it looked like it was encoded into hex. Therefore, we went back to Cyberchef to confirm our suspicion. Once we use the hex recipe, we got the decoded password of Elf Server. We were right that it was encoded with hex. Next, we navigate to eMail folder where we saw ElfMail key. We opened it and the password was encoded once again. Back to Cyberchef, we deduce that it was encoded from HTML Entity due to the hint left in the note. We entered the input and received the decoded password value in the output. Once we retrieved the ElfMail password, we found the Elf Security System key in the Recycle Bin. It seemed like it was deleted by the hacker. We opened the key and found the username and password of the Elf Security System easily. In the notes however, there was a long number stored in it. We gathered that it might be leading us to the flag. We decode the notes left with Cyberchef. As for the recipe, we add two From Charcode, changed the Delimiter to comma, and set the base to base 10. The output showed us a link which led us to our flag.