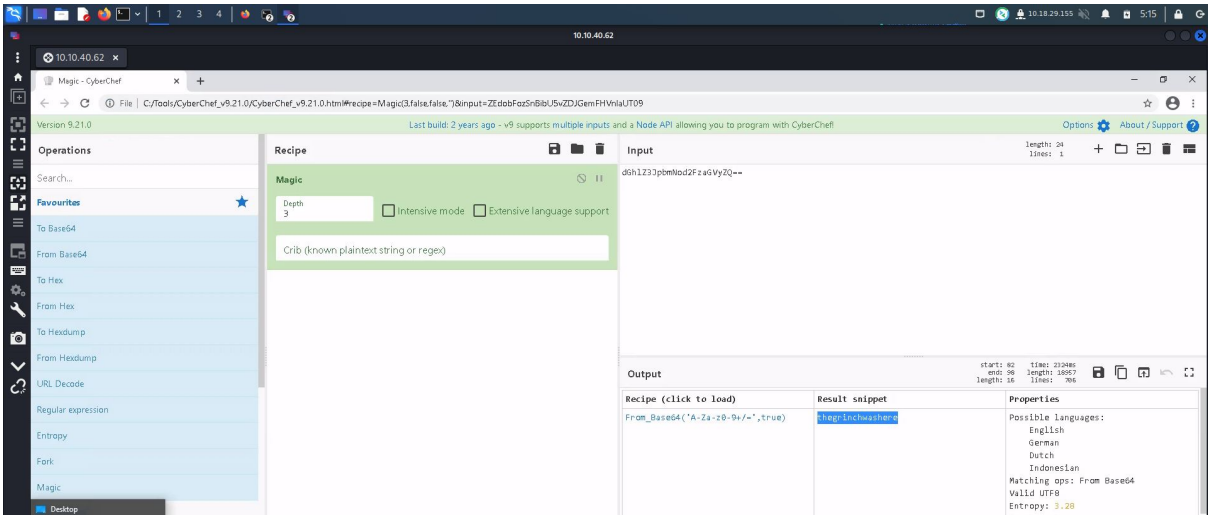
Day 22 - [Blue Teaming] Elf McEager becomes CyberElf

Tool used: kali Linux, Firefox, Remmina, Powershell, Cyberchef

Solution/Walkthrough:

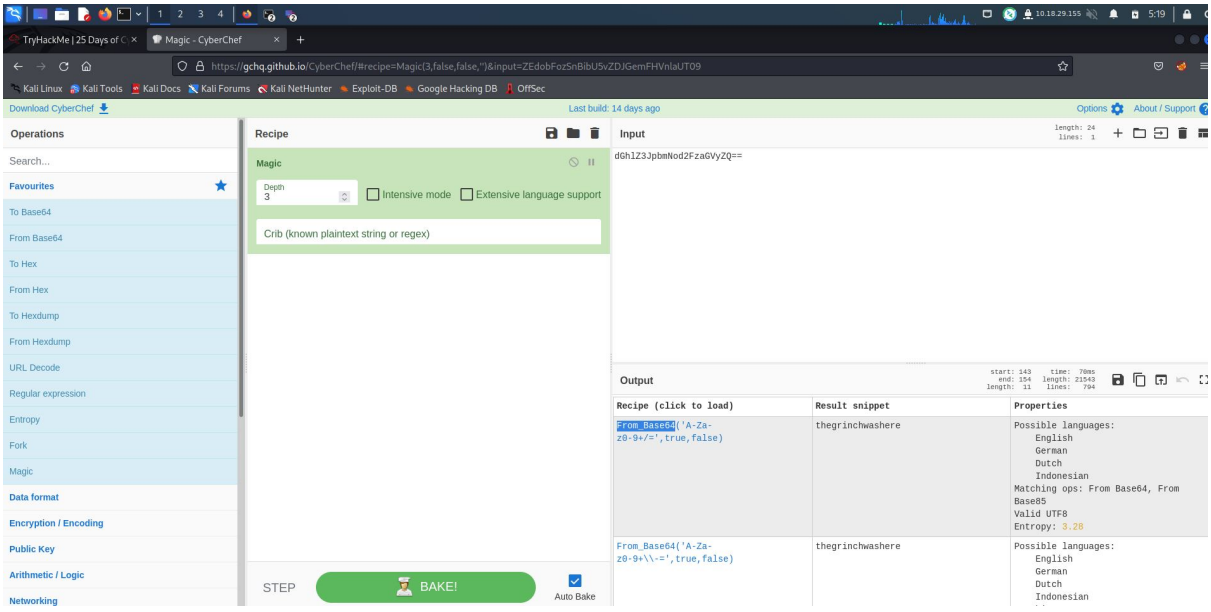
Q1

We log into the remote machine using Remmina. In the machine, we cannot log into the KeePass database. However, we find that there is a suspicious file name as it is in an encrypted code form. We copy out the file name, and use Cyberchef to decode it.



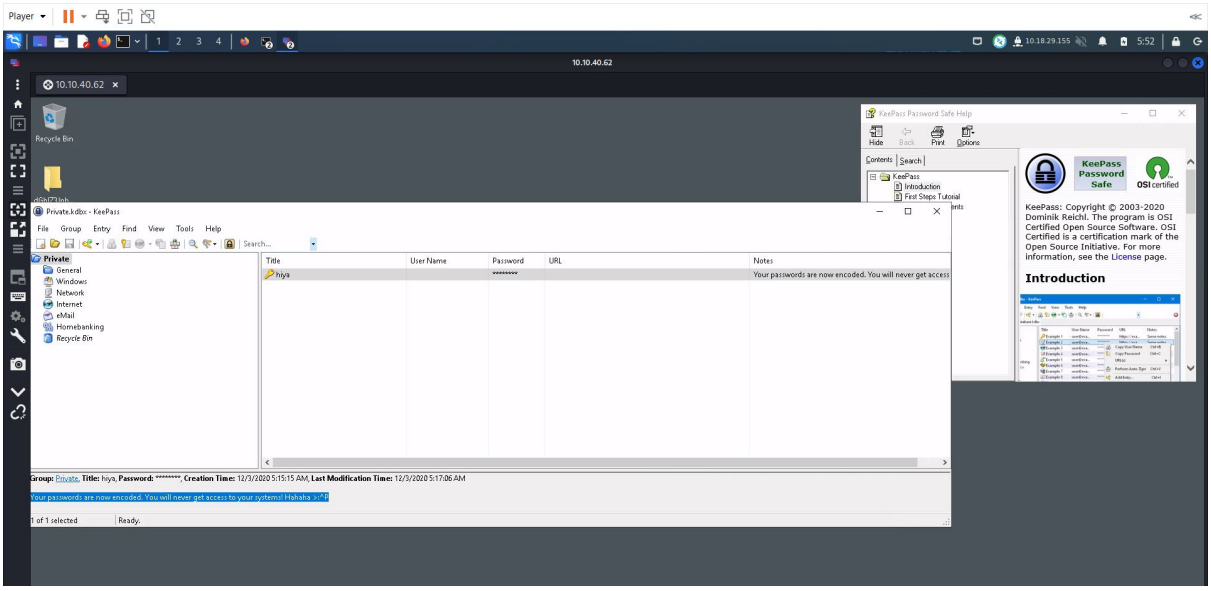
We use ‘magic’ recipe to decode the name, and we get our KeePass database password.

Q2



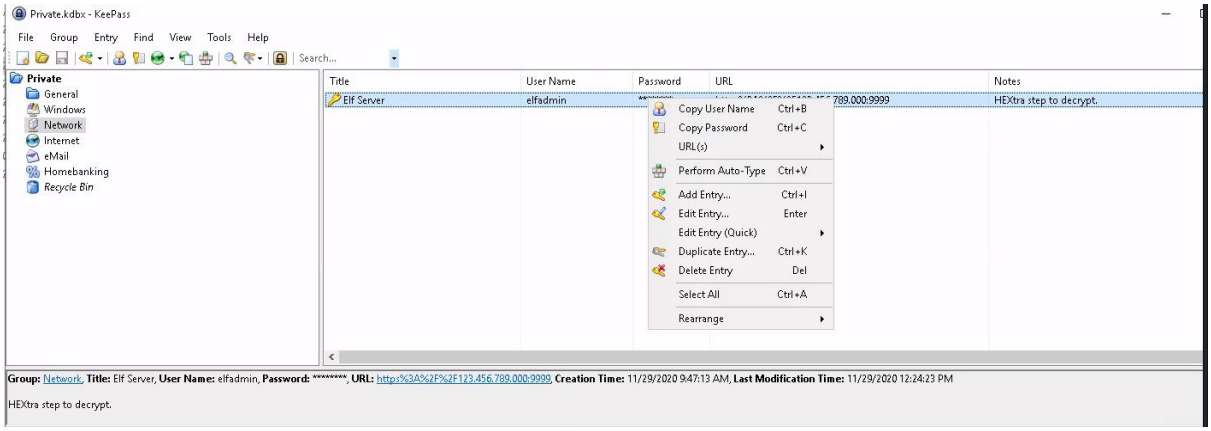
At ‘recipe’, we can find out the encoding method.

Q3

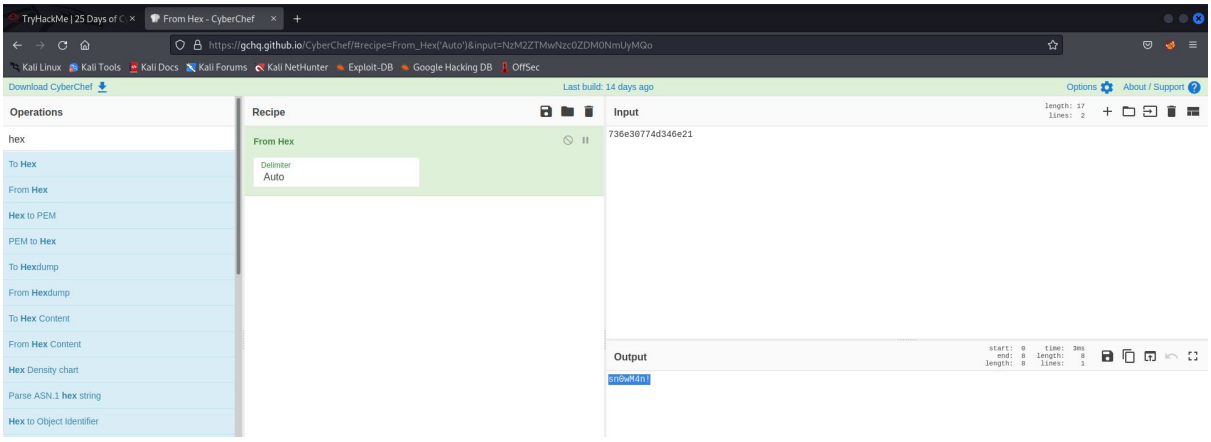


We log into KeePass database. In the first folder, we can see the ‘hiya’ and its note. Copy it.

Q4&Q5

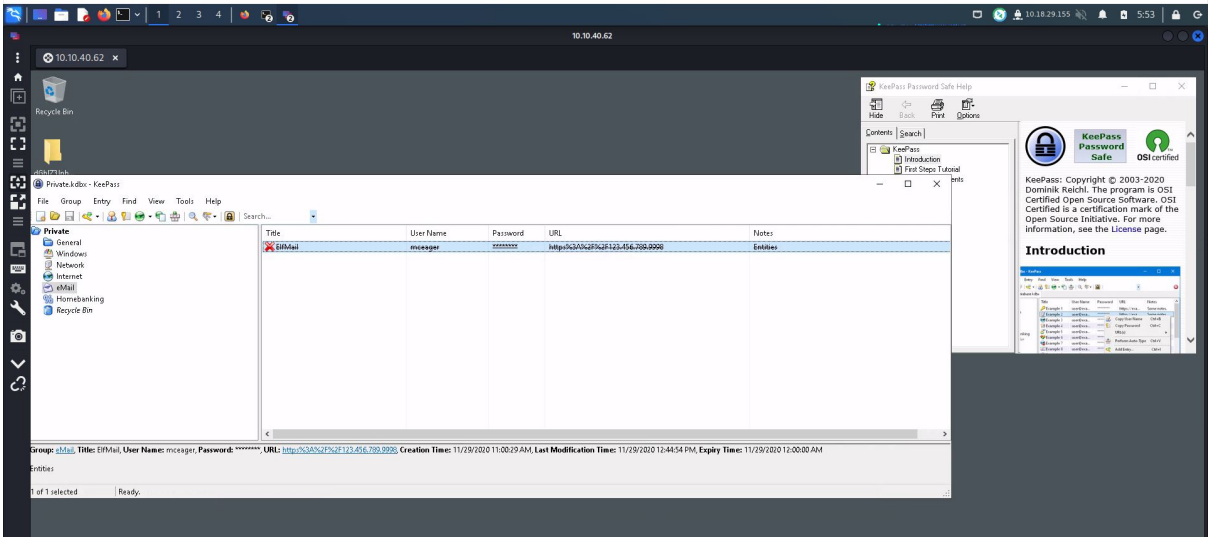


Firstly, we look for ‘Elf Server’ in the KeePass database. At ‘Elf Server’, we have access to the encrypted password and the notes. Copy the password.

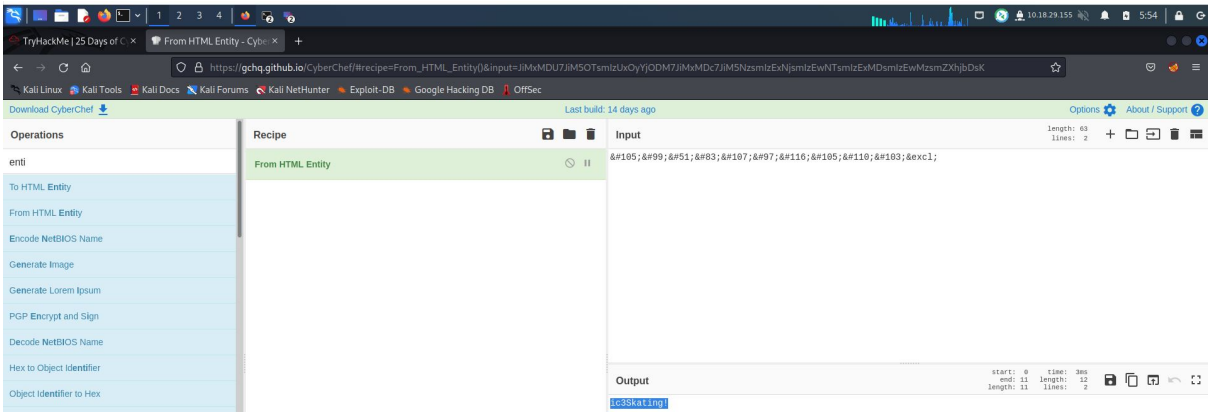


We follow the note to decode the password with ‘from Hex’ operation in Cyberchef. The password is decoded correctly.

Q6

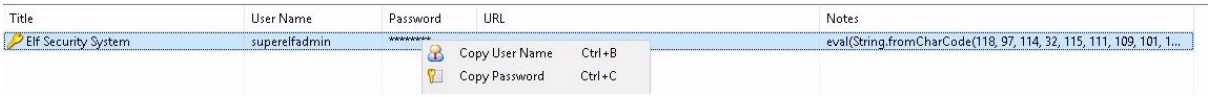


We look after ‘ElfMail’. Then, we similarly copy out the password.



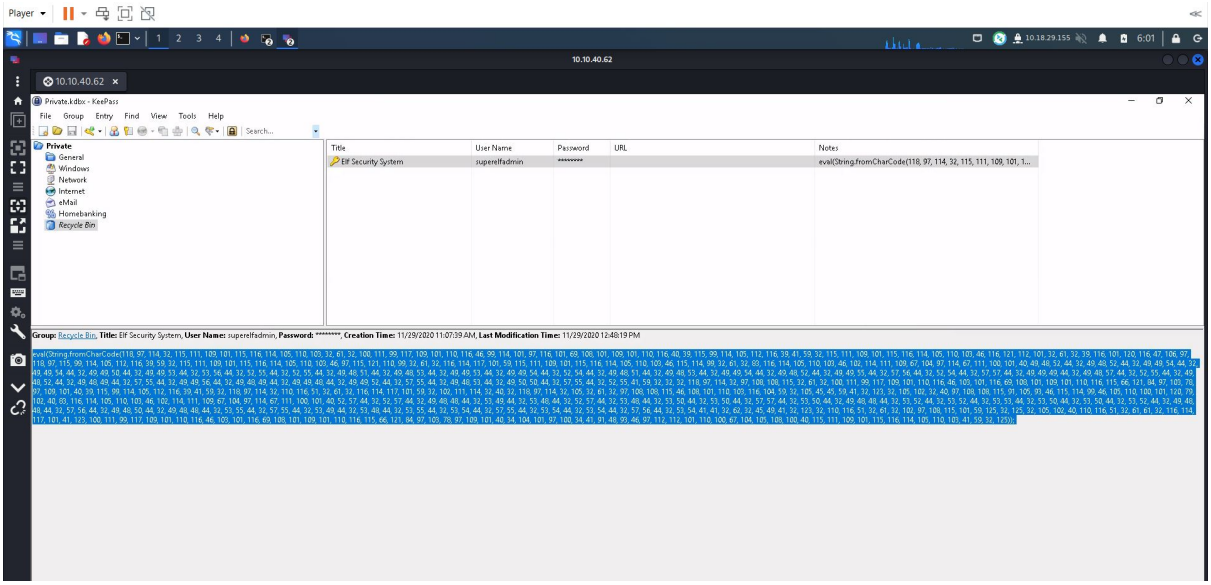
With the note of ‘ElfMail’, we search ‘entities’ in Cyberchef. There are several options of operation for us to utilise. When we use ‘from HTML Entity’ operation, we gain the correct password.

Q7

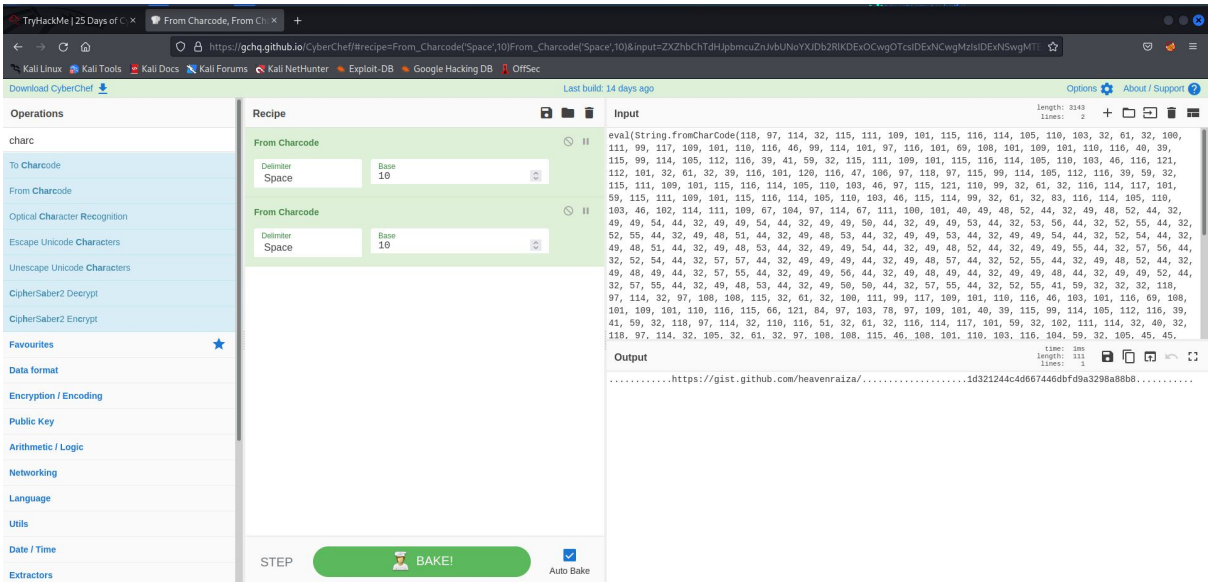


We searched for ‘Elf Security System’. Then, we can see the username and also the password. Copy out both of them.

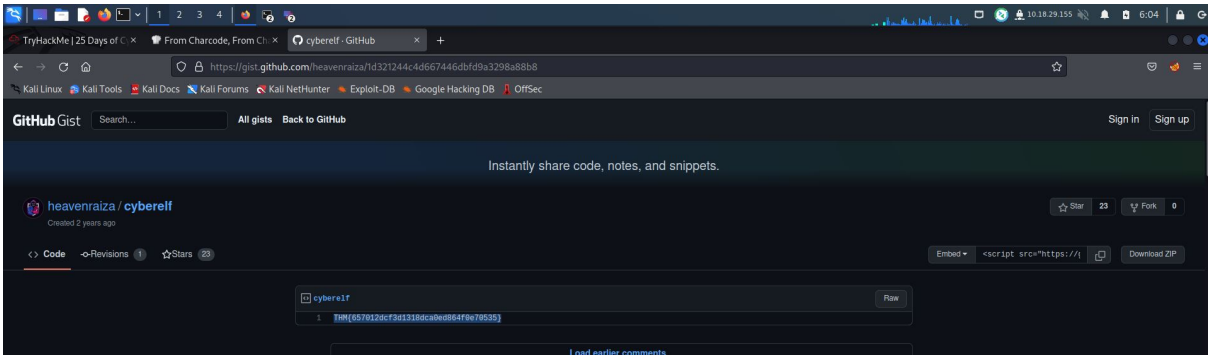
Q8



The password does not have any value for us. However, we notice that the note is suspicious. Therefore, we try to decode the suspicious note in Cyberchef.



From the hint of TryHackMe, we know that we need to use an operation twice a row to decode the password. While also, we notice that the note has a string ‘fromCharCode’. Therefore, we use ‘from Charcode’ twice to decode it, and we get a url.



We use the url. On the website, we find out the flag. Capture the flag.