

PSP0201

Week 6

Writeup

Group Name: ikun no 1

Members

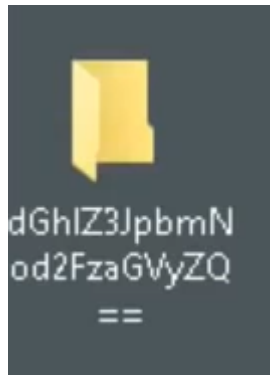
ID	Name	Role
1211102058	Chu Liang Chern	Leader
1211101401	Chong Jii Hong	Member
1211103206	Ng Kai Keat	Member
1211103095	Siddiq Ferhad Bin Khairil Anual	Member

Day 22 - [Blue Teaming] Elf McEager becomes CyberElf

Tool used: kali Linux, Firefox, Remmina, Cyberchef

Solution/Walkthrough:

Q1,Q2.



Download CyberChef [Download](#) Last build: 15 days ago Options [About / Support](#)

To Hex

- From Hex
- To Hexdump
- From Hexdump
- URL Decode
- Regular expression
- Entropy
- Fork
- Magic

Data format

Encryption / Encoding

Public Key

Arithmetic / Logic

Recipe

Magic

Depth: 3 ☐ Intensive mode

☐ Extensive language support

Crib (known plaintext string or regex)

Input

dGhIZ3JpbmNod2FzaGVyZQ==

Output

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

STEP **BAKE!** Auto Bake

The folder name looks suspicious. Try copying the name and decrypting it with cyberchef.

Q2. Base 64 is stated at cyberchef.

Q3.

Edit Entry

You're editing an existing entry.

Entry | Advanced | Properties | Auto-Type | History

Title: Icon:

User name:

Password:

Repeat:

Quality: 47 bits 16 ch.

URL:

Notes:

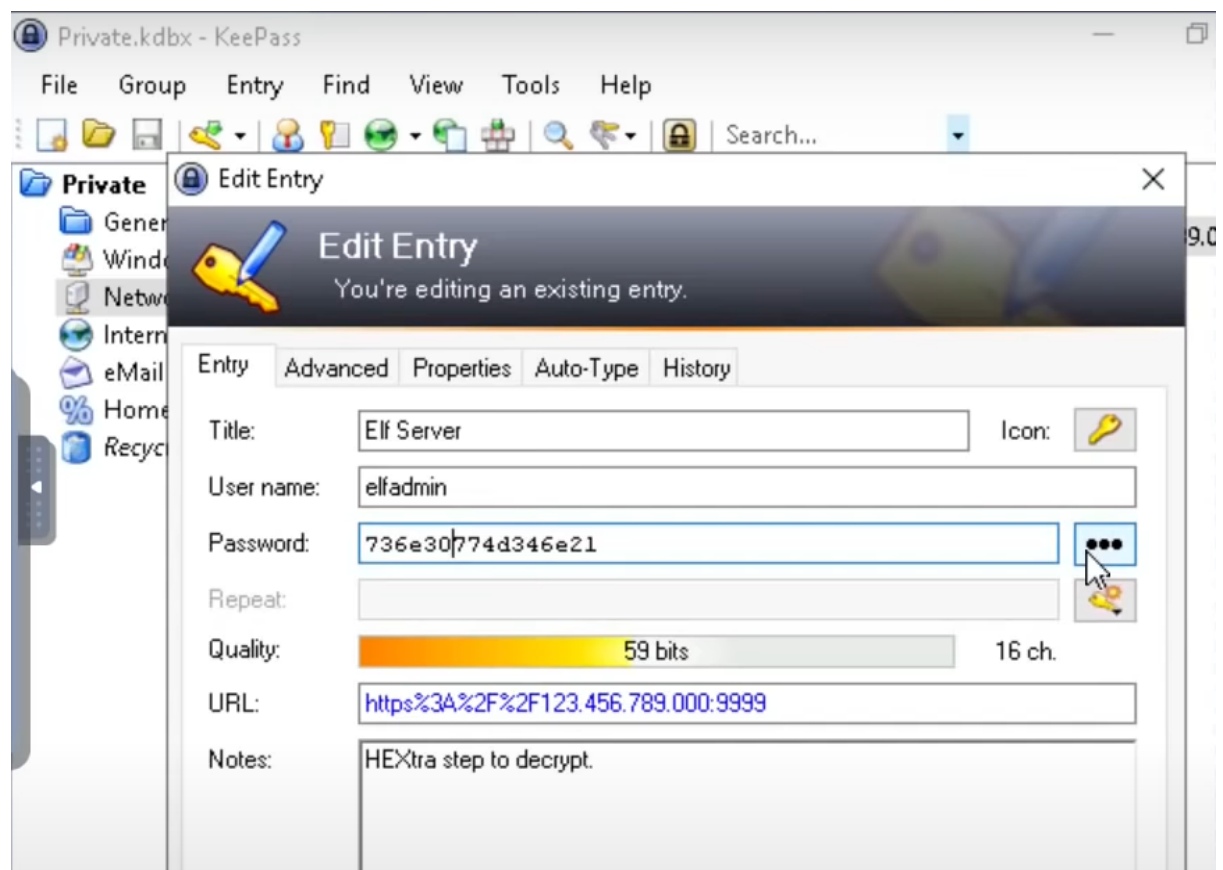
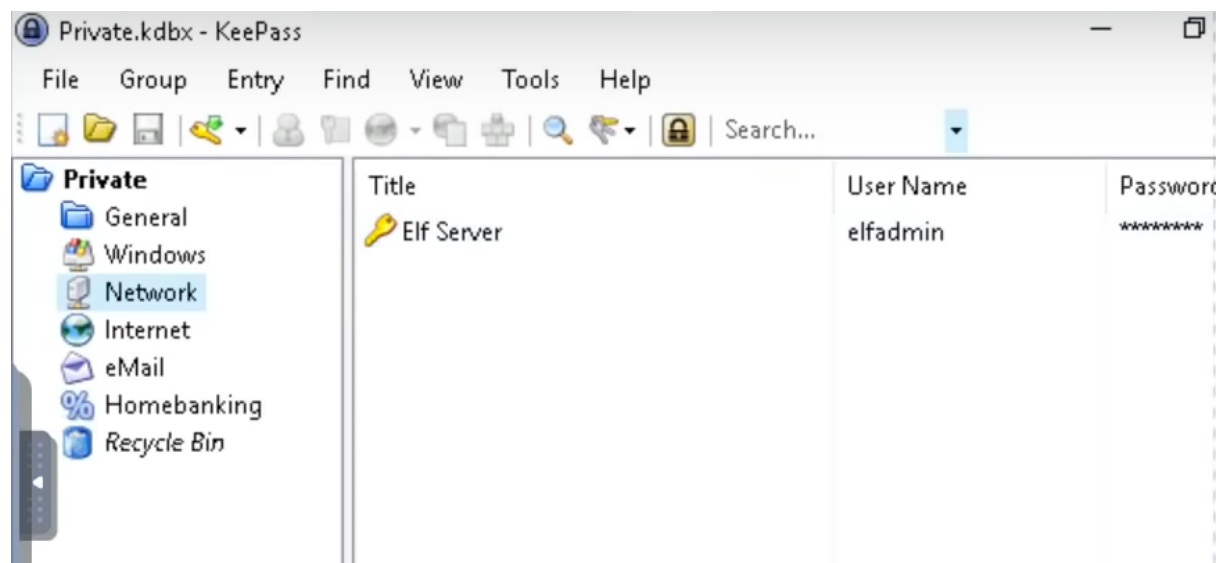
Your passwords are now encoded. You will never get access to your systems!
Hahaha >:^P

☐ Expires:

Tools OK Cancel

Login into KeePass. Right click and choose the edit option. The notes can be found.

Q4,Q5.



Input	length: 1
-------	-----------

736e30774d346e21

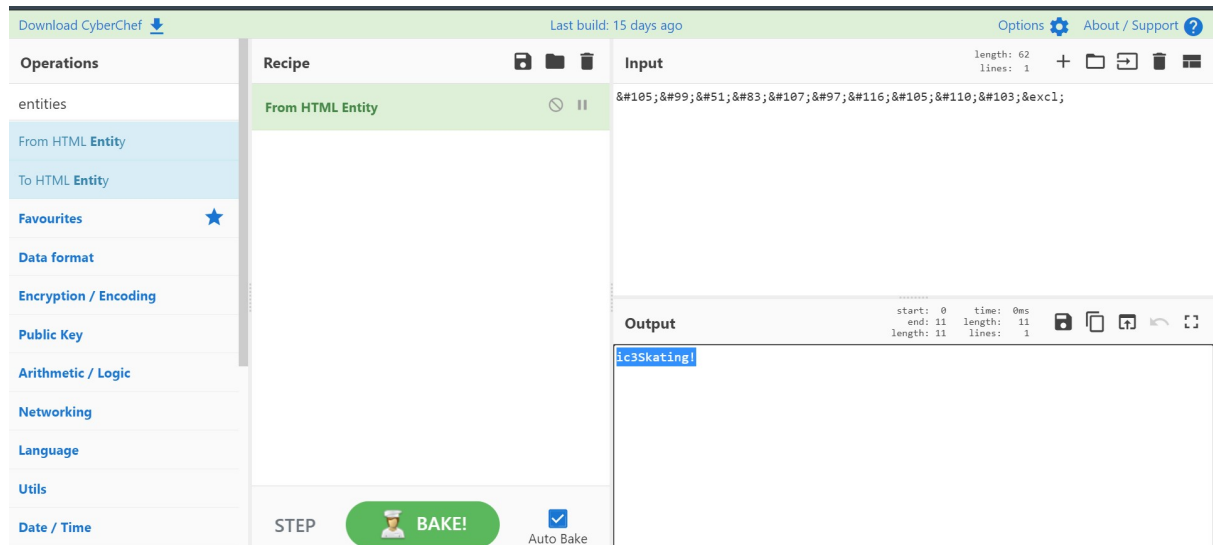
Output	start: 0 ti end: 8 leng length: 8 lin
--------	--

sn0wM4n!

Q4. Explore around Keeppass. Choose edit and find the password. Copy the password and paste it into Cyberchef to decrypt it. Change the filter to Hex as stated in the notes of the password. The password can be found.

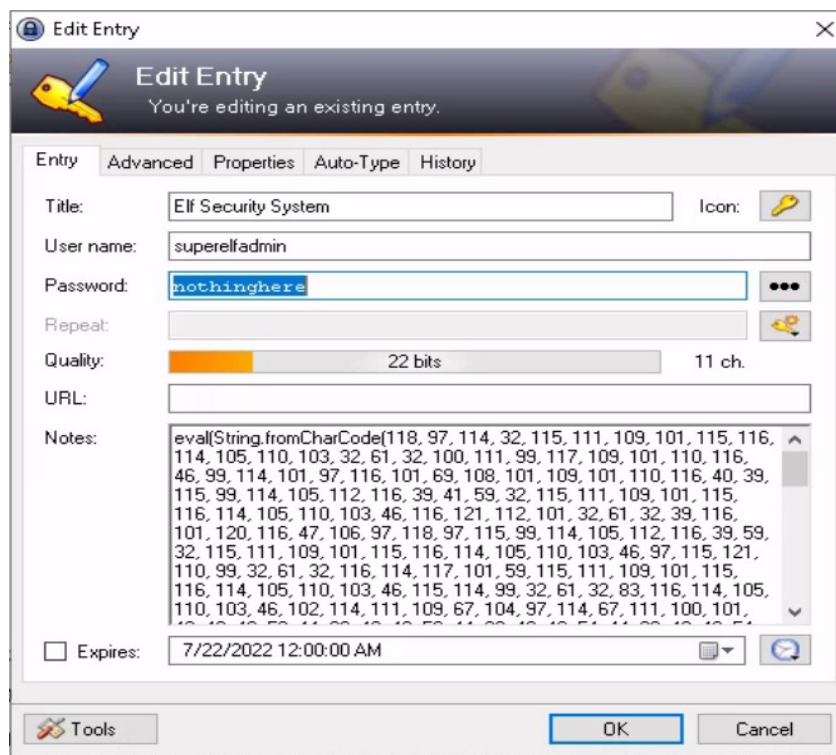
Q5. From the notes of the password we can find out that it is a HEX.

Q6.



Find out the password in Elfmail. Choose the edit options and copy the password. Paste it into Cyberchef and change the filter to HTML Entity. The output then can be found

Q7,Q8.



Q7.The username and password can be found easily by looking at the edit options of the ELF Security System.

Q8. Copy the notes from the ELF Security System and paste it into CyberChef. Decode it twice and the link that contains the flag can be found. Click at the link and capture the flag.