So, we got a flag.enc file and the challenge is also reverse engineering, so I expect to find some sort of binary somewhere.

As a result, I decided to look through the HTTP objects, and the last one is a file called peanutcrypt. But it's not a binary. What is it?

```
┌──(kali㉿kali)-[/tmp/VMwareDnD/SUT8JY]
└─$ file peanutcrypt
peanutcrypt: Byte-compiled Python module for CPython 3.8, timestamp-based, .py t
imestamp: Mon May 10 14:55:50 2021 UTC, .py size: 2826 bytes
```

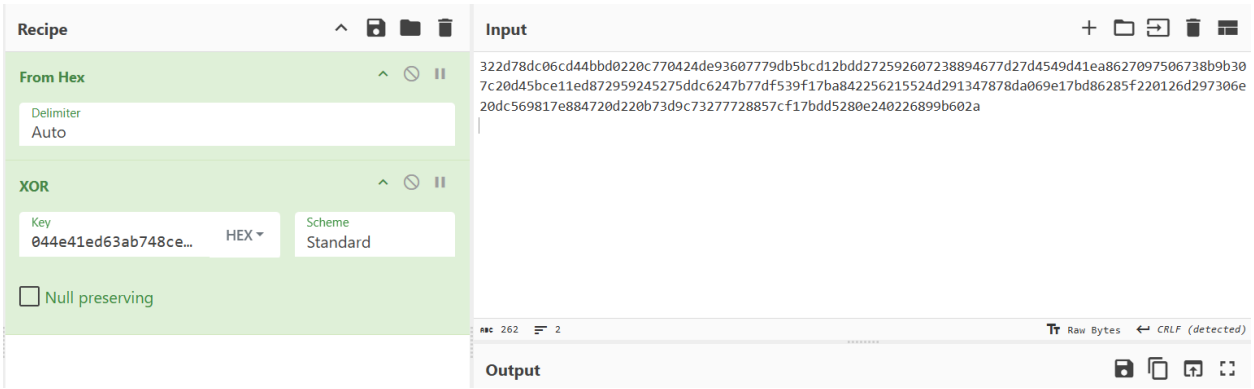
Oh, it's a pyc, my bad.

I changed its extension and decompiled it with pylingual.io

Reading through it, it looks like some ransomware written in python.

I any case, the flag was encrypted using aes cbc, so we need to recover the key and iv. These were randomly generated, and sent to a remote server, using port 31337. Using this info I assumed those must be in the network capture, so I came back to it and applied the filter "tcp.port == 31337"

This led me to a tcp stream which I followed, printed the conversation in raw and opened up cyberchef:



I also converted the super_secret_key to hex and used it in the xor. This way, I got the key and iv!

Now getting the flag is easy, I just told chatgpt to make me a decrypt script using that key and iv (and the aes cbc mentioned) and I quickly got the flag.

Made with love by: AndreiCat