

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.

In 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:

The screenshot shows the CyberChef web interface. On the left, the 'Recipe' panel is active, showing a 'From Hex' step with 'Delimiter' set to 'Auto'. Below it is an 'XOR' step with a 'Key' field containing the hex string '044e41ed63ab748ce...', a 'Scheme' dropdown set to 'Standard', and a 'Null preserving' checkbox. On the right, the 'Input' panel displays a long hex string: '322d78dc06cd44bbd0220c770424de93607779db5bcd12bdd272592607238894677d27d4549d41ea8627097506738b9b307c20d45bce11ed872959245275ddc6247b77df539f17ba842256215524d291347878da069e17bd86285f220126d297306e20dc569817e884720d220b73d9c73277728857cf17bdd5280e240226899b602a'. The 'Output' panel at the bottom is empty. The interface includes various icons for saving, deleting, and toggling steps.

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**