W1seGuy

Recover two flags via an XOR-based encryption challenge running on port 1337.

When you download the task files, you'll see a Python script that:

1. Listens on TCP port 1337 when run

2. Generates a random 5-character key composed of letters and digits.

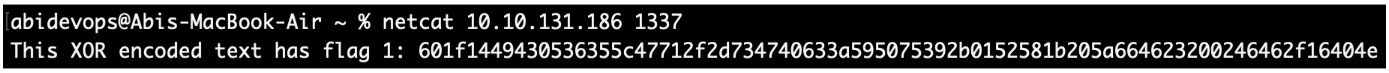
3. XOR-encrypts a hard-coded flag ("THM{thisisafakeflag}") with the key, cycles the key over the flag length, and then hex-encodes the result.

4. Sends that hex-encoded ciphertext (Flag 1) to the client.

5. Prompts the user to submit the key. If it matches, the server reveals Flag 2 (loaded from flag.txt) .

My IP Was - **10.10.131.186 (** I used OPENVPN & nectar to connect the target machine to my pc)

- Command - nc 10.10.131.186 1337

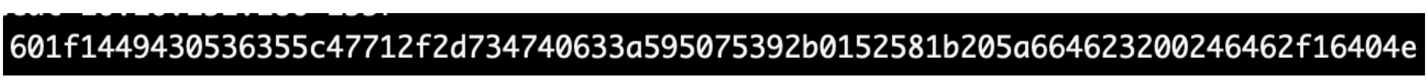


```
abidevops@Abis-MacBook-Air ~ % netcat 10.10.131.186 1337
This XOR encoded text has flag 1: 601f1449430536355c47712f2d734740633a595075392b0152581b205a664623200246462f16404e
```

Recover the key prefix

- Grab the first 4 bytes of the ciphertext.

- XOR them with "THM{" to recover the first 4 key characters:



```
601f1449430536355c47712f2d734740633a595075392b0152581b205a664623200246462f16404e
```

For eg: my text was - **601f1449 (in hex)** and the Key was - **4WY2**

Brute-force the final character

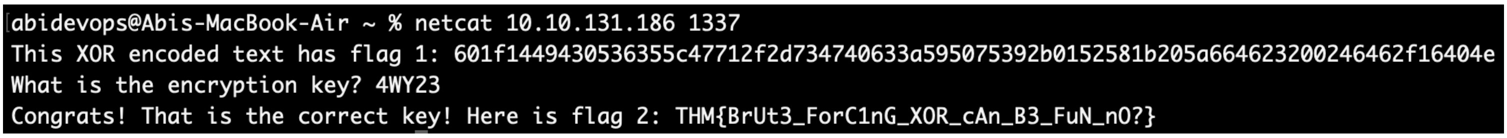
- The key is exactly 5 characters. Brute-forcing the last character (62 possibilities) gives you the complete key.

- Check by decrypting the ciphertext and verifying it:

- Starts with THM{

- Ends with }

The final key I got was - **4WY23**



```
[abidevops@Abis-MacBook-Air ~ % netcat 10.10.131.186 1337
This XOR encoded text has flag 1: 601f1449430536355c47712f2d734740633a595075392b0152581b205a664623200246462f16404e
What is the encryption key? 4WY23
Congrats! That is the correct key! Here is flag 2: THM{BrUt3_ForC1nG_XOR_cAn_B3_FuN_nO?}
```