Writeups CTF-2022

Simple Crypto

Basic Things 2: Decode base 64

Basic Things 1: Decode unusual Morse Code, use <https://en.wikipedia.org/wiki/Morse_code>– Timing

Basic Things 5: Decode URL, use <https://en.wikipedia.org/wiki/Percent-encoding>,<https://www.urldecoder.org/>

Basic Things 3: Decode ASCII code, use <http://www.unit-conversion.info/texttools/ascii/> , then you have a bite string, this is multibyte XOR. You can install Cryptool 1 on Windows, open the file with this text, click “analisys – Symmetric Encryption – ciphertext-only – XOR/Vernam”, get a graph of autocorrelation and than get a key and decrypt a message.

Strange Thing 2: Just copy all text and decode base 64 many times

Crypto

Basic Crypto 1: Decode Caesar cipher, you can use online decoder <https://planetcalc.ru/1434/> or write your own

Basic Crypto 2: This is RSA <https://en.wikipedia.org/wiki/RSA_(cryptosystem>) write python code and use it

Basic Crypto 3: Decode base 64 and then it is substitution cipher, you can use frequency analisys of the text, or notice that in parentheses the combination of letters reminds CTF\_FLAG{….} and then look at the little words.

Advanced crypto 1: This is XOR, it can be decoded by Cryptool, like in BasicThings3.

OSINT

Coffe Time: Search the photo in google and found in the google maps the location wt were loking for. This is Costa Coffee.

Hiking Trail: This is a photo of lego, you can search this proto in google and find a fwitter account. Than you can see in the hint another twitter account in which also mentioned Lego. If you scroll if further, you can see the post with sign “Lets go hiking” and the geolocation mark we were looking for.

Park: We can also search this photo in google and find out that it is one of the famous skyscrapers of China, its name and location, find this area on the google map and compare it with the damaged map that you also have. After all you can see Hexi central Park, which was a flag.

Exhibition: You may search the photo in google and find a this bird’s name and that it is a symbol of Faroe Islands. And a name of the man, who made it. And than you can find on the forum that he mentioned that he mentioned at the forum that the first Lego exhibition will take place in the Faroe Islands in Torshavn. That is a flag.

Windy Island: Search photo in google did not give interesting results, unless, we can see that maybe it is somewhere in northern Europe if you look at the architecture style. You can search in google “Windy island with sheeps” and found The Faroe Islands. Then you can pick up the letters and found that it is a hotel “Zarepta”. That was what we were looking for.

Stego

Stego 1: We need to open zip archive, where was our flag.

Stego3: There is a png picture and we need to decipher the secret message. To do this, we used a special online application <https://aperisolve.fr/> that can give us picture data. We find a passwors in the section “String” and than use <https://www.pelock.com/products/steganography-online-codec>to decode hidden message.

Misc

Lunch: Very similar to the previous one, we use the same online services.