KopiCTF - k4n4s4i

Hello! Welcome to the k4n4s4i challenge for KopiCTF!

Group Members

- Randolph Wong (1001043)
- Nigel Leong (1001095)
- Tan Shun Yu (1001171)
- Leong Keng Hoe (1000957)

Scenario

Your four best friends have been meeting a lot in secret recently. With some clever sleuthing on your part, you have found that they have created a website which requires four aliases to login. Further online shenanigans have yielded some potential clues for finding out the four aliases.

Mini-challenge 1: Cherry Packet(s) (Forensic)

Cherry had been talking about how she had come up with her own protocol (using UDP) for logging into GreatMail. As a master hacker, you have managed to capture some of her packets in transmission, saved as `sniffed.pcap`. Perhaps there might be some important information in there.

Mini-challenge 2: Alice’s Present (Crypto)

Being the hacking prodigy that you are, you have hacked into Alice’s Github account and found a repository named `Secret`. The folder contains the following files: `present.py`, `pair`, `ecb.py`, and `not_a_diary.e`.

You recognise `present.py` and `ecb.py` from the security lab that you and Alice have did together. However, you also notice that she has modified one line of code:

```
sbox=[i for i in range(16)]
```

What was Alice thinking? The whole algorithm is now linear! You immediately recall from your security lecture that this means you can express a ciphertext as a linear combination of the message and round-keys, so the information in `pair` will come in handy. Your genius hacker instincts also tell you that `not_a_diary.e` is encrypted in ECB mode using `ecb.py`. With this, you can easily decrypt the diary to find Alice’s secret alias.

Mini-challenge 3: Monty’s Secret Website (Steganography)

By intercepting some messages exchanged between your friends, you have managed to find out that Monty owns a website which requires a password to access. Knowing Monty’s forgetfulness and resourcefulness, he would likely hide his password in plain sight. With that in mind, you work at hacking into his secret website to find the alias that he is using.

Mini-challenge 4: Billy’s Cipher (Crypto)

Billy had accidentally uploaded a text file onto your MeChat group chat. The file, named `billysecret.txt`, contains a short message that has been scrambled, likely using a transposition cipher.

From experience, you know that Billy uses keys which are all lowercase alphabets and do not contain duplicate characters. His message length is also always divisible by his key length. Decrypting this message should give you what you’re looking for.