Category:

Forensics

Name:

Can you give us the secret

Message:

Find the flag from the file.

Objective:

Extract client secret value, used to post blog from the memory dump file.

Instructions:

The dump is a program that waits for a windows OS command at port 8553.

When command is received, the program executes and post the result to "https://acsgforesicc.blogspot.com/"

The flag to this challenge is client secret value in the API token to post data to the blog.

flag is divided into 3 parts of string and then encoded with base64.

Thus if you could find those base64 string values then simply concatenating and decoding should lead to the flag.