Segurança de Dados - Assignment 1

Pedro Malainho PG61005

1. Question 1

In my code attached there is a function that creates the “file_shadow” if it doesn’t exists, and if it already exists, it simply prints “file already exists” - although this part is currently commented out. The basic functions on this program are to protect, update and verify files that exist or are going to be added to the “file_shadow”.

To do this, the program can be started in three different modes: Protect; Update; Verify

- **Protect:** Each hash has a randomly generated 16-byte salt. After generating the salt, I use a function called secure_sha256 that takes as input the absolute path and the salt to produce a hash. Then, it is saved in the file as “path:hash_value:salt”.
- **Update:** I load the file_shadow into a dictionary, generate a new hash_value with a new salt, and save it into the file_shadow, overwriting the previous one.
- **Verify:** Once again, I load the file_shadow into a dictionary and receive a list of paths. For each item in this list, I take its absolute path and check if it exists in the file_shadow. If it does, I store both the hash_value and salt in separate variables. I then use the secure_sha256 function with the stored salt and absolute path; if the new hash equals the stored hash, everything is intact — otherwise, something has been modified.