HOMEWORK #5: ACCESS

OVERVIEW

The access executable provided in this HW is a piece of software used for granting access to a turnstile. It provides simple user authentication using standard username/password combinations. Unfortunately, the company that developed the software inserted a backdoor to allow unfettered access to all the organizations that use the physical access control system.[1]

TASKS

1. Find the routine responsible for logging invalid credentials and the routine that checks if your credentials are valid. Rewrite both routines in C pseudocode. Note that symbols are not present in the binary so when disassembling with IDA, the functions you must find will be named 'sub_xxxxx'.

2. Determine how the backdoor operates and how to use it.

[1] Crashing the process is not the backdoor because the physical system is engineered to fail secure (i.e., the door's default behavior is to remain locked).