SE507μ Hacking Password Hashes with Rainbow Tables

Mission 2: John the Ripper

This assessment evaluates the following competencies:

- *CS007 – Understand why it is important to store passwords carefully* *(+1)*
- *CS210 – Understand how passwords can be stored securely in databases* *(+1)*
- *CS205 – Write an application that stores passwords securely* *(+1)*
- *CS901 – Understand how passwords database can be attacked* *(+1)*

In this mission, you have to write a program that produces a password file, that is, it should store several (identifier, password) pairs in a text file (one per line). Use the LM Hash algorithm to produce the hashed passwords and choose weak passwords, to not wait for hours or days... Then, you should use John the Ripper to attack this password file. To succeed the mission, you have to:

1. Install John the Ripper on your computer.

2. Write the program that creates the password database, hashed with the LM Hash algorithm.

3. Crack the database file with John the Ripper.

4. Explain and show to the teacher how you created the password database and cracked it, and be prepared to answer questions from him/her about password database protection.

You can find the John the Ripper tool and instructions about how to install and use it at the following address: https://www.openwall.com/john/pro.