Winter 2020
Sébastien Combéfis

SE507μ Hacking Password Hashes with Rainbow Tables

Quizz 3: Rainbow table

This assessment evaluates the following competencies:

- *CS007 – Understand why it is important to store passwords carefully*
- *CS901 – Understand how passwords database can be attacked*
- *CS502 – Understand how rainbow table can be used to find a password given the hashed passwords database*

Three affirmations are given for each assessed competency. For each of them, you have to decide whether it is true or false. To get a star for the competency, you must have the correct answer for the three affirmations.

CS007	**True**	**False**
If an attacker knows your identifier and managed to find your password (in clear), he/she can be authenticated on any website/platform where you use this (identifier, password) pair.	□	□
A longer password with a very diverse charset (character, digit, special character, etc.) is better than a short one with only digits (such as a PIN code).	□	□
Encrypting a passwords database file may slow down the account creation and login processes, but increases the security of the system in case of a theft of the passwords database.	□	□

CS901	**True**	**False**
Reversing a password that has been hashed with a salt is not impossible, but very time consuming.	□	□
Given one hashed password, I can find the corresponding clear passwords, for sure, just by enumerating all the possible passwords.	□	□
Given one hashed password, I may find the corresponding clear passwords just by enumerating all the possible passwords, but I am not sure to find it.	□	□

CS502	**True**	**False**
A rainbow table is a collection of hash chains, that is alternating sequences of clear passwords and their corresponding hashes.	□	□
A rainbow table can be used to store many (password, hash) pairs efficiently regarding memory consumption.	□	□
Given a rainbow table with 1000 chains and 1000 reduction functions, in the worst case it will take about 1000000 operations to try all the represented (password, hash) pairs.	□	□