**Pre-Computed hash attack**

**Other name: rainbow table attack**

**Description 1.**

A rainbow table is a table that contains a hash function’s inputs and corresponding outputs. A rainbow table makes brute forcing a password hash much easier, by removing the most computationally complicated part of a brute force – performing the hash function itself. With all of the values already computed, it’s simplified to just a simple search-and-compare operation on the table.

With rainbow tables, you are comparing a table of known inputs and outputs to a bunch of unknown outputs. If there’s a match, you know for certain that the hash function returns that output for it’s corresponding input in the table. A large portion of the security of the hash (the fact that the hash function is not an instant operation, and requires some amount of computational power, and therefore time, to perform) is bypassed with rainbow tables, meaning that if you’re lucky, you’ll find some matches. [1]

**Description 2.**

Precomputed attacks are a form of offline attacks. In this attack, also known as ‘rainbow table attack’, the password hashes are stored in a file. The size of this file can be very large, for example storing all LM hashes requires 310 terabytes of storage. Using Dr. Phillippe Oechslin time-memory trade-off drastically reduces the amount of storage space required to hold the hashes, to 17 gigabytes.

Precomputed hashes can greatly decrease the time needed to crack passwords. In fact, they can decrease the time required to find a password from months or weeks to just a few hours or even minutes. [2]

References

[1] <https://learncryptography.com/hash-functions/rainbow-tables>

[2] Ewaida, Bashar. "Pass-the-hash attacks: Tools and Mitigation." *Last accessed September* 11 (2013).