1. Each bit of salt used doubles the amount of computation and storage required for a pre-computed table. If the salt is too short, an attacker can easily build a lookup table for every possible salt since having a salt with fewer values minimises the total number of possible salts.
2. Null passwords that contain zero characters give zero protection to a system. Correspondingly, passwords shorter than 8 characters are easy to crack and make systems vulnerable to attacks since the lesser the characters the fewer possible permutations. As a result, weak passwords make it easier for hackers to gain full user access and create data breaches.
3. A good cryptographic hash function should be computationally hard to reverse, hard to find a different input with the same hash, and hard to find two different inputs of any length that result in the same hash.
4. A typical time period should be an ever-increasing delay between successive failed login attempts. For instance, first you allow an instant retry, followed by a wait time of one second, then two seconds, four, eight, and so forth. The downside is that it punishes forgetful users; however, it is enough to stymie any brute force attack.