A Brute Force Attack is a method to get access to a server or website. It involves frequent attempts of trying different password combinations to break into any server, website, or anything that is protected. Frequent attempts refer to attackers trying different combinations of numbers, letters, and symbols until they gets it right. This repetitive process is like an army attacking a castle.

In the world of cyber crimes, hackers are using this method with the help of bots to make such attacks. We think that passwords keep our data safe, but research has shown that it is not enough. For hackers, it's a piece of cake to hack into our systems, steal our data, and misuse it. In 2012, researchers proved that hackers could crack any eight-characters long password in less than six hours. And that was back in 2012 when machines were not as efficient or effective as they are today.

**How to Prevent Brute Force Attack?**

There are different methods of brute force attack such as:

* **Hybrid Brute Force Attack** uses a list of common words in a dictionary. For example, if your password is '12345678’', then the bot can crack your password within seconds.
* **Reverse Brute Force Attack** uses an individual password or a common group of passwords against a list of possible user IDs.
* **Credential Stuffing** uses the known pairing of username and password to gain access to multiple networks or websites.

Brute force attacks are successful because of careless network administration and weak passwords. Luckily, these both areas can be improved easily to prevent such attacks that could bring our network or website to their knees. The attacks mentioned above can be avoided by:

* Using strong and unique passwords with characters, upper- and lower-case letters, numbers, and spaces.
* Using different usernames or passwords for different networks.
* Allowing limited login attempts.
* Locking the account after login-attempts limit is reached.
* Restricting multiple login attempts from a single IP address.
* Enabling two-factor authentication like face detection or biometric verification.
* Changing password right away when an email, received from a service provider tells you that someone logged into your account from a different location.
* Using a good bot detection software that can detect strange activities.

Nowadays, it is crucial to educate ourselves about the importance of strong passwords and best practices in order to keep our systems secure. People will keep falling victim to such attacks if security does not become a strong part of our culture.