Password Spraying

https://doubleoctopus.com/security-wiki/threats-and-tools/password-spraying/

Password spraying is a type of bruteforce attack. An attacker uses a list of usernames and default passwords to try logging into the application. This attack can be used with applications that allow users to set a default password.

Brute force prevention should be on both username and password. Account lockout policies after a certain amount of failed logins should be implemented. Captcha should be used. Multi-factor authentication should be enabled. External facing services should require multi-factor authentication.

Password spraying is an attack that tries to guess common passwords for a lot of accounts. A traditional brute force attack tries to guess a single password. Password spraying uses a low-and-slow approach. It first tries a common password, then moves onto another common password, etc., until it finds a match.Password spraying attacks typically target single sign-ons and cloud-based applications that utilize federated authentication protocols. This allows attackers to mask malicious traffic. Attacks against email applications help maximize access to intellectual property, if successful.Credential stuffing is a type of attack that involves stealing or guessing credentials by exploiting a website's login system. This is done without any user interaction. To avoid this kind of attack, you need to use two-factor authentication (2FA) instead of passwords.

A list of usernames should be acquired. This can be done by finding accounts that belong to people who work for the organization. Once these accounts are found, we can use them to create new accounts. We can also search the internet for usernames. There are many ways to acquire this data.Hackers should always spray passwords. They should also know how long to wait before trying another password. This helps them avoid being detected by account holders who set timeouts.Password spray is a common method used by hackers to gain access to an account or system. A hacker uses one password to gain access to an online service. Then, he gains access to other services using the same password.A lot of people use the same password over and over again. You should change your passwords regularly. Make sure you use different passwords for each website or service you use.