What is password spraying?

Password spraying is a brute-force variant that tries a single common password (like Season+Year or Company123) across many accounts, rather than many passwords against one account. By spreading attempts across users and pacing them under the lockout threshold, the attacker finds accounts with weak passwords without locking anyone out. It is a common initial-access and privilege technique against Active Directory. Defend with strong password policy, MFA, and detection tuned for the spray pattern.

HOW IT WORKS

01 How the attack works

The attacker first enumerates valid usernames (from OSINT, or via Kerberos pre-auth with `kerbrute userenum`), then sprays a common password with a tool such as `kerbrute passwordspray users.txt 'Autumn2025!'`, pacing attempts to stay under the lockout window. One weak password on any account gives a foothold, and if that account is privileged, escalation. Shown for defensive testing.

SOURCES

[1] MITRE ATT&CK Enterprise Matrix

[2] MITRE ATT&CK: Password Spraying (T1110.003)

Test your Active Directory before an attacker does.

`securelayer7.net/learn/active-directory/password-spraying`

Open online