CS-028 · Passwords & Authentication

Password Spraying

Trying a few common passwords across many accounts to stay under lockout thresholds.

Executive Summary

Password spraying flips the usual guessing attack around. Instead of trying many passwords against one account, an attacker tries one or a few very common passwords against a large list of accounts. By using only a handful of attempts per account, the attacker stays below lockout thresholds and can quietly find the few users who chose a weak, popular password.

What It Is

Password spraying is a low and slow account takeover technique. Traditional guessing hammers a single account with many passwords, which quickly triggers lockout. Spraying inverts this. The attacker selects a small set of the most common passwords, then tries each one against a broad list of usernames, waiting between rounds so no single account accumulates enough failures to lock. The attacker only needs a small percentage of users to have chosen a weak password for the campaign to succeed. Corporate directories, cloud email portals, and single sign on gateways are frequent targets because their usernames are often predictable from public information.

Why It Matters

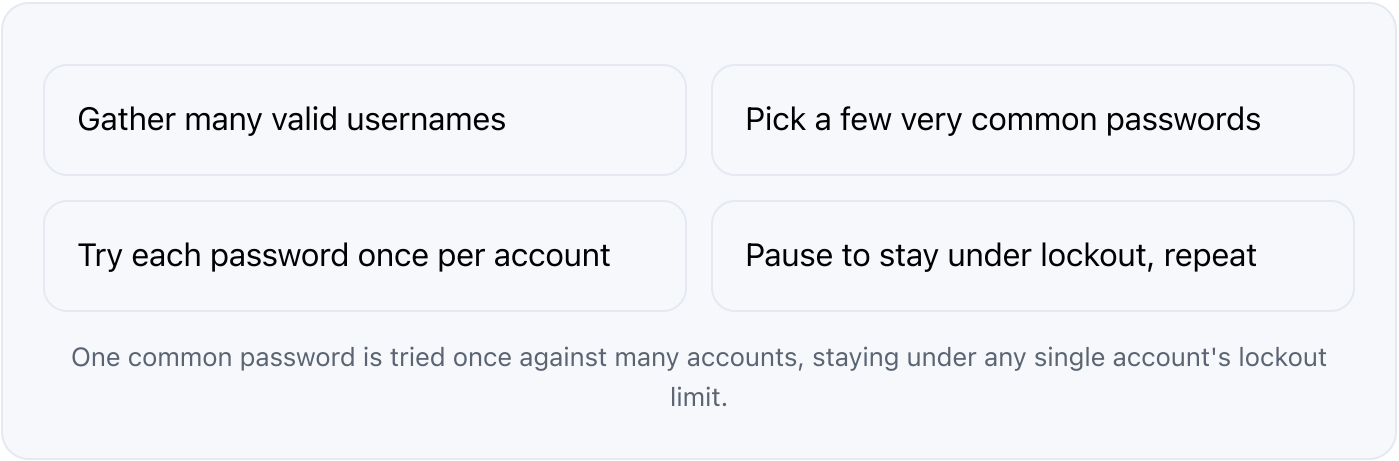
Spraying is dangerous precisely because it is quiet and evades the classic defense of account lockout. It exploits the reality that in any large population of users, some will choose a password from the tiny set of extremely common ones. A single compromised corporate account can open email, internal systems, and a path to deeper intrusion. Because the attack spreads thinly across many accounts, it can slip past controls tuned to catch repeated failures on one account. For a

professional, understanding spraying is key to configuring detection that watches across accounts, not just per account, and to justifying MFA and breached password screening.

How It Works

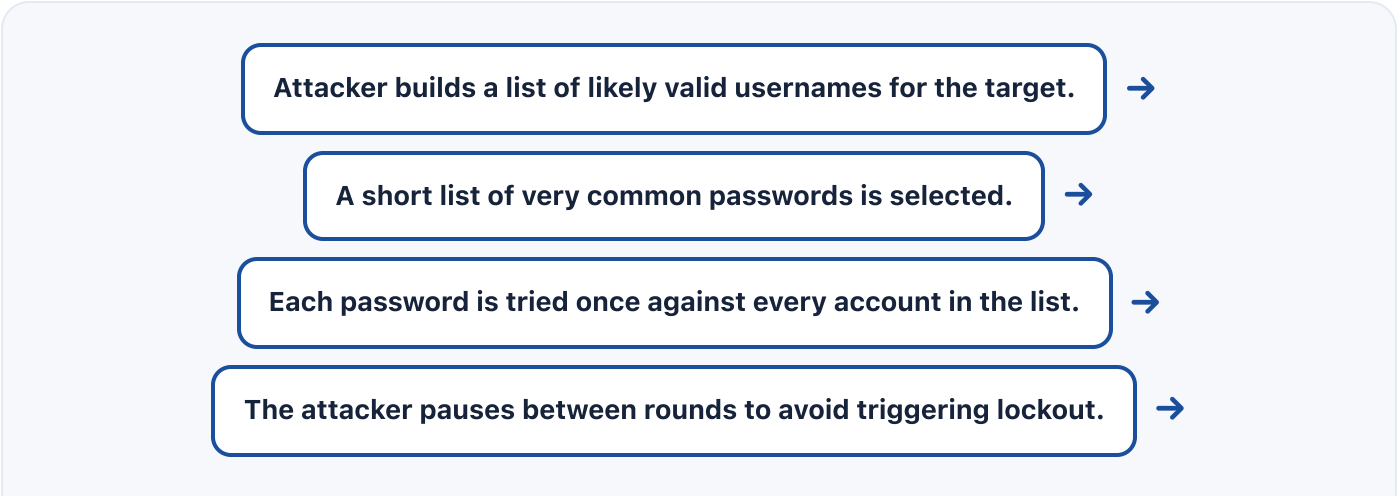
The attacker first gathers or guesses a list of valid usernames, often derived from a predictable email format and public directories. They then choose a few passwords that are statistically common or seasonally likely, and attempt each password once across the whole username list before moving to the next password and pausing between rounds. Because each account sees only one or two failures at a time, lockout thresholds tuned to single account behavior do not trigger. Detection therefore has to correlate failures across many accounts from the same source or the same password, look for a low steady rate of failures organization wide, and require MFA so even a correct guess does not grant access.

Architecture Diagram



One common password is tried once against many accounts, staying under any single account's lockout limit.

Visual Workflow



Any account with a weak common password authenticates and is taken over. →

Defenders detect the cross account pattern and force resets with MFA.

Common Attacks

- Spraying seasonal or company themed passwords against corporate directories
- Targeting cloud email and single sign on portals with predictable usernames
- Timing attempts to stay under per account lockout thresholds
- Using distributed sources so the traffic does not cluster on one address
- Combining a captured password with real time phishing of the second factor

Common Mistakes

- Tuning detection only per account and missing the cross account pattern
- Allowing users to set extremely common or seasonal passwords
- Relying on lockout alone, which spraying is specifically designed to evade
- Leaving legacy protocols enabled that bypass modern MFA on portals
- Publishing predictable username formats without compensating controls

Best Practices

- Require MFA so a correctly sprayed password still cannot complete login
- Screen and block common and breached passwords at the point of creation
- Monitor for a low steady rate of failures spread across many accounts
- Correlate failures by source and by password, not just per account
- Disable legacy authentication protocols that bypass MFA
- Alert on any successful login that follows a spray pattern

Quick Checklist

- [x] MFA enforced on all externally reachable logins

- [x] Common and breached passwords blocked at creation
- [x] Cross account failure correlation and alerting configured
- [x] Legacy authentication protocols disabled
- [x] Detection tuned for low, distributed failure rates
- [x] Playbook to force resets after a detected spray

Recommended Tools

Identity threat detection
Correlates login failures across many accounts to spot spraying

Breached and common password screening
Prevents users from choosing sprayable passwords

Authenticator app or security key
Second factor that stops a sprayed password from succeeding

SIEM with authentication analytics
Surfaces organization wide failure patterns and successful anomalies

Industry Standards

NIST SP 800-63B
Recommends screening common and breached passwords and strong authenticators

OWASP Authentication Cheat Sheet
Guidance on login protections that reduce spraying success

CISA Guidance on MFA
Supports MFA and disabling legacy protocols against sprayed credentials

Career Relevance

Password spraying is a staple of security operations and identity defense. SOC analysts build detections that correlate failures across the whole directory; IAM and security engineers enforce

MFA, block weak passwords, and disable legacy protocols; and GRC analysts assess whether authentication controls meet framework expectations. The ability to explain why per account lockout is not enough, and how cross account detection works, is a valuable skill for the roles AI-Governance-Jobs.com serves.

Interview Questions

- How does password spraying differ from a brute force attack on one account?
- Why does password spraying evade traditional account lockout?
- What detection strategy catches spraying that per account monitoring misses?
- Why does disabling legacy authentication protocols matter against spraying?
- How does MFA defend against a successfully sprayed password?

Related Certifications

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | ISC2 SSCP

Further Reading

- NIST SP 800-63B Digital Identity Guidelines
- CISA: More Than a Password
- OWASP Authentication Cheat Sheet

Key Takeaways

- Password spraying tries a few common passwords across many accounts.
- By limiting attempts per account, it slips under lockout thresholds.
- It succeeds when even a few users pick a very common password.
- Detection must correlate failures across accounts, not just per account.
- MFA and common password screening are the strongest defenses.

FAQ

▶ **Why is password spraying hard to detect?**

▶ **Does account lockout stop password spraying?**

▶ **What accounts are most at risk from spraying?**

Related Careers

RELATED ROLES

Soc Analyst | Iam Engineer | Security Engineer

RELATED CERTIFICATIONS

CompTIA Security+ | ISC2 Certified in Cybersecurity (CC) | ISC2 SSCP

CURRENT OPENINGS

Live roles are on the job board.

Browse all jobs

GUIDES & SALARY

Career guides | Role roadmaps | Salary data | Career tools

SUGGESTED LEARNING PATH

1. Ground the basics with CS-001 Cybersecurity
2. Study this sheet: **Password Spraying**
3. Go deeper: Passwords
4. Go deeper: Multi-Factor Authentication (MFA)
5. Validate it: work toward **CompTIA Security+**
6. Find the role: browse current openings

RELATED SHEETS

CS-022 Passwords | CS-025 Multi-Factor Authentication (MFA) | CS-027 Credential Stuffing | CS-029 Brute Force Attacks | CS-031 Account Lockout