Distributed Password Spraying via Authentication Failures Across Multiple Accounts, Detection Strategy DET0487

Archived: 2026-04-05 16:22:36 UTC

AN1336

A high volume of authentication failures using a single password (or small set) across many different user accounts within a defined time window

Log Sources

Mutable Elements

Field	Description
PasswordReuseThreshold	Number of distinct accounts a password is used against before alerting
TimeWindow	Window over which the correlation is measured (e.g., 10 mins)
TargetGroupFilter	Limit detection to sensitive or monitored user groups (e.g., Admins)

AN1337

Authentication failures across different accounts using a repeated or similar password via SSH or PAM stack within a short window

Log Sources

Mutable Elements

Field	Description
PasswordReusePattern	Repetition or minor variation of the same password across user attempts
IPAggregationWindow	Length of time to observe distributed spray attempts from single source

AN1338

Multiple failed login attempts across different users using common password patterns (e.g., 'Welcome2023')

Log Sources

Mutable Elements

Field	Description
RetryCountThreshold	Total number of attempts before alerting
CommonPasswordList	List of passwords considered suspicious due to widespread use

AN1339

Sign-in failures across enterprise SSO applications or SaaS platforms from same IP address using the same password against multiple user identities

Log Sources

Mutable Elements

Field	Description
GeoIPAnomalyCheck	Use geolocation mismatches to strengthen signal
FailedUserRatio	Proportion of total user base affected to filter noise

AN1340

Authentication failure logs on routers/switches showing repeated use of default or common passwords across multiple accounts

Log Sources

Mutable Elements

Field	Description
AuthFailureBurst	Cluster of failed attempts in short period indicating spray
InterfaceFilter	Limit detection to console/SSH vs web UI interfaces

AN1341

Repeated failed authentication attempts to container APIs, control planes, or login shells across many user names using same password

Log Sources

Mutable Elements

Field	Description
OrchestrationScope	Detect spray attempts scoped to single pod vs full cluster
ServiceAccountFilter	Limit detection to non-service accounts to reduce noise

AN1342

Failed authentication attempts across user mailboxes using identical or common passwords (e.g., OWA brute attempts)

Log Sources

Mutable Elements

Field	Description
MailboxAccessAttempts	Threshold on mailbox login failures by same IP
EmailPatternAnalysis	Match target usernames to common spray dictionaries

AN1343

SaaS applications receiving authentication failures for dozens of accounts using same password or login signature

Log Sources

Mutable Elements

Field	Description
CloudAppScope	Restrict detection to identity providers or select high-risk SaaS platforms
UserPopulationSensitivity	Adjust based on size and role of account pool

---