Credential Stuffing Detection via Reused Breached Credentials Across Services, Detection Strategy DET0460

Archived: 2026-04-05 14:41:37 UTC

AN1262

Multiple failed authentication attempts using distinct username/password pairs from a single IP address or session within a short time window, targeting common services like RDP or SMB

Log Sources

Mutable Elements

Field	Description
UsernameUniquenessThreshold	Minimum number of unique usernames in failed login attempts before triggering alert
TimeWindow	Duration (e.g., 5 minutes) to observe the behavior chain of rapid login attempts
SourceIPScope	Whether to group by full IP or CIDR block for bursty behavior from botnets

AN1263

Rapid login failures across different users from a single IP address, targeting SSH or PAM login with distinct username-password pairs

Log Sources

Mutable Elements

Field	Description
LoginFailureRatio	Ratio of failed logins per unique user attempted
AuthServiceFilter	Restrict detection to certain protocols (e.g., sshd, login, su)

AN1264

Burst of failed authentications with rotating usernames against loginwindow or remote management service using reused breached credentials

Log Sources

Mutable Elements

Field	Description
DistinctUsernameCount	Tunable threshold for number of attempted usernames in a time window
RemoteAccessFilter	Restrict behavior detection to remote login interfaces

AN1265

Same source IP performing multiple authentication attempts using known breached username/password combinations across different identities in Azure AD, Okta, or Duo

Log Sources

Mutable Elements

Field	Description
BreachedCredentialSourceMatch	Optional enrichment using known leaked credentials database
SSOServiceScope	Targeting only federated or hybrid identity auth flows

AN1266

Multiple sign-in failures against cloud-based applications using username/password combinations leaked from unrelated domains

Log Sources

Mutable Elements

Field	Description
UserAccountOverlap	Correlate credentials reused across multiple SaaS platforms
FailedAttemptsPerIP	Number of failed logins from same IP before alerting

AN1267

Router/firewall/syslog logs showing authentication failures with unique usernames and reused credentials from same source IP

Log Sources

Mutable Elements

Field	Description
AuthProtocolFilter	Limit detection to interactive logins rather than SNMP/RPC
FailedAuthBurst	Detection trigger when failure rate exceeds normal profile

AN1268

Credential stuffing attempts against Kubernetes API or containerized login shells using stolen or leaked user credentials

Log Sources

Mutable Elements

Field	Description
PodAccessScope	Detect attempts across multiple pods/namespaces using same IP
CredentialSetSize	Number of username/password pairs used in attack attempt

AN1269

Use of leaked credential pairs against Outlook Web Access (OWA), Microsoft 365, or Exchange from a single client IP with multiple failures

Log Sources

Mutable Elements

Field	Description
PasswordSourceMatch	Optional: cross-reference to haveibeenpwned or internal credential dumps
MailboxLoginThreshold	Tunable value for how many unique mailbox attempts trigger alert

AN1270

Burst of failed login attempts across VM instances using leaked credential pairs from single IP in public cloud environments

Log Sources

Mutable Elements

Field	Description
InstanceIDScope	Define if detection should group logins per host or across cluster
IPBehaviorHistory	Correlate against past IP reputation or behavioral profiles

---