Brute Force Authentication

What it is

A brute force alert detects repetitive, unsuccessful login activity, sometimes followed by a successful login

Attacker Behavior

Attackers will use credentials compromised in unassociated breaches or list of common passwords to try to get access to a valid account. Often, they need to try many times in hopes of finding valid credentials

Common False Positive Factors

- Password change or expiry
- Forgotten password
- User testing legitimate access
- Data incorrectly reporting login failures

Triage Playbook

	Do This	What to look for	Where to look	Takeaways
1	Identify who or what uses the Account	Figure out what services or people use this account. Some accounts are shared and some accounts belong to a system or application	Search Active Directory via the company address book or AD portal Some orgs import this AD data into your SIEM tool	Accounts associated with high privilege services or users are more interesting. Regular user accounts, less so.
2	Check if the account is disabled, if the password expired or if the password was changed recently	Look for recent changes to an account that would potentially affect a person or systems ability to login	Active directory console, such as Azure Active Directory. Log data including Windows events: 4725, 4740, 4723, 4724 Chapter 8 Account Management Events (ultimatewindowssecurity.com)	Recent changes such as an expired password that happen before the alert can often explain the login failure activity.
3	Identify what is being accessed **AND** where the login is coming from	Figure out what system or service is being logged into. Also, identify if this is typical for this account	Search authentication logs for the target account(s). Non-domain accounts may only appear in application or system logs	If nothing else looks different other than new login failure, there is likely an explainable reason for the failures.
4	Count login failures and successes	Look for how many login attempts have happened, how many (if any) were successful, and in what order the logins happened.	Search authentication logs for the target account(s). Non-domain accounts may only appear in application or system logs	Many failures followed by a success are more interesting. A mix of successes and failures over a period of time could mean there is an issue with how the data is being read

Cyber Alert Triage Playbook

	Do This	What to look for	Where to look	Takeaways
5	Check threat intelligence around the account and sources	External intelligence on related attacker infrastructure **AND** recent alerts and incidents involving in scope systems and accounts	Opensource tools such as IPvoid, and Paid intel reports Search for other relevant alerts in your SIEM tool	Obviously, an intel match is interesting. Be wary of intel on external IPs, which can often be shared by many legitimate services and changed quickly

Common False Positive Scenarios

A user recently changed their password and tries a few, unsuccessful attempts before recalling the new credential. These logins will be interactive (Windows logon type 2), meaning someone typed a password.

A service account expired, and the system using that account keeps trying to unsuccessfully login. These events will begin after the password expired and failures will commonly occur on regular intervals.

Audit logs indicate alternating failed and successful logins. Some system logs include erroneous failure messages produced by unused login services. Look for changing login services between failures and successes

A system or application admin tests their access to many systems. Developers and Admins often have elevated or partially elevated privilege to systems and may, during the course of their work, find the limits of their access. In these cases the admin may generate many failed login attempts.

What to do next

If No Threat Found

- Update alert notes with details of your investigation
- Record any new queries you used to gather context for future use
- If ongoing behavior, recommend temporary alert tuning rule to exclude account from use case
- Recommend blocking of any malicious external sources identified during investigation

If Potential Threat Identified

Its best practice to follow your incident response plan anytime you identify a potential threat. In the case of a significant compromise, taking a remediation action before consulting your incident response plan can make larger response and recovery more difficult.

Credential Eviction:

https://d3fend.mitre.org/technique/d3f:CredentialEviction