**1. Brute Force Detection**

Brute Force Detection Based on Windows Event ID 4625

What is Event ID 4625?

This is generated when a logon attempt fails, typically due to:

* Wrong password
* Invalid username
* Account restrictions

Detection Logic

Goal: Identify multiple 4625 events from the same IP address or against the same account within a short time period.

Step-by-Step Approach

Step 1: Enable Detailed Logging

* Ensure "Logon/Logoff" auditing is enabled in Local Security Policy:
* Security Settings → Advanced Audit Policy Configuration → Audit Policies → Logon/Logoff → Audit Logon (Success, Failure)

Step 2: Analyze Event ID 4625

Key fields in 4625 to look at:

|  |  |
| --- | --- |
| Field | Description |
| Account Name | Targeted username |
| Source Network Address | IP of attacker |
| Logon Type | 10 = RDP, 3 = Network, 2 = Local |
| Failure Reason | Like "bad password" |
| Process Name | Source application (optional) |
| Workstation Name | Target machine name |

Step 3: Detect Suspicious Patterns

Look for:

* ≥5 failed attempts from the same Source IP in ≤1 minute.
* Attempts targeting same user account in quick succession.
* High frequency of Logon Type 3 or 10 failures.