**Splunk Brute Force Detection (Linux Logs)**

**Goal**: Detect SSH brute-force attacks, failed logins, and create dashboards + alerts using Splunk SPL from *linux\_secure* logs.

**Data Source**

| **Field** | **Value** |
| --- | --- |
| index | linux\_logs |
| sourcetype | linux\_secure |
| Input Log | /var/log/auth.log |

**Basic Search**

*index=linux\_logs sourcetype=linux\_secure*

**Detect Failed SSH Logins**

*index=linux\_logs sourcetype=linux\_secure "Failed password"*

*| rex "Failed password for (invalid user )?(?<user>\w+)"*

*| stats count by user, host, \_time*

*| sort - count*

**Detect Brute Force Attempts**

*index=linux\_logs sourcetype=linux\_secure "Failed password"*

*| rex "Failed password for (invalid user )?(?<user>\w+)"*

*| stats count by user, src, host, bin(\_time, 5m)*

*| where count >= 5*

*| sort - count*

**Threshold**: 5+ attempts in 5 minutes

### Successful SSH Logins

*index=linux\_logs sourcetype=linux\_secure "Accepted password"*

*| rex "Accepted password for (?<user>\w+)"*

*| stats count by user, src, \_time*

**Dashboard Panels**

**Top Failed Users**

*index=linux\_logs sourcetype=linux\_secure "Failed password"*

*| rex "Failed password for (invalid user )?(?<user>\w+)"*

*| top user*

**Top Source IPs**

*index=linux\_logs sourcetype=linux\_secure "Failed password"*

*| rex "from (?<src\_ip>\d+\.\d+\.\d+\.\d+)"*

*| top src\_ip*

**Timeline of Attempts**

*index=linux\_logs sourcetype=linux\_secure "Failed password"*

*| timechart count by host*

**Real-Time Alert Setup**

Query: Use Brute Force SPL above

Trigger: If number of results > 0

Time Range: Real-time (rolling 5 min window)

Actions:

1. Send email
2. Run script (block IP)
3. Create incident ticket

**Testing:**

To generate logs: SSH Failed Password

*ssh invaliduser@localhost*

To confirm on system:

*sudo grep "Failed password" /var/log/auth.log*

| **Feature** | **Implemented** |
| --- | --- |
| Failed Login Detection | ✅ |
| Brute Force Detection | ✅ |
| Top User/IP Report | ✅ |
| Real-time Alerts | ✅ |
| Dashboard Panels | ✅ |
| Data Source Verified | ✅ |