**📘 Skill Proof — SOC Monitoring & Event Analysis**

**📌 Objective**

To detect and visualize **multiple failed login attempts (Event ID 4625)** using Splunk Enterprise for monitoring potential brute-force or suspicious logon behavior.

**🧠 Description**

This project demonstrates how to use **Splunk Enterprise** to analyze **Windows Security Event Logs** for failed logon attempts.  
We’ll identify which user accounts and IP addresses are frequently failing authentication.

**⚙️ Tools Used**

* **Splunk Enterprise**
* **Windows Security Log Data (WinEventLog:Security)**
* **Sample log file:** windows\_failed\_logons.log

**🧾 Dataset Details**

Indexed in Splunk as:

index="soc\_lab"

sourcetype="WinEventLog:Security"

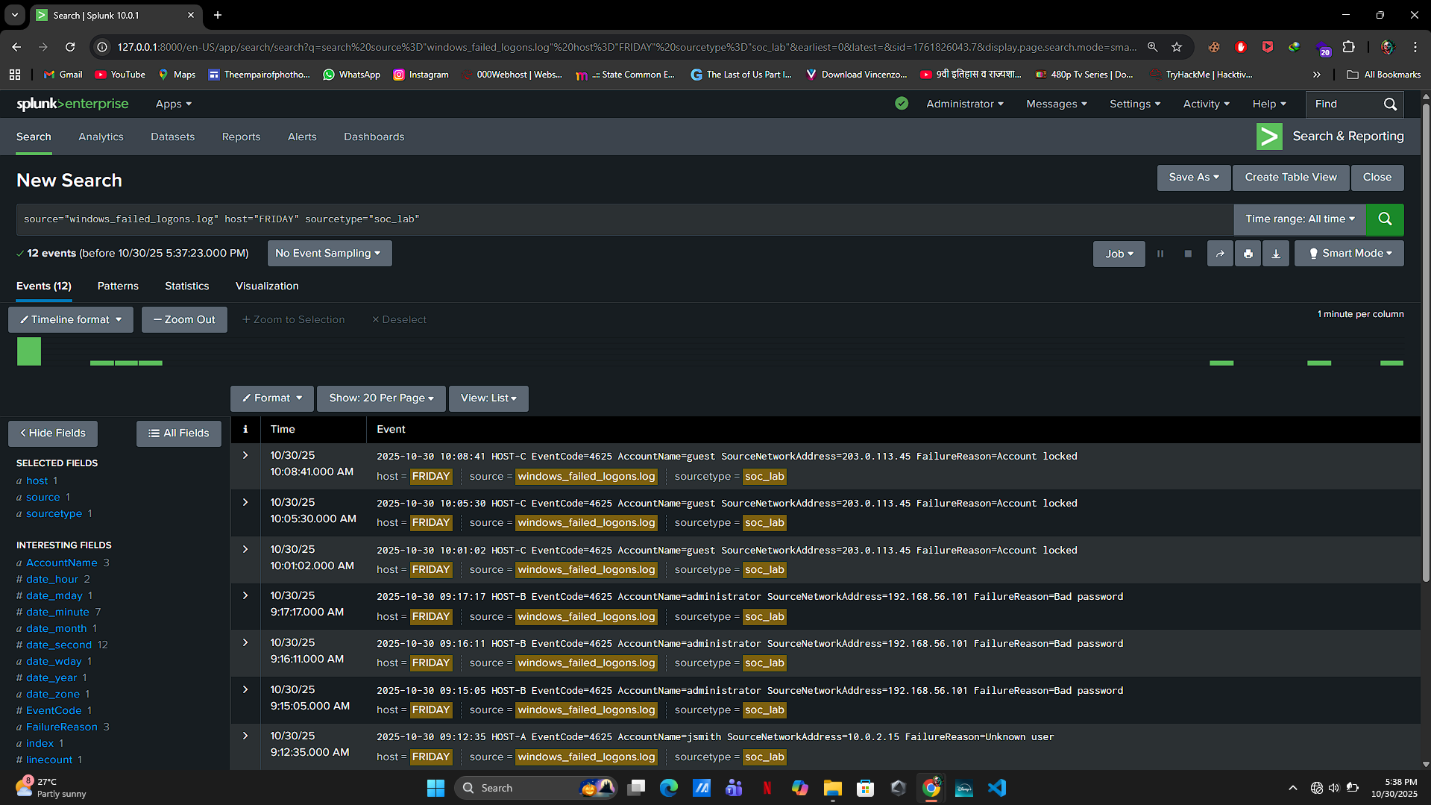
Each log record contains:

* EventCode
* AccountName
* SourceNetworkAddress
* FailureReason

**🪜 Step-by-Step Procedure**

**🧩 Step 1 — Create Index & Upload Log File**

1. Open Splunk Enterprise → **Settings → Indexes → New Index**  
   → Create index named soc\_lab.
2. Go to **Add Data → Upload File → Select windows\_failed\_logons.log → Index: soc\_lab**
3. Click **Start Searching** once data upload completes.



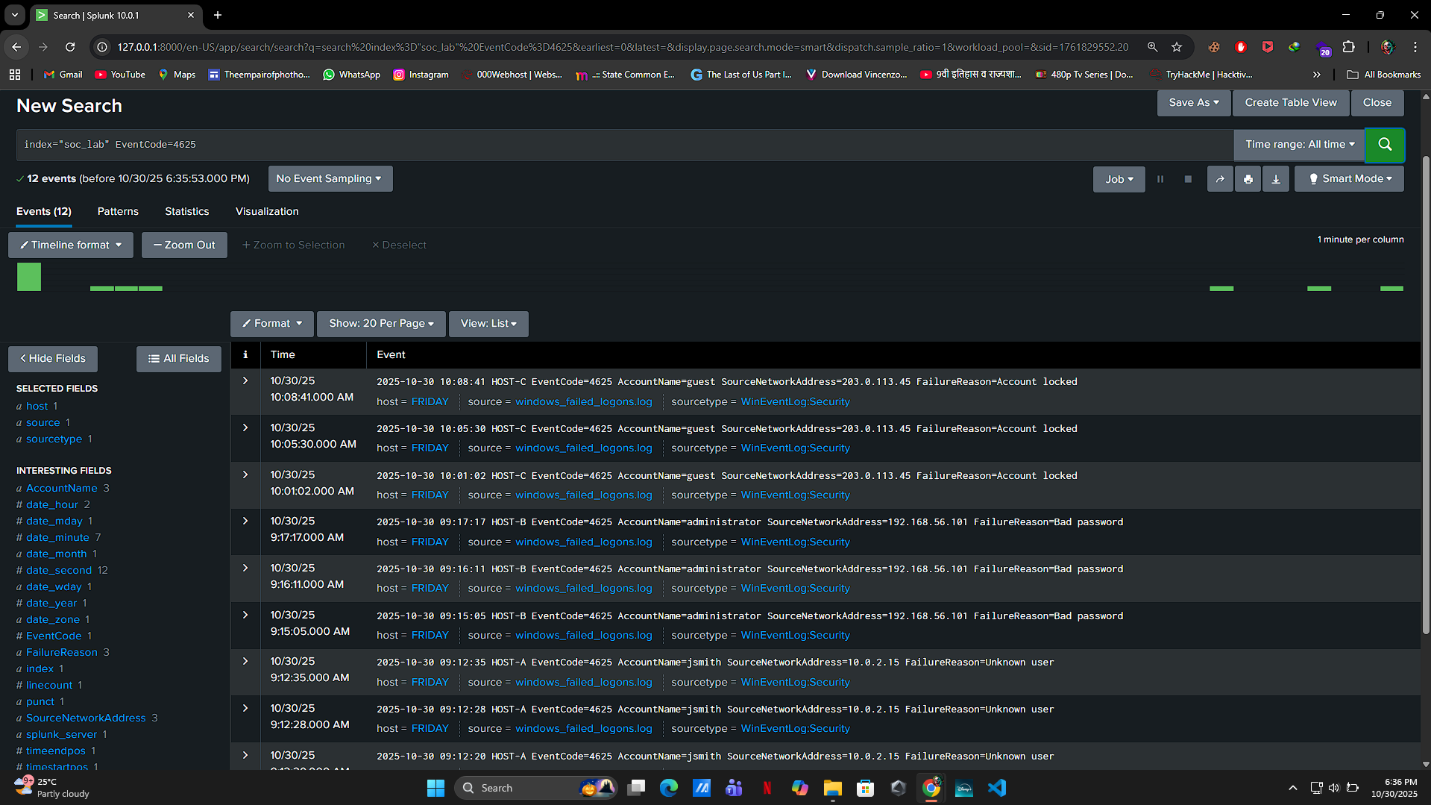
📸 **Figure-1:** Data upload into Splunk (Add Data screen)

**🧩 Step 2 — Run Basic Search Query**

In the search bar, run:

index="soc\_lab" EventCode=4625

✅ This displays all failed login attempts.



📸 **Figure-2:** Output of base query showing failed logon events.

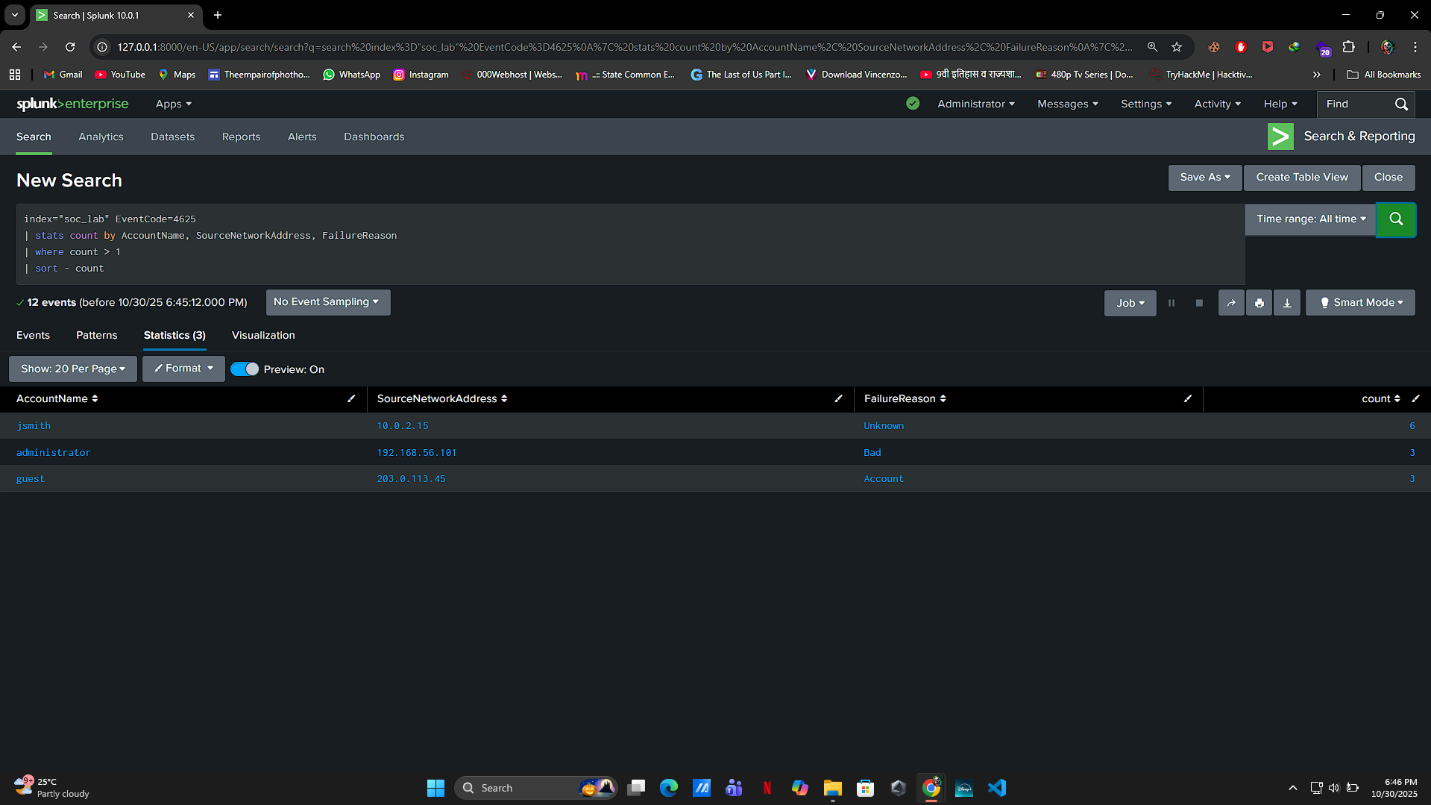
**🧩 Step 3 — Summarize Failed Logons**

Run:

index="soc\_lab" EventCode=4625

| stats count by AccountName, SourceNetworkAddress, FailureReason

| sort – count



📸 **Figure-3:** Table showing users with repeated failed logins and source IPs.

**🧩 Step 4 — Create Visualization**

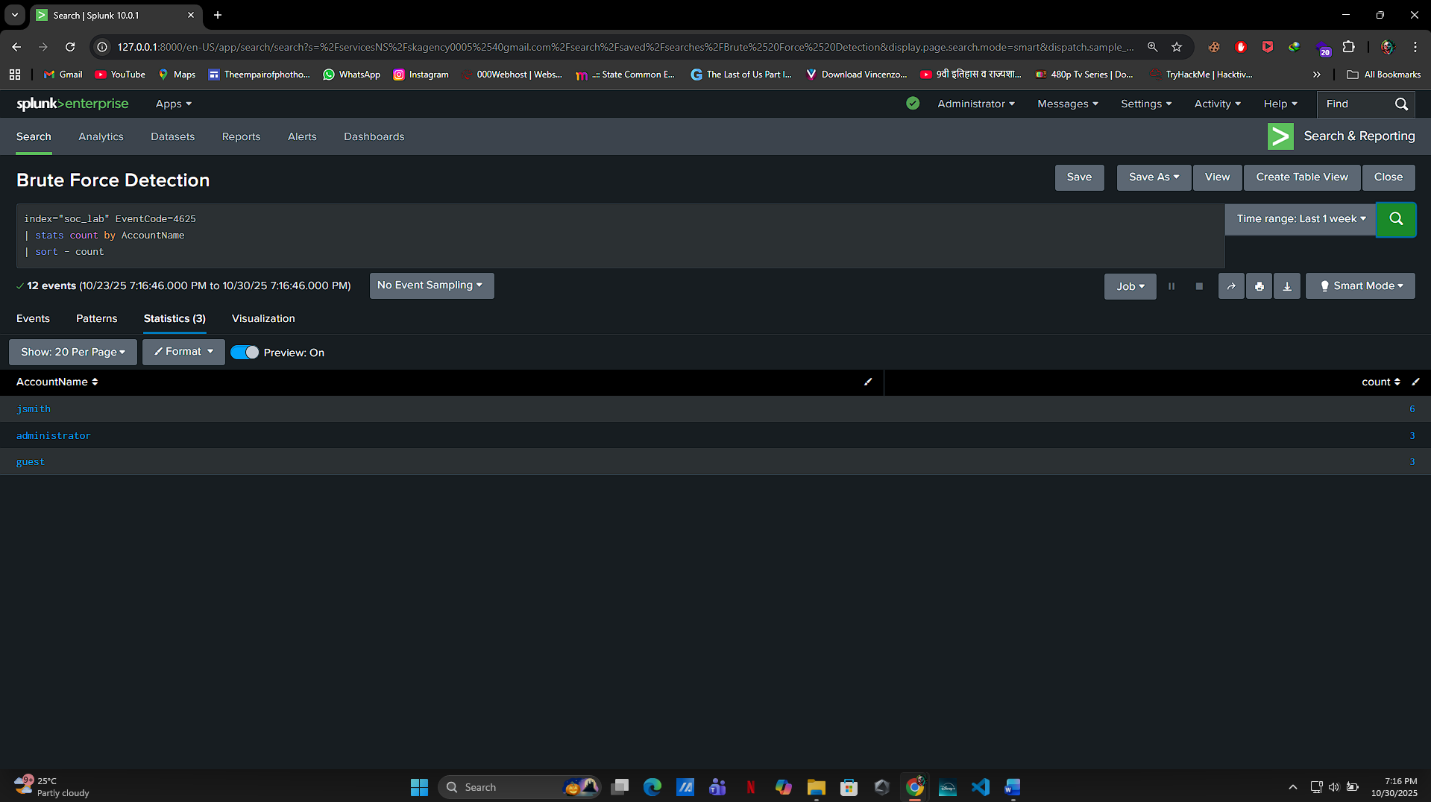
Run:

index="soc\_lab" EventCode=4625

| stats count by AccountName

| sort – count

Switch to **Visualization → Bar Chart** to visualize top failed user accounts.



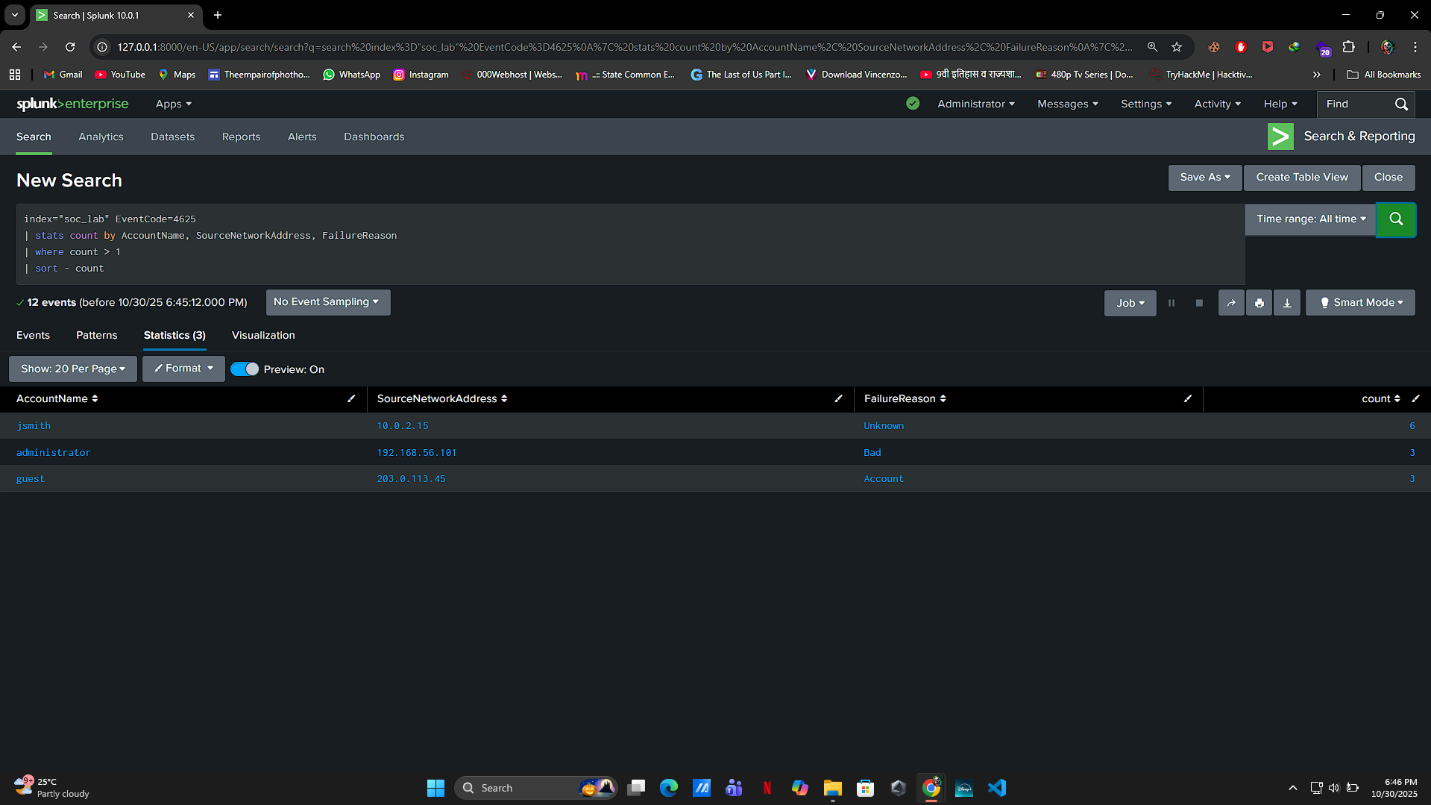
📸 **Figure-4:** Bar chart of users with most failed logins.

**🧩 Step 5 — Dashboard Panels**

Create a new dashboard named:  
**“Failed Login Detection Dashboard”**

Add three panels:

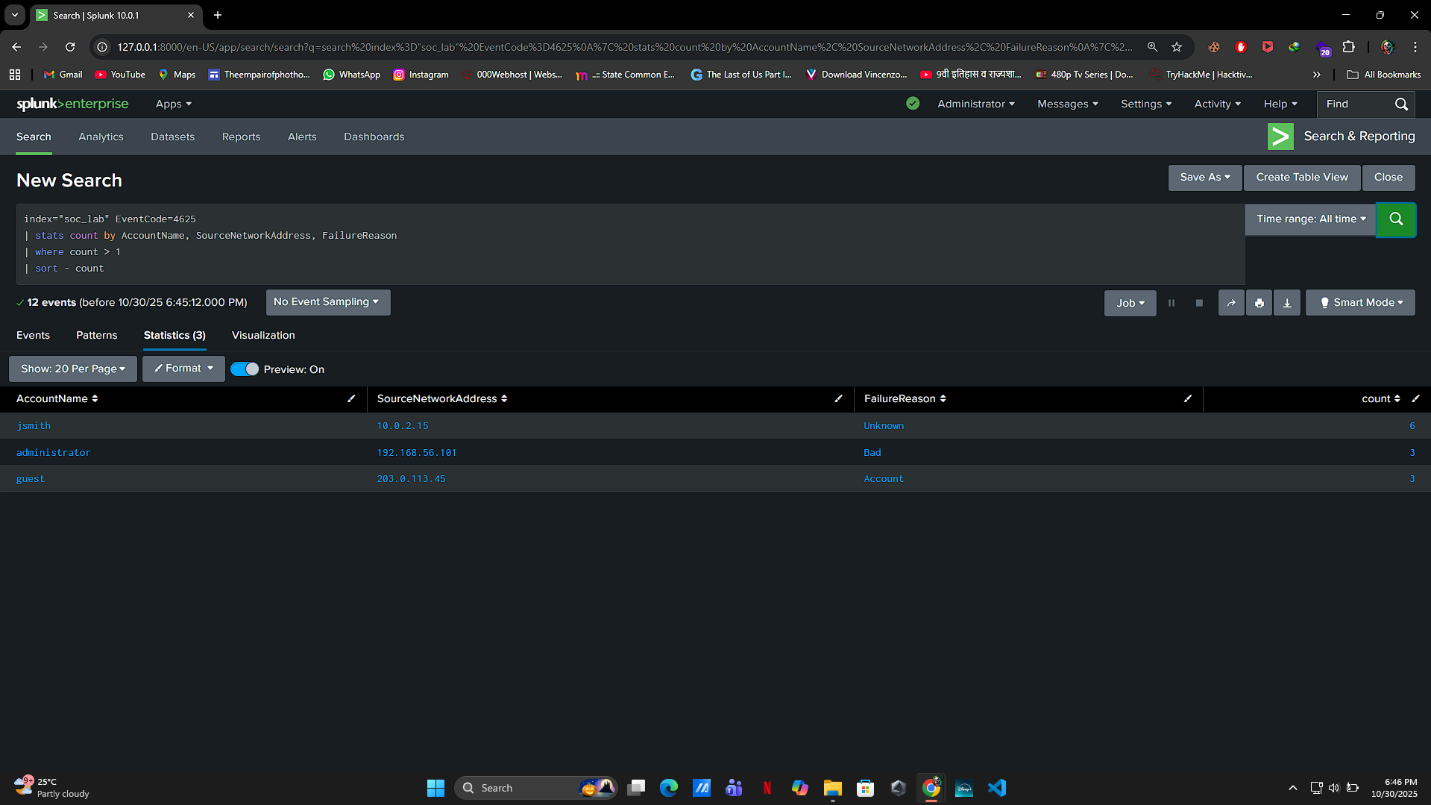
| **Panel Name** | **SPL Query** | **Visualization Type** |
| --- | --- | --- |
| Failed Login Summary | `index="soc\_lab" EventCode=4625 | stats count by AccountName, SourceNetworkAddress` |
| Top Failed User Accounts | `index="soc\_lab" EventCode=4625 | stats count by AccountName |
| Failure Reason Breakdown | `index="soc\_lab" EventCode=4625 | stats count by FailureReason` |



📸 **Figure-5:** Splunk dashboard showing failed login summary and charts.

**🧾 Example Output**

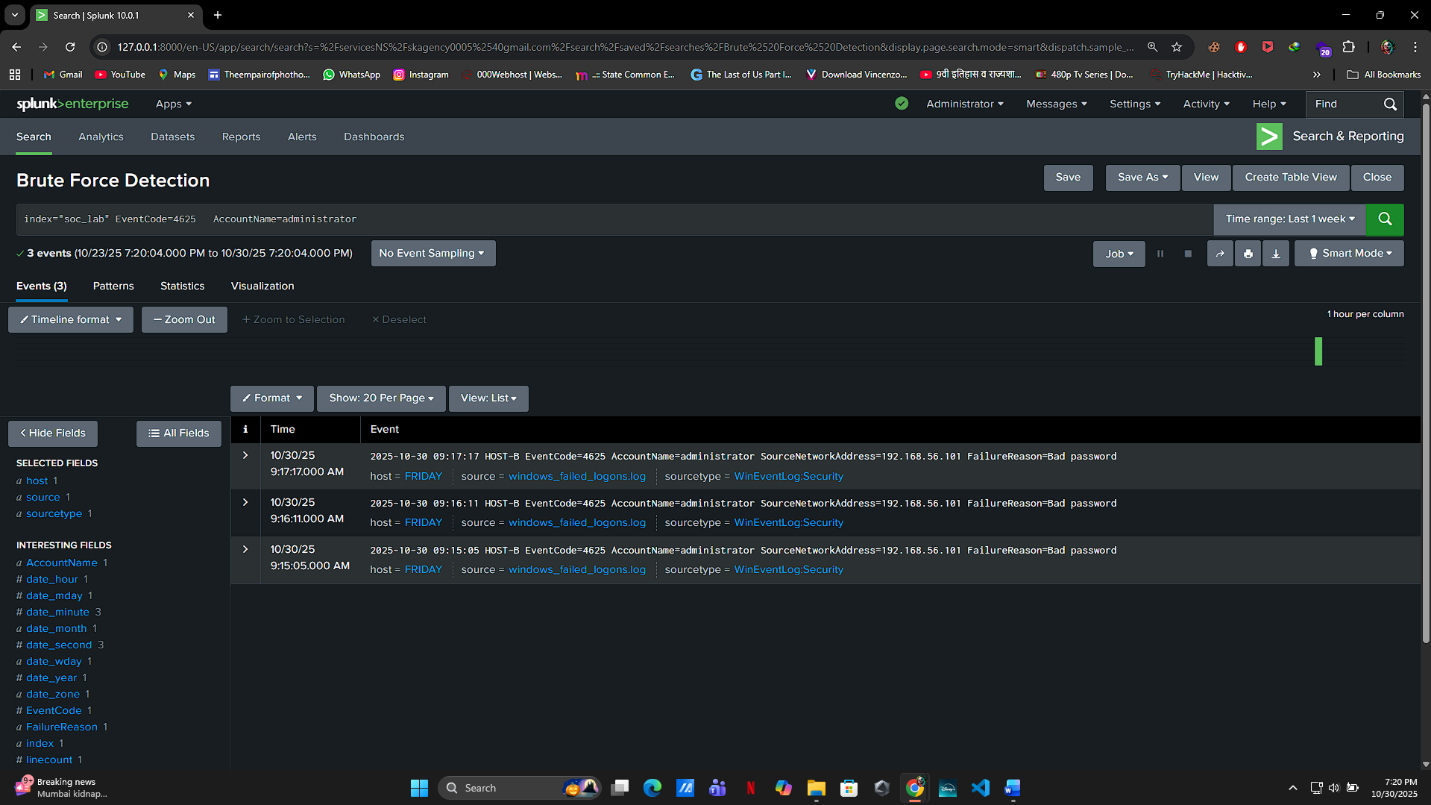
| **AccountName** | **SourceNetworkAddress** | **FailureReason** | **Count** |
| --- | --- | --- | --- |
| administrator | 192.168.56.101 | Bad password | 4 |
| guest | 203.0.113.45 | Account locked | 3 |
| jsmith | 10.0.2.15 | Unknown user | 2 |



📸 **Figure-6:** Example log table result in Splunk Search view.

**⚠️ Findings**

* administrator account shows multiple failed logins from 192.168.56.101 → possible brute-force attempt.
* guest account locked due to repeated failures → targeted login attempts.



📸 **Figure-7:** Highlight showing FailureReason="Bad password" and repeated attempts.

**🛡️ Recommendations**

* Implement **account lockout policy** to prevent brute-force attempts.
* Restrict login access to **known IP ranges only**.
* Configure Splunk **alert rule** to trigger when a user exceeds 5 failed logins within 10 minutes.

**✅ Conclusion**

Using **Splunk Enterprise**, we successfully analyzed failed login attempts and visualized them in dashboards.  
This method can be extended to detect brute-force activity, insider misuse, or compromised accounts.