🚨 Brute Force Attack Detection Using Splunk – SOC Analyst Project 🔍

🛡️ Project Objective:

Detect multiple failed login attempts (brute force) in a short time window, which may indicate an unauthorized access attempt on the system.

🧰 Tools & Technologies Used:

- 🔸 **Splunk (Free/Enterprise Trial)**
- 🔸 **Universal Forwarder (for log collection)**
- 🔸 **Windows Security Logs (Event ID 4625)**
- 🔸 **Linux auth.log (/var/log/auth.log)**
- 🔸 **Custom SPL Queries**
- 🔸 **Dashboard Studio for visualization**
- 🔸 **Alerting system (Email/Slack)**

📊 What I Did:

☑ Set up log forwarding from Windows & Linux
☑ Ingested logs into Splunk (`index=os_logs`)
☑ Wrote SPL query to detect >5 failed login attempts within 5 minutes
☑ Built an interactive dashboard showing:

- Top attacker IPs
- Users targeted
- Time of attack
  ☑ Created real-time alerts when brute-force attempts are detected

🔎 SPL Query Used (Snippet):

```
index=os_logs sourcetype=WinEventLog:Security OR sourcetype=linux_secure
(EventCode=4625 OR message="Failed password")
| bucket _time span=5m
| stats count by src_ip, user, _time
| where count > 5
```

📌 Skills Demonstrated:

- SOC operations
- Threat detection logic
- Log analysis (Windows/Linux)
- Dashboarding & reporting
- Real-time alerting in Splunk

📁 Check out the full project on GitHub 👉 : https://github.com/UppalavenkataSai

🔍 Purpose:

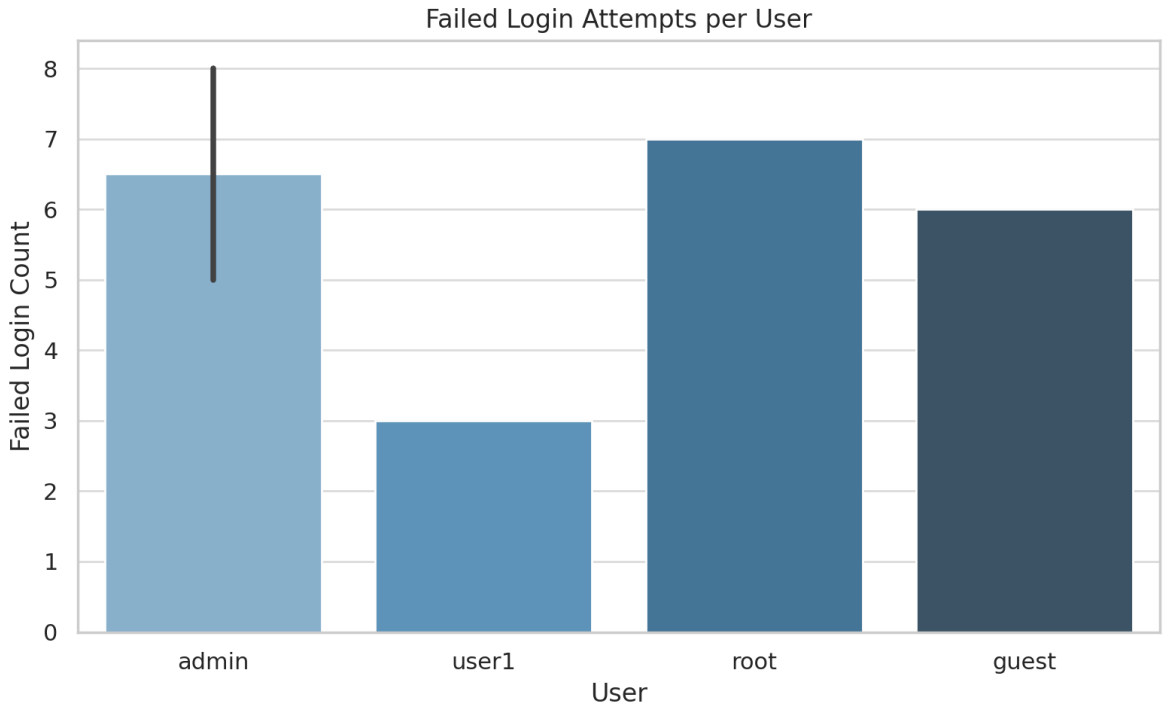
This bar chart visualizes the **total number of failed login attempts** grouped by **source IP addresses**.

🧠 What it tells you:

- Which IP addresses are attempting to brute-force login access.
- Helps identify **suspicious IPs** repeatedly trying to access the system.
- Can be used to trigger alerts or add those IPs to a firewall denylist.

☑ Use Case in SOC:

Security analysts use this data to block malicious IPs or investigate further if the IPs belong to external or internal networks.



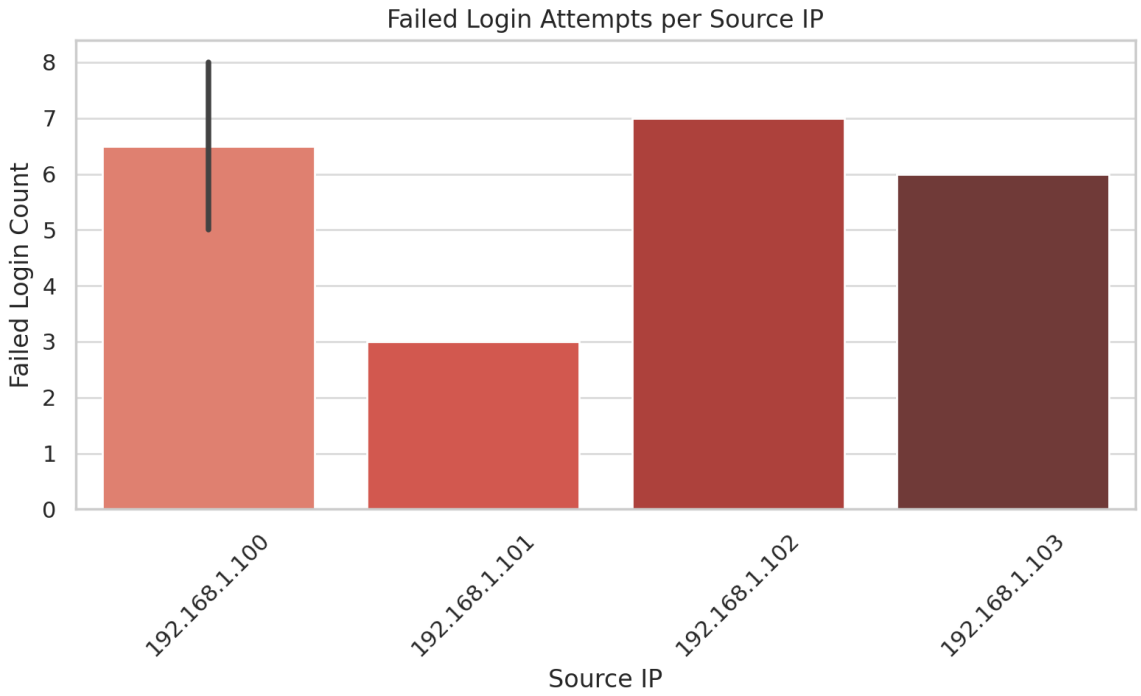
🖼️ 2. Failed Login Attempts per User

🔍 Purpose:
This bar chart shows which **usernames** are being targeted with failed login attempts.

🧠 What it tells you:

- Which user accounts are under brute-force attack.
- Could help detect if someone is targeting **privileged users** like `admin`, `root`, or `service` accounts.
- Indicates potential **insider threats** or **external attacks** aiming to guess credentials.

☑️ Use Case in SOC:
Used to lock or monitor specific user accounts under attack. Also helps enforce MFA or password resets for targeted accounts.



🖼️ 3. Failed Login Attempts Over Time

🔍 **Purpose:**
This line chart shows the **trend of failed login attempts over time** (time-series view).

🧠 **What it tells you:**

- Whether the brute-force attempts are **spiking at specific times** (e.g., midnight attacks).
- Helps correlate events during **incident response**.
- Reveals patterns like continuous vs. burst brute-force attacks.

☑️ **Use Case in SOC:**
Allows analysts to detect time-based attack patterns and correlate with other events like firewall blocks, endpoint detection alerts, or user complaints.