# SOC Detection Lab - Basic Brute Force Detection

## Objective

To demonstrate basic detection of failed login attempts using Splunk SIEM.

## Tools Used

- Splunk Free

- Windows Security Log dataset (Event ID 4625)

## Procedure

1. Installed Splunk locally and uploaded sample Windows logs.

2. Searched failed logins using `index="soc\_lab" EventCode=4625`.

3. Created detection rule to find accounts with >5 failed logins.

4. Configured alert named "Brute Force Detection".

## Result

Successfully identified repeated failed logins for specific users.

## Screenshots

- Splunk Dashboard

- Log Upload Success

- Search Query Result

- Brute Force Alert Configuration

## Conclusion

This proves ability to use SIEM tools to detect brute-force login attempts.