

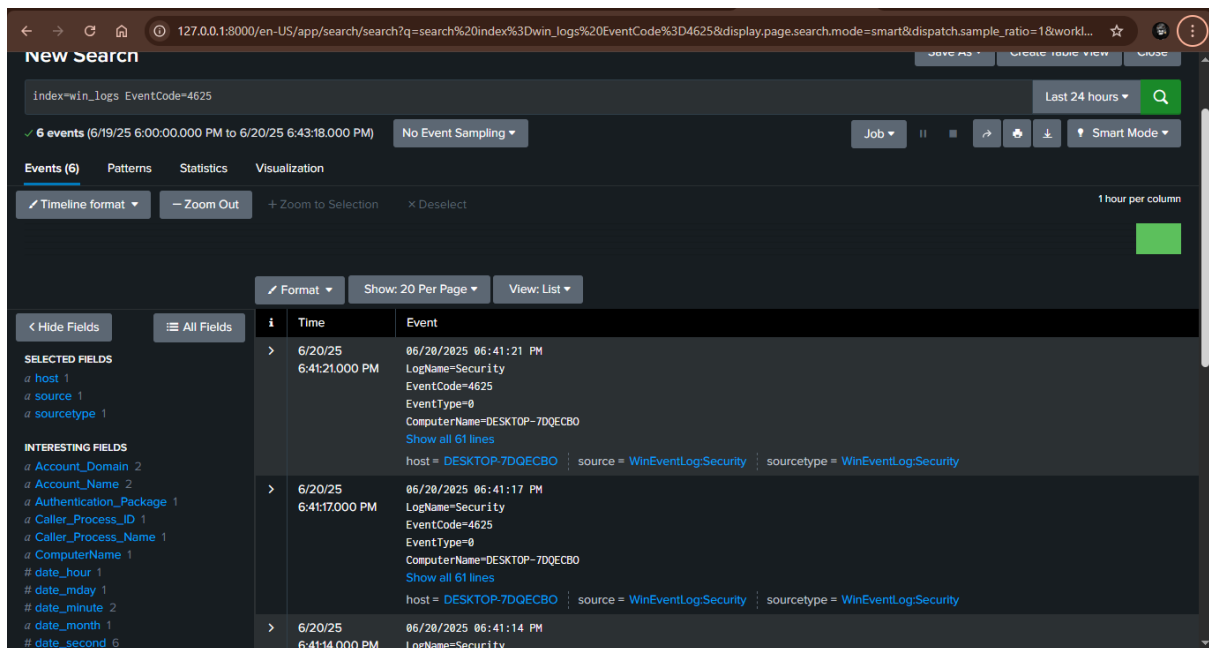
Simple Windows Log Analysis Using Splunk

Performed a basic analysis of Windows system logs using **Splunk** in window 10, identifying potential security anomalies and gaining insights into user and system behaviour.

- Access the dashboard via `http://localhost:8000`.
- **Indexer IP** (Splunk server)
- **Monitored logs** (choose: Security, System, Application)
- **Enable Event Log Forwarding**
- Ensure these logs are selected:
 - `WinEventLog://Security`
 - `WinEventLog://System`
 - `WinEventLog://Application`

➤ Failed Logon Attempts

`index=main sourcetype=WinEventLog:Security EventCode=4625`



The screenshot displays the Splunk search interface. The search bar contains the query `index=win_logs EventCode=4625`. The results are shown in a table format with columns for Time and Event. The table lists three failed logon attempts on 6/20/25.

Time	Event
6/20/25 6:41:21.000 PM	06/20/2025 06:41:21 PM LogName=Security EventCode=4625 EventType=0 ComputerName=DESKTOP-7DQECBO Show all 61 lines host = DESKTOP-7DQECBO source = WinEventLog:Security sourcetype = WinEventLog:Security
6/20/25 6:41:17.000 PM	06/20/2025 06:41:17 PM LogName=Security EventCode=4625 EventType=0 ComputerName=DESKTOP-7DQECBO Show all 61 lines host = DESKTOP-7DQECBO source = WinEventLog:Security sourcetype = WinEventLog:Security
6/20/25 6:41:14.000 PM	06/20/2025 06:41:14 PM LogName=Security

➤ Successful Logons

index=main sourcetype=WinEventLog:Security EventCode=4624

New Search

index=win_logs EventCode=4624 Last 24 hours Q

✓ 12 events (6/19/25 6:00:00.000 PM to 6/20/25 6:42:45.000 PM) No Event Sampling Job || ↶ ↷ ⬇ Smart Mode

Events (12) Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection x Deselect 1 hour per column

Format Show: 20 Per Page View: List

< Hide Fields All Fields

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Account_Domain 3
- a Account_Name 3
- a Authentication_Package 1
- a ComputerName 1
- # date_hour 1
- # date_mday 1
- # date_minute 4
- a date_month 1
- # date_second 5

i	Time	Event
>	6/20/25 6:41:26.000 PM	06/20/2025 06:41:26 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-7DQECBO Show all 70 lines host = DESKTOP-7DQECBO source = WinEventLog:Security sourcetype = WinEventLog:Security
>	6/20/25 6:41:26.000 PM	06/20/2025 06:41:26 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-7DQECBO Show all 70 lines host = DESKTOP-7DQECBO source = WinEventLog:Security sourcetype = WinEventLog:Security

New Search

index=win_logs EventCode=4624 Last 24 hours Q

✓ 12 events (6/19/25 6:00:00.000 PM to 6/20/25 6:42:45.000 PM) No Event Sampling Job || ↶ ↷ ⬇ Smart Mode

Events (12) Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection x Deselect 1 hour per column

Format Show: 20 Per Page View: List

< Hide Fields All Fields

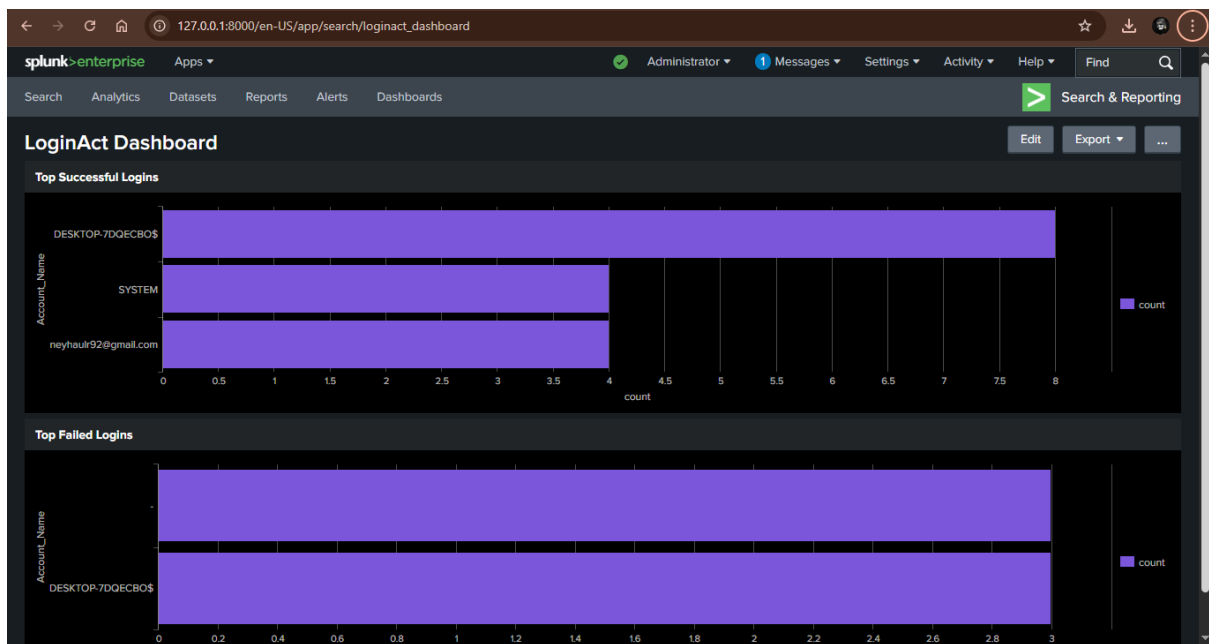
SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- a Account_Domain 3
- a Account_Name 3
- a Authentication_Package 1
- a ComputerName 1
- # date_hour 1
- # date_mday 1
- # date_minute 3
- a date_month 1
- # date_second 4
- a date_wday 1
- # date_year 1
- a date_zone 1
- a Elevated-Token 2
- # EventCode 1
- # EventType 1
- a Impersonation_Level 1
- a index 1
- # Key_Length 1
- a Keywords 1
- # linecount 1
- a Linked_Logon_ID 5
- a LogName 1
- a Logon_GUID 1
- a Logon_ID 5
- a Logon_Process 3

i	Time	Event
>	6/20/25 6:37:44.000 PM	06/20/2025 06:37:44 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-7DQECBO Show all 70 lines host = DESKTOP-7DQECBO source = WinEventLog:Security sourcetype = WinEventLog:Security
>	6/20/25 6:36:48.000 PM	06/20/2025 06:36:48 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-7DQECBO Show all 70 lines host = DESKTOP-7DQECBO source = WinEventLog:Security sourcetype = WinEventLog:Security
>	6/20/25 6:36:48.000 PM	06/20/2025 06:36:48 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-7DQECBO Show all 70 lines host = DESKTOP-7DQECBO source = WinEventLog:Security sourcetype = WinEventLog:Security
>	6/20/25 6:36:48.000 PM	06/20/2025 06:36:48 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-7DQECBO Show all 70 lines host = DESKTOP-7DQECBO source = WinEventLog:Security sourcetype = WinEventLog:Security



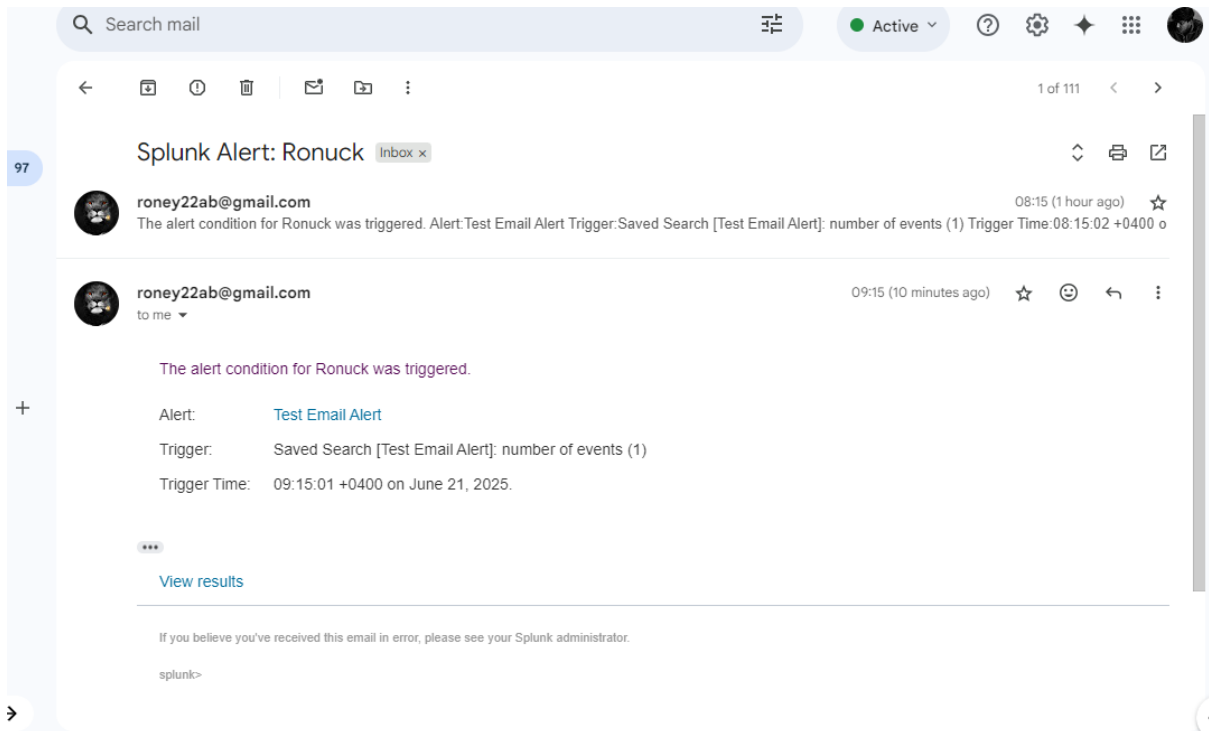
The dashboard LoginAct showing the bar chart result of the window logins

➤ Observations

Set up an email alert after each login attempt

The screenshot shows the 'Save As Alert' dialog box in Splunk. The 'When triggered' dropdown is set to 'Send email'. The 'To' field contains 'neyhauir92@gmail.com'. The 'Priority' is set to 'Normal'. The 'Subject' is 'Splunk Alert: Ronuck'. The 'Message' field contains 'The alert condition for Ronuck was triggered.' The 'Save' button is highlighted in green.

The screenshot shows the 'Test Email Alert' configuration page. The 'Enabled' checkbox is checked. The 'App' is set to 'search'. The 'Permissions' are set to 'Private, Owned by ronuck'. The 'Modified' date is 'Jun 20, 2025 7:02:54 PM'. The 'Alert Type' is 'Scheduled, Hourly, at 15 minutes past the hour'. The 'Trigger Condition' is '.. Number of Results is > 0'. The 'Actions' section shows '1 Action' with 'Send email' selected. A message at the bottom states: 'There are no fired events for this alert.'



Proof of the alert created for logins

➤ Observations

- High number of failed logon attempts with Status: 0xC000006D (bad username/password).
- PowerShell process triggered by non-admin user — flagged for review.
- Enable account lockout policy after 5 failed attempts.
- Restrict PowerShell execution to administrator roles.
- Monitor off-hours logins with alerts.
- Schedule Splunk alerts for:
 - Multiple failed logins in 15 mins every hour