

Splunk SOC Lab – Log Generation, Detection & Dashboard

BY:- KAVINDRA PATEL

Project Objective

Content :

- ▶ Simulated real –world security logs
- ▶ Detected brute-force login attempts
- ▶ Analyzed Windows Event IDs
- ▶ Build security monitoring dashboard in Splunk

Lab Setup

Lab Architecture:

- ▶ Host Machine : Windows 11
- ▶ Target Server : Windows Server 2019
- ▶ Attacker Machine : kali Linux
- ▶ SIEM Tool: Splunk Enterprise
- ▶ Log Collector: Splunk Universal Forwarder

Installation & Setup

Install Splunk Enterprise :

- ▶ Go to official Splunk website
- ▶ Click Free Trial/Free Downloads
- ▶ Create Register Account
- ▶ Login to your Splunk Account & Download Splunk Enterprise
- ▶ After Installation configure admin username & password
- ▶ Splunk Web via **<https://localhost:8000>**

Universal Forwarder Setup

- ▶ Downloaded Splunk Universal Forwarder
- ▶ Install universal forwarder on windows
- ▶ Configured log forwarding to Splunk SIEM

Brute Force –Failed Login Attempts Generation

- ▶ Used Kali Linux to simulate brute-force attack
- ▶ Targeted Windows Server RDP service
- ▶ Executed Hydra tool with username and password wordlistndows Server RDP service
- ▶ **Command Used:**
- ▶ **hydra -V -f -l administrator -P rockyou.txt rdp://192.168.232.131 (target ip)**

Verifying Generated Logs in Windows Event Viewer

- ▶ Logged into Target Windows Server
- ▶ Opened **Event Viewer**
- ▶ Navigated to:
Windows Logs → Security
- ▶ Filtered for **Event ID 4625 (Failed Login)**
- ▶ Verified multiple failed login events generated by brute-force attack
- ▶ Save all Events for file

How to add data in Splunk

- ▶ Go to :Settings → Add Data , Click : Upload
- ▶ Click: Select File → Choose your .log or .txt file
- ▶ Click Next
- ▶ Source Typ:If it's a normal log → choose auto-detect
- ▶ Or manually select appropriate sourcetype
- ▶ Choose: Default
- ▶ Last : Review
- ▶ Start Searching

How to Use SPL Queries

STEP BY STEP

source="security.evtx" host="WINB89000131DR"sourcetype="WinEventLog:Security"
EventCode="4624"

(4624 Successful Logon)

source="security.evtx" EventCode="4624" | Time range: All time ▾  

✓ 99 events (before 08/02/2026 11:18:13.000) No Event Sampling ▾ Job ▾ || ▶ ⌂ ⌄ Smart Mode ▾

Events (99) Patterns Statistics Visualization

Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect 1 minute per column

Format ▾ Show: 20 Per Page ▾ View: List ▾ < Prev 1 2 3 4 5 Next

Time	Event
30/01/2026 09:58:27.000	01/30/2026 09:58:27.799 AM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-B89000131DR Show all 70 lines host = WIN-B89000131DR source = security.evtx sourcetype = WinEventLog:Security
30/01/2026 09:58:27.000	01/30/2026 09:58:27.799 AM LogName=Security EventCode=4624 EventType=0 ComputerName=WIN-B89000131DR Show all 70 lines host = WIN-B89000131DR source = security.evtx sourcetype = WinEventLog:Security

< Hide Fields  All Fields i

SELECTED FIELDS
[host](#) 1
[source](#) 1
[sourcetype](#) 1

INTERESTING FIELDS
[Account_Domain](#) 7
[Account_Name](#) 11
[Authentication_Package](#) 2
[ComputerName](#) 1
[Elevated_Token](#) 2
[EventCode](#) 1
[EventType](#) 1
[Impersonation_Level](#) 2
[index](#) 1

source=" security.evtx" host="WINB89000131DR"sourcetype="WinEventLog:Security"
EventCode="4625"

(4625 = Failed Logon)

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** source="security.evtx" EventCode="4625"
- Results Summary:** 39 events (before 08/02/2026 11:16:34.000) | No Event Sampling
- Time Range:** All time
- Event List:** The results table displays two event entries from January 29, 2026, at 09:58:22.000. Both events have the following fields:
 - host = WIN-B89000131DR
 - source = security.evtx
 - sourcetype = WinEventLog:Security
 - Time: 01/29/2026 09:58:22.175 AM
 - LogName=Security
 - EventCode=4625
 - EventType=0
 - ComputerName=WIN-B89000131DR
- Fields Panel:** Shows selected fields (host, source, sourcetype) and interesting fields (Account_Domain, Account_Name, Authentication_Package, Caller_Process_ID, Caller_Process_Name, ComputerName, EventCode, EventType, Failure_Reason).

```
source="security.evtx" host="WINB89000131DR"  
sourcetype="WinEventLog:Security" | sort -_time  
|
```

sort Events by Time(Most Recent First)

The screenshot shows a Splunk search interface with the following details:

- Search Bar:** source="security.evtx" | sort -_time
- Time Range:** All time
- Event Count:** 798 events (before 08/02/2026 11:15:02.000)
- Sampling:** No Event Sampling
- Job Status:** Job 1
- Visualization:** Timeline format (1 hour per column)
- Event List:** The list displays two events from 30/01/2026 at 10:07:05.728 AM. Both events have LogName=Security, EventCode=4798, EventType=0, and ComputerName=WIN-B89000131DR. The first event also includes host = WIN-B89000131DR, source = security.evtx, and sourcetype = WinEventLog:Security.
- Selected Fields:** host 1, source 1, sourcetype 1
- Interesting Fields:** Account_Domain 7, Account_Name 13, Algorithm_Name 4, ComputerName 1, EventCode 24, EventType 3, index 1, Key_Name 5, Key_Type 2

source=" security.evtx" host="WINB89000131DR"
sourcetype="WinEventLog:Security" Account_Name="Administrator"

(Filter by Username)

source="security.evtx" Account_Name="Administrator"

Time range: All time ▾

159 events (before 08/02/2026 11:13:30.000) No Event Sampling ▾

Job ▾ II Smart Mode ▾

Events (159) Patterns Statistics Visualization

Timeline format ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per color

Format ▾ Show: 20 Per Page ▾ View: List ▾

< Prev 1 2 3 4 5 6 7 8 Next

Time	Event
30/01/2026 10:07:05.728 AM 10:07:05.000	LogName=Security EventCode=4798 EventType=0 ComputerName=WIN-B89000131DR Show all 27 lines host = WIN-B89000131DR source = security.evtx sourcetype = WinEventLog:Security
30/01/2026 10:07:05.728 AM 10:07:05.000	LogName=Security EventCode=4798 EventType=0 ComputerName=WIN-B89000131DR Show all 27 lines host = WIN-B89000131DR source = security.evtx sourcetype = WinEventLog:Security

◀ Hide Fields All Fields

SELECTED FIELDS

- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- Account_Domain 3
- Account_Name 4
- Authentication_Package 2
- Caller_Process_ID 1
- Caller_Process_Name 1
- ComputerName 1
- EventCode 11
- EventType 2
- Failure_Reason 1

```
source=" security.evtx" host="WINB89000131DR"  
sourcetype="WinEventLog:Security" | top limit = 10 EventCode
```

(Top 10 EventCodes)

New Search

source="security.evtx" | top limit=10 EventCode

798 events (before 08/02/2026 11:11:38.000) No Event Sampling

Save As ▾ Create Table View Close

Time range: All time ▾

EventCode	count	percent
5379	246	30.827068
4624	99	12.406015
5061	96	12.030075
5058	96	12.030075
4672	90	11.278195
4625	39	4.887218
4688	33	4.135338
4799	27	3.383459
4648	18	2.255639
5059	6	0.751880

```
source=" security.evtx" host="WINB89000131DR"  
sourcetype="WinEventLog:Security" | stats count by SourceName
```

(Group Events by Source and Count)

New Search

Save As ▾ Create Table View Close

source="security.evtx" | stats count by SourceName

Time range: All time ▾

798 events (before 08/02/2026 11:07:16.000) No Event Sampling ▾ Job ▾

Events Patterns Statistics (2) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

SourceName	count
Microsoft Windows security auditing.	792
Microsoft-Windows-Eventlog	6

```
source=" security.evtx" host="WINB89000131DR"  
sourcetype="WinEventLog:Security" | timechart span=1h count
```

EventsOverTime(Hourly)

The screenshot shows the Splunk Enterprise search interface with the following details:

- Search Bar:** The search query is `source="security.evtx" | timechart span=1h count`. The results show 798 events found before 08/02/2026 11:05:55.000.
- Statistics View:** The **Statistics (26)** tab is selected. The results table displays hourly event counts for January 29, 2026. The data is as follows:

Time	Count
2026-01-29 09:00	51
2026-01-29 10:00	0
2026-01-29 11:00	0
2026-01-29 12:00	0
2026-01-29 13:00	0
2026-01-29 14:00	0
2026-01-29 15:00	0
2026-01-29 16:00	0

```
source=" security.evtx" host="WINB89000131DR"  
sourcetype="WinEventLog:Security" | stats count by ComputerName | sort-count  
(Sort by ComputerName)
```

← → ⌂ ⓘ 127.0.0.1:8000/en-GB/app/search/search?q=search%20source%3D"security.evtx"%20%7C%20stats%20count%20by%20ComputerName%20%7C%20sort-count&display.page.search.mode=smart&... 🔎 ⭐ ⓘ

New Search

Save As ▾ Create Table View Close

New Search
source="security.evtx" | stats count by ComputerName | sort-count

Time range: All time ▾

798 events (before 08/02/2026 11:04:42.000) No Event Sampling ▾

Job ▾ II ■ ↻ ↺ Smart Mode ▾

Events Patterns Statistics (1) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

ComputerName	count
WIN-B89000131DR	798

source=" security.evtx" host="WINB89000131DR"
sourcetype="WinEventLog:Security" | table_time,EventCode,Message
(See Message Details for Each Event)

New Search

source="security.evtx" | table_time,Eventcode,Message

798 events (before 08/02/2026 11:02:15.000) No Event Sampling

Save As ▾ Create Table View Client

Time range: All time ▾

Events Patterns Statistics (798) Visualization

Show: 20 Per Page ▾ Format Preview: On

1 2 3 4 5 6 7 8 ...

_time	Eventcode	Message
2026-01-30 07:49:58		An account was successfully logged on.
		Subject:
		Security ID: NT AUTHORITY\SYSTEM
		Account Name: WIN-B89000131DR\$
		Account Domain: WORKGROUP
		Logon ID: 0x3E7
		Logon Information:
		Logon Type: 5
		Restricted Admin Mode: -
		Virtual Account: Yes
		Elevated Token: Yes
		Impersonation Level: Impersonation
		New Logon:
		Security ID: NT SERVICE\Splunkd

source=" security.evtx" host="WINB89000131DR"
sourcetype="WinEventLog:Security" EventCode=4740

(AccountLockouts)

monitor users who were locked out due to repeated login failures

← → ⌂ ⓘ 127.0.0.1:8000/en-GB/app/search/search?q=search%20source%3D"security.evtx"%20EventCode%3D4740&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=0&lat... ⭐ ⓘ

New Search

source="security.evtx" EventCode=4740

3 events (before 08/02/2026 11:00:50.000) No Event Sampling

Events (3) Patterns Statistics Visualization

Timeline format - Zoom Out + Zoom to Selection × Deselect

1 millisecond per column

Format Show: 20 Per Page View: List

i	Time	Event
>	29/01/2026 09:58:22.000	01/29/2026 09:58:22.170 AM LogName=Security EventCode=4740 EventType=0 ComputerName=WIN-B89000131DR Show all 25 lines host = WIN-B89000131DR source = security.evtx sourcetype = WinEventLog:Security
>	29/01/2026 09:58:22.000	01/29/2026 09:58:22.170 AM LogName=Security EventCode=4740 EventType=0 ComputerName=WIN-B89000131DR Show all 25 lines host = WIN-B89000131DR source = security.evtx sourcetype = WinEventLog:Security

Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 1
a Account_Name 2
a Caller_Computer_Name 1
a ComputerName 1
EventCode 1
EventType 1
a index 1
a Keywords 1
linecount 1

source="security.evtx" host="WINB89000131DR"
sourcetype="WinEventLog:Security" EventCode=4720

(New Users Creation)

← → ⌂ ⓘ 127.0.0.1:8000/en-GB/app/search/search?q=search%20source%3D"security.evtx"%20EventCode%3D4720&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=0&lat... ☆ k

splunk>enterprise Apps ▾

Administrator 1 Messages Settings Activity Help Find Search

Search Analytics Datasets Reports Alerts Dashboards Modules > Search & Reporting

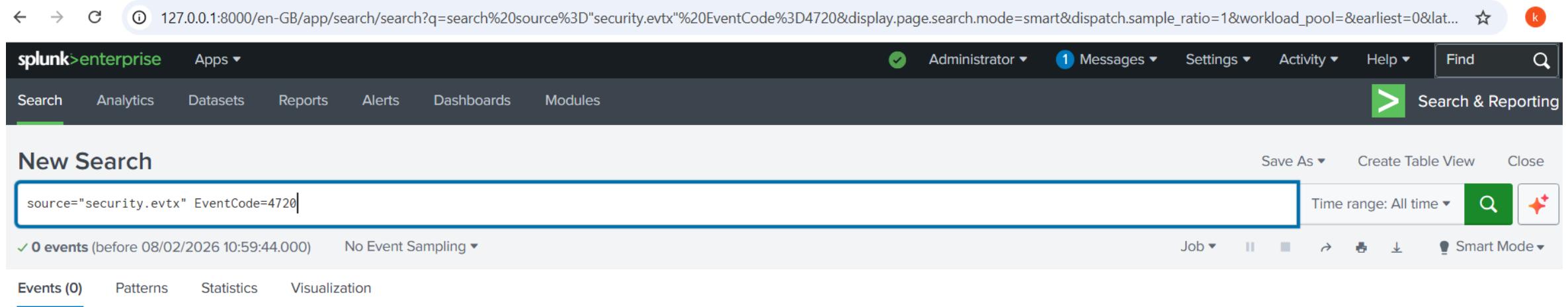
New Search Save As Create Table View Close

source="security.evtx" EventCode=4720 Time range: All time

✓ 0 events (before 08/02/2026 10:59:44.000) No Event Sampling Job Smart Mode

Events (0) Patterns Statistics Visualization

No results found.



source=" security.evtx" host="WINB89000131DR"
sourcetype="WinEventLog:Security" EventCode=4728

(User Added to Admin Group)

Alert on privilege escalation attempts.

← → ⌂ ⓘ 127.0.0.1:8000/en-GB/app/search/search?q=search%20source%3D"security.evtx"%20EventCode%3D4728&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=0&lat... ☆ ⓘ

splunk>enterprise Apps ▾

Administrator 1 Messages Settings Activity Help Find

Search Analytics Datasets Reports Dashboards Modules > Search & Reporting

New Search Save As Create Table View Close

source="security.evtx" EventCode=4728 Time range: All time

✓ 0 events (before 08/02/2026 10:58:45.000) No Event Sampling Job II ⏪ ⏴ ⏵ Smart Mode

Events (0) Patterns Statistics Visualization

No results found.

source=" security.evtx" host="WINB89000131DR"
sourcetype="WinEventLog:Security" EventCode=4624 Logon_Type=10

(Remote Logon Detection)

← → ⌂ ⓘ 127.0.0.1:8000/en-GB/app/search/search?q=search%20source%3D"security.evtx"%20EventCode%3D4624%20Logon_Type%3D10&display.page.search.mode=smart&dispatch.sample_ratio=1&workload... ☆ k

splunk>enterprise Apps ▾

Administrator 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Search

Search Analytics Datasets Reports Alerts Dashboards Modules > Search & Reporting

New Search

Save As ▾ Create Table View Close

source="security.evtx" EventCode=4624 Logon_Type=10 Time range: All time ▾

0 events (before 08/02/2026 10:53:27.000) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events (0) Patterns Statistics Visualization

No results found.

source=" security.evtx" host="WINB89000131DR"
sourcetype="WinEventLog:Security" EventCode=1102

(Clearing of EventLogs)

suspicious:someone tried to cover their tracks by clearing logs.

← → ⌂ ⓘ 127.0.0.1:8000/en-GB/app/search/search?q=search%20source%3D"security.evtx"%20EventCode%3D1102&display.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&earliest=0&lat... ☆ ⓘ

New Search

Save As ▾ Create Table View Close

source="security.evtx" EventCode=1102 Time range: All time ▾

3 events (before 08/02/2026 10:55:56.000) No Event Sampling ▾ Job ▾

Events (3) Patterns Statistics Visualization

Timeline format ▾ – Zoom Out + Zoom to Selection × Deselect 1 millisecond per column

Format Show: 20 Per Page ▾ View: List ▾

Time	Event
29/01/2026 09:57:13.000	01/29/2026 09:57:13.445 AM LogName=Security EventCode=1102 EventType=4 ComputerName=WIN-B89000131DR Show all 17 lines host = WIN-B89000131DR source = security.evtx sourcetype = WinEventLog:Security
29/01/2026 09:57:13.000	01/29/2026 09:57:13.445 AM LogName=Security EventCode=1102 EventType=4 ComputerName=WIN-B89000131DR Show all 17 lines host = WIN-B89000131DR source = security.evtx sourcetype = WinEventLog:Security

< Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Name 1
a ComputerName 1
a Domain_Name 1
EventCode 1
EventType 1
a index 1
a Keywords 1
linecount 1
a LogName 1

```
source=" security.evtx" host="WINB89000131DR"sourcetype="WinEventLog:Security"  
EventCode=4625 | stats count by Account_Name,Workstation_Name
```

(Top Failed Logins)

see which users or systems are generating the most failures

← → ⌂ ⓘ 127.0.0.1:8000/en-GB/app/search/search?q=search%20source%3D"security.evtx"%20%7C%20stats%20count%20by%20Account_Name%2C%20Workstation_Name&display.page.search.mode=smart&di... ⭐ ⓘ

source="security.evtx" | stats count by Account_Name, Workstation_Name Time range: All time

✓ 798 events (before 08/02/2026 10:47:24.000) No Event Sampling Job || □ □ □ □ □ Smart Mode

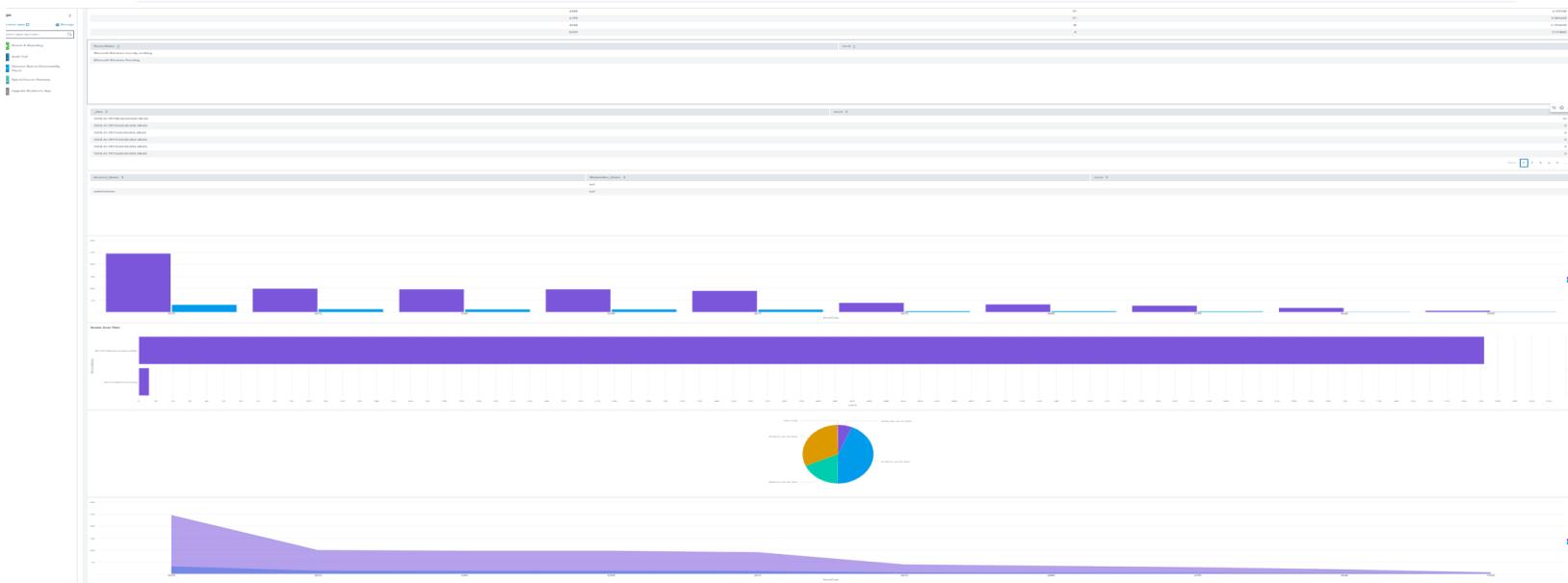
Events Patterns Statistics (14) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

Account_Name	Workstation_Name	count
-	-	3
-	kali	39
Administrator	WIN-B89000131DR	3
DWM-1	-	6
LOCAL SERVICE	-	3
NETWORK SERVICE	-	3
SYSTEM	-	72
SplunkForwarder	-	3
Splunkd	-	3
UMFD-0	-	3
UMFD-1	-	3
WIN-B89000131DR\$	-	93
WIN-B89000131DR\$	WIN-B89000131DR	3
administrator	kali	39

Security Monitoring Dashboard

- ▶ This dashboard was created to monitor brute-force failed login attempts in real-time.
- ▶ It visualizes security logs collected from Windows Server using Splunk SIEM.



Conclusion

- ▶ Successfully simulated brute-force attack in controlled lab environment
- ▶ Generated and analyzed Windows Security logs (Event ID 4625)
- ▶ Detected suspicious login activity using SPL queries
- ▶ Designed a real-time security monitoring dashboard
- ▶ Demonstrated practical understanding of SIEM implementation