Brute Force Authentication Detection Using Splunk

By Adam Mohmoud

The objective of this project was to configure Splunk to ingest Windows Security Event Logs and develop a detection for brute force authentication attempts. The project focused on identifying repeated failed login attempts within short time windows and correlating authentication activity to detect potential credential-based attacks. This lab simulates a realistic SOC analyst workflow focused on log analysis and detection engineering.

Project Objectives:

- Ingest and validate Windows Security Event Logs in Splunk
- Identify failed authentication events (Event ID 4625)
- Analyze authentication behavior to detect brute force attempts
- Build time-based correlation logic using SPL
- Document findings in a SOC-style format

Tools & Technologies:

- Splunk Enterprise
- Windows Security Event Logs
- Search Processing Language (SPL)

MITRE ATT&CK Mapping

- T1110 Brute Force
- T1078 Valid Accounts (when successful logons follow failures)

Data Source:

Log Type: Windows Security Event Logs

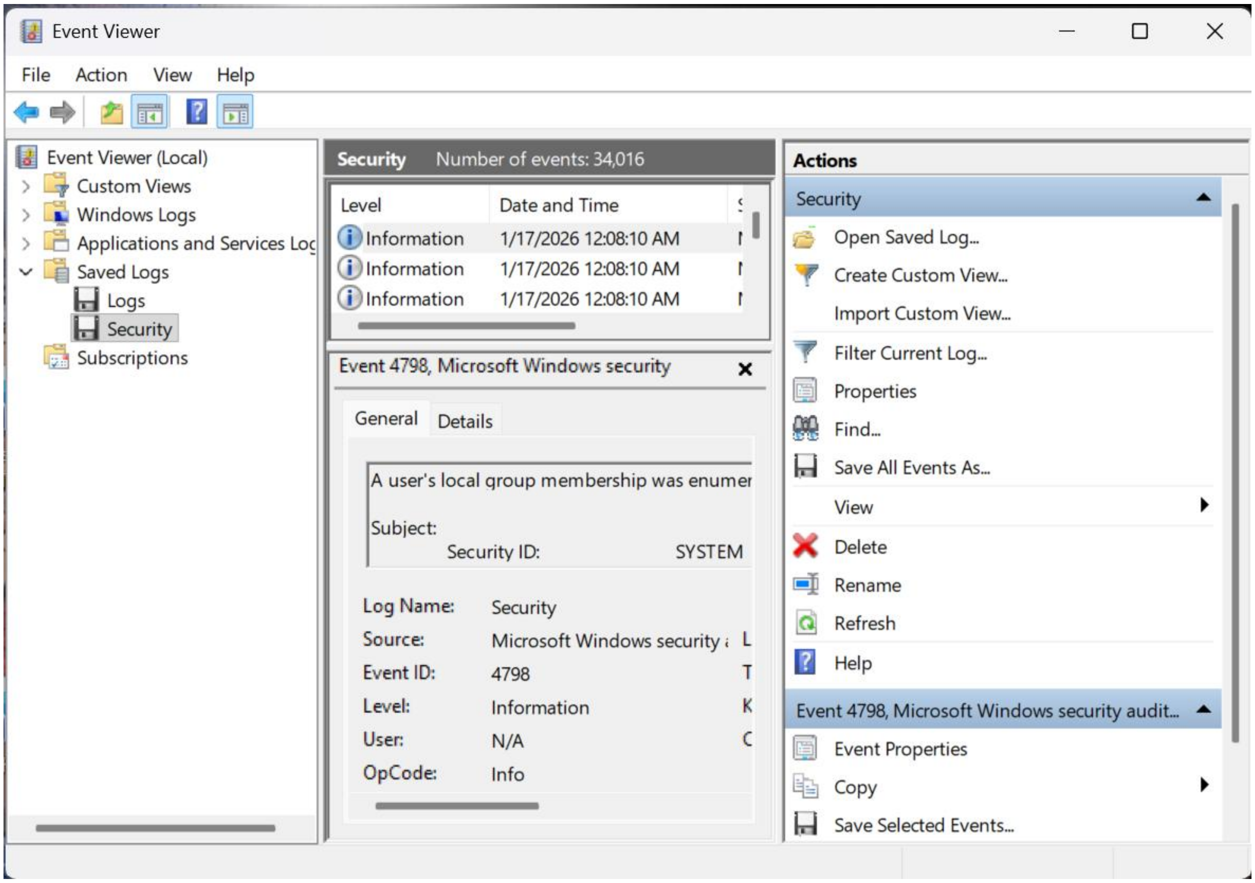
Collection Method: Local Event Logs input in Splunk

Relevant Event IDs:

- 4625 – Failed logon
- 4624 – Successful logon (used for correlation)

Step 1: Data Ingestion & Validation

Event Viewer → Navigate to **Windows Logs** → **Security** → Save as **.evtx**



Security Number of events: 34,016

Level	Date and Time
Information	1/17/2026 12:08:10 AM
Information	1/17/2026 12:08:10 AM
Information	1/17/2026 12:08:10 AM

Event 4798, Microsoft Windows security

A user's local group membership was enumer

Subject:
Security ID: SYSTEM

Log Name: Security
Source: Microsoft Windows security
Event ID: 4798
Level: Information
User: N/A
OpCode: Info

Splunk was configured to ingest Windows Security logs using the **Local Event Logs** input. This ensured proper parsing of '.evtx' data and automatic field extraction.

Validation steps included:

- Confirming '*WinEventLog:Security sourcetype*'
- Verifying human-readable event messages
- Ensuring authentication-related fields were extracted correctly

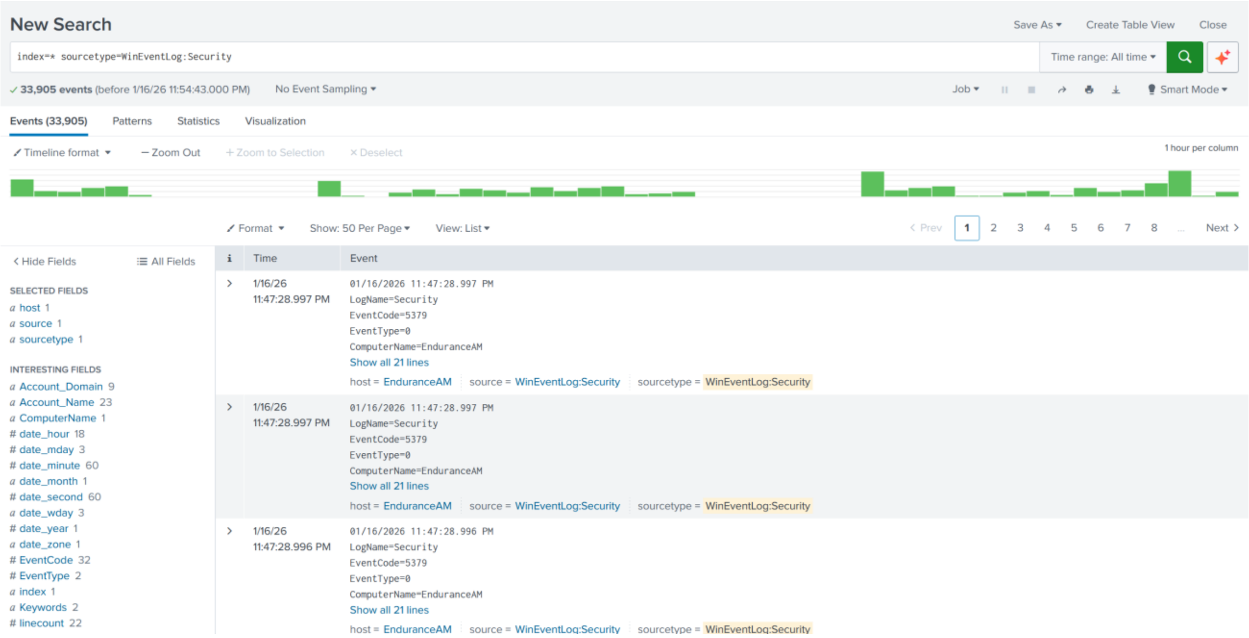
Validation SPL: `index=* sourcetype=WinEventLog:Security`

This confirms that authentication events, including failed logons, were present. This highlights four critical confirmations:

1. Data source is correct – The .evtx format is being parsed correctly and logs are not corrupted or binary. The SIEM is receiving the correct log source.
2. Security auditing is enabled – Authentication related logs are being actively logged; host is generating audit logs that can be analyzed.
3. Authentication events exist in the data – Within the expanded results, I saw fields like EventCode, Logon_Type, Account_Name, TargetUserName, Source_Network_Address.

These events are suitable for brute force attacks, therefore, we have the right telemetry to detect login attacks.

4. Field extraction works – The data is normalized enough to build detections.



```
index=* sourcetype=WinEventLog:Security
```

✓ **33,905 events** (before 1/16/26 11:54:43.000 PM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a Account_Domain 9
a Account_Name 23
a ComputerName 1
# date_hour 18
# date_mday 3
# date_minute 60
a date_month 1
# date_second 60
a date_wday 3
# date_year 1
a date_zone 1
EventCode 32
EventType 2
a index 1
a Keywords 2
# linecount 22

i	Time	Event

›	1/16/26
	11:47:28.997 PM
		01/16/2026 11:47:28.997 PM
		LogName=Security
		EventCode=5379
		EventType=0
		ComputerName=EnduranceAM
		Show all 21 lines
		host = EnduranceAM source = WinEventLog:Security sourcetype = WinEventLog:Security

›	1/16/26
	11:47:28.997 PM
		01/16/2026 11:47:28.997 PM
		LogName=Security
		EventCode=5379
		EventType=0
		ComputerName=EnduranceAM
		Show all 21 lines
		host = EnduranceAM source = WinEventLog:Security sourcetype = WinEventLog:Security

›	1/16/26
	11:47:28.996 PM
		01/16/2026 11:47:28.996 PM
		LogName=Security
		EventCode=5379
		EventType=0
		ComputerName=EnduranceAM
		Show all 21 lines
		host = EnduranceAM source = WinEventLog:Security sourcetype = WinEventLog:Security

Step 2: Identification of Failed Authentication Events

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

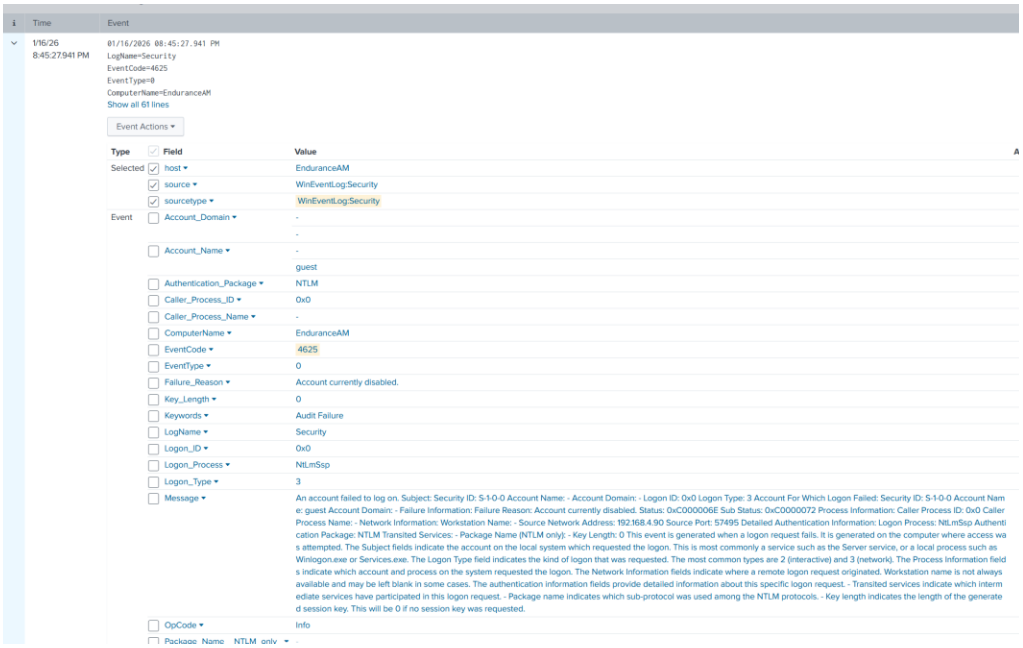
Failed logon activity was isolated using **Event ID 4625**, which represents unsuccessful login attempts.

Exploratory SPL: `index=* sourcetype=WinEventLog:Security EventCode=4625`

```
| table _time TargetUserName Source_Network Address Logon_Type ComputerName
Failure_Reason
```

This step provided visibility into:

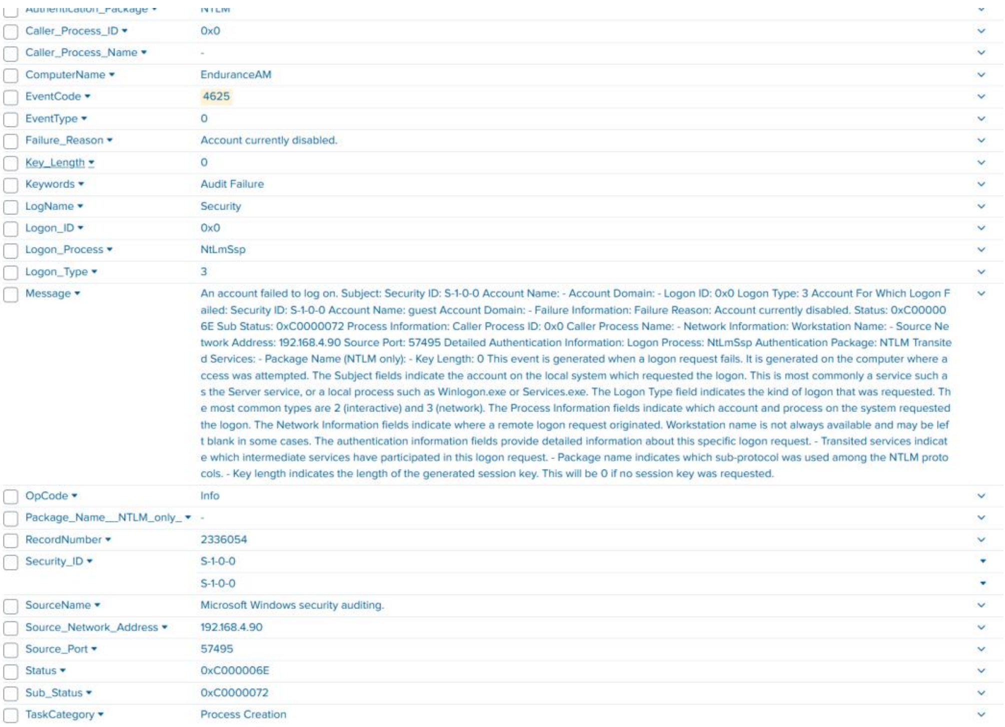
- Targeted user accounts
- Source IP addresses
- Logon types (e.g., network-based logons)
- Failure reasons such as disabled accounts or bad credentials



i	Time	Event

⌄	1/16/26
	8:45:27.941 PM
		01/16/2026 08:45:27.941 PM
		LogName=Security
		EventCode=4625
		EventType=0
		ComputerName=EnduranceAM
		Show all 61 lines

Type	☑ Field	Value
Selected	☑ host ▾	EnduranceAM
	☑ source ▾	WinEventLog:Security
	☑ sourcetype ▾	WinEventLog:Security
Event	□ Account_Domain ▾	- -
	□ Account_Name ▾	- guest
	□ Authentication_Package ▾	NTLM
	□ Caller_Process_ID ▾	0x0
	□ Caller_Process_Name ▾	-
	□ ComputerName ▾	EnduranceAM
	□ EventCode ▾	4625
	□ EventType ▾	0
	□ Failure_Reason ▾	Account currently disabled.
	□ Key_Length ▾	0
	□ Keywords ▾	Audit Failure
	□ LogName ▾	Security
	□ Logon_ID ▾	0x0
	□ Logon_Process ▾	NtLmSsp
	□ Logon_Type ▾	3
	□ Message ▾	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: guest Account Domain: - Failure Information: Failure Reason: Account currently disabled. Status: 0xC000006E Sub Status: 0xC0000072 Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: - Source Network Address: 192.168.4.90 Source Port: 57495 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
	□ OpCode ▾	Info
	□ Package_Name__NTLM_only_ ▾	-



□ Authentication_Package ▾	NTLM	⌄
□ Caller_Process_ID ▾	0x0	⌄
□ Caller_Process_Name ▾	-	⌄
□ ComputerName ▾	EnduranceAM	⌄
□ EventCode ▾	4625	⌄
□ EventType ▾	0	⌄
□ Failure_Reason ▾	Account currently disabled.	⌄
□ Key_Length ▾	0	⌄
□ Keywords ▾	Audit Failure	⌄
□ LogName ▾	Security	⌄
□ Logon_ID ▾	0x0	⌄
□ Logon_Process ▾	NtLmSsp	⌄
□ Logon_Type ▾	3	⌄
□ Message ▾	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: guest Account Domain: - Failure Information: Failure Reason: Account currently disabled. Status: 0xC000006E Sub Status: 0xC0000072 Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: - Source Network Address: 192.168.4.90 Source Port: 57495 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.	⌄
□ OpCode ▾	Info	⌄
□ Package_Name__NTLM_only_ ▾	-	⌄
□ RecordNumber ▾	2336054	⌄
□ Security_ID ▾	S-1-0-0 S-1-0-0	▾ ▾
□ SourceName ▾	Microsoft Windows security auditing.	⌄
□ Source_Network_Address ▾	192.168.4.90	⌄
□ Source_Port ▾	57495	⌄
□ Status ▾	0xC000006E	⌄
□ Sub_Status ▾	0xC0000072	⌄
□ TaskCategory ▾	Process Creation	⌄

Step 3: Performing Event Analysis

Failed authentication event revealed:

- Logon Type 3 (Network Logon)
- Source IP address attempting remote authentication
- Audit Failure classification (Access Attempt)

Step 4: Brute Force Detection Logic

To differentiate normal authentication errors from brute force activity, failed logons were correlated within a defined time window.

Detection SPL:

```
index=* sourcetype=WinEventLog:Security EventCode=4625
| bin _time span=5m
| stats count as failed_attempts by TargetUserName, Source_Network_Address,
ComputerName, _time
| where failed_attempts = 5
```

Detection Criteria:

- 5 or more failed logins
- Same source IP
- Same target account
- Within a 5-minute window

Note: This logic aligns with common SOC detection thresholds for brute force attacks.

Step 5: Enhanced Detection – Success After Failure

To increase detection fidelity, a correlation was added to identify successful logins following multiple failures.

Advanced SPL:

```
index=* sourcetype=WinEventLog:Security (EventCode=4625 or
EventCode=4624)
| stats
    count(eval(EventCode=4625)) as failures
    count(eval(EventCode=4624)) as successes
    by TargetUserName, Source_Network_Address, ComputerName
| where failures = 5 ; successes = 1
```

This pattern may indicate credential compromise following brute force activity.

Step 6: Visualization & Alerting

The detection results were visualized using tables and charts showing:

- Source IPs with the highest number of failures
- Targeted user accounts
- Failed authentication volume over time

The detection search was saved and configured as a Splunk alert to simulate a real SOC monitoring event per this project.