LOG ANALYSIS FOR THREATS

Indroduction

- **Network logs in Windows** are records that show what's happening with your computer's network connections
- Logs act as recorded evidence of system activities such as user authentication, service execution, and network communication.
- Studying logs helps establish a baseline of normal behavior, which is necessary before detecting suspicious activity or security incidents.
- Log analysis is a fundamental activity in cybersecurity that involves collecting, reviewing, and understanding logs generated by operating systems and networks.

PART A: Log Collection and Initial Analysis

---

1. Objective

- To collect logs from host and network sources.
- To understand how authentication and system events are recorded.
- To analyze a normal log event and interpret its meaning.
- To build familiarity with log fields and their security relevance.

---

2. Tools Used

- **Windows Event Viewer** (to access Windows Security logs)
- **Kali Linux Terminal** (to view Linux authentication logs)
- **Wireshark** (to capture and inspect network packets)
- **Manual analysis** (to interpret log entries)

---

3. Log Sources Used

3.1 Windows Security Logs

- Location: Event Viewer → Windows Logs → Security

- Type of logs:
    - Authentication events
    - Service logons
    - System-level activities

3.2 Linux Authentication Logs

- Location: cd /var/log
- Less auth.log (To look)
- Contains:
    - User login attempts
    - sudo usage
    - Authentication failures

3.3 Network Traffic Logs

- Captured using Wireshark.
- Includes:
    - DNS queries
    - TCP connections
    - TLS-encrypted traffic

---

4. Log Collection Process

- Opened Windows Event Viewer and navigated to Security logs.
- Identified authentication-related events.
- Viewed Linux authentication logs using terminal commands.
- Captured live network traffic by browsing normal websites and observing packets in Wireshark.

---

5. Windows Security Event Analysis (Event ID 4624)

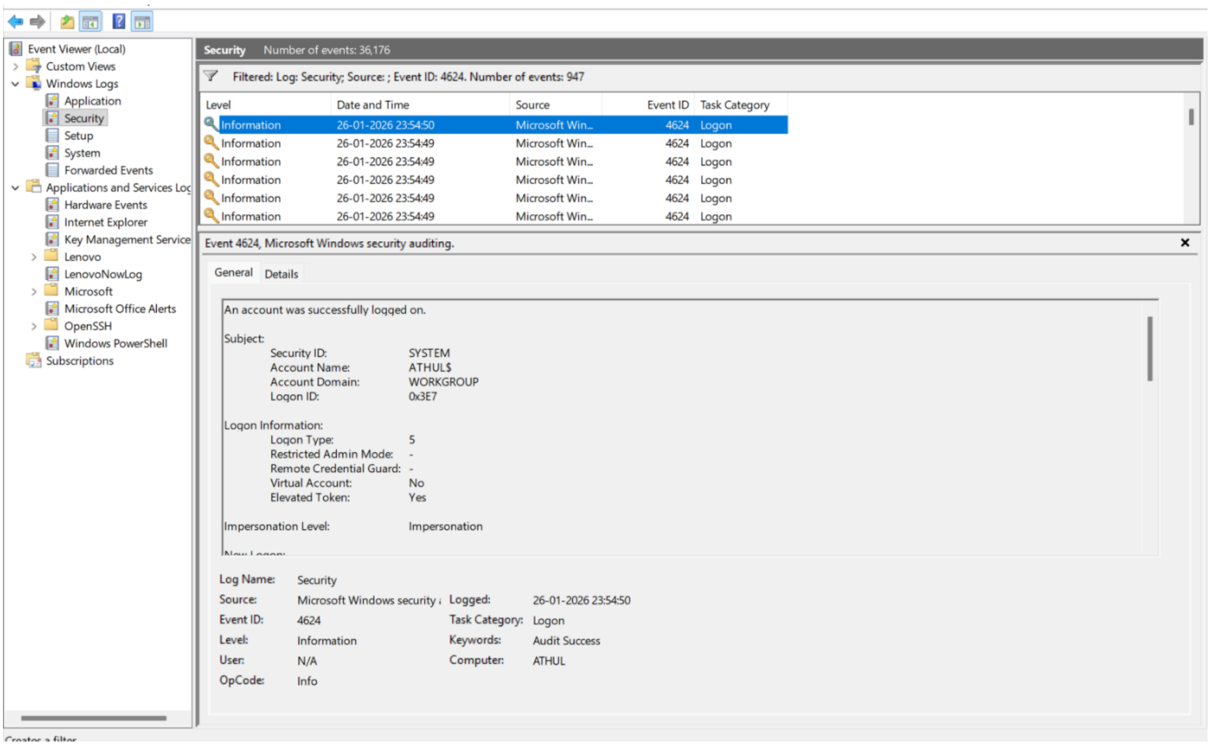
5.1 Event Overview

• **Event ID:** 4624 (Logon)
(Indicates a successful logon event)

- **Event Type:** Audit Success
(Authentication was completed successfully)

- **Event Category:** Logon
(Related to user or system authentication)

- **Log Name:** Security
- **Event Source:** Microsoft Windows Security Auditing
- **Date & Time:** 26-01-2026 23:54:50
- **Computer Name:** ATHUL



Security   Number of events: 36,176

Filtered: Log: Security; Source: ; Event ID: 4624. Number of events: 947

Level	Date and Time	Source	Event ID	Task Category
Information	26-01-2026 23:54:50	Microsoft Win...	4624	Logon
Information	26-01-2026 23:54:49	Microsoft Win...	4624	Logon
Information	26-01-2026 23:54:49	Microsoft Win...	4624	Logon
Information	26-01-2026 23:54:49	Microsoft Win...	4624	Logon
Information	26-01-2026 23:54:49	Microsoft Win...	4624	Logon
Information	26-01-2026 23:54:49	Microsoft Win...	4624	Logon

Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           ATHUL$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Information:
        Logon Type:             5
        Restricted Admin Mode:  -
        Remote Credential Guard: -
        Virtual Account:        No
        Elevated Token:         Yes

Impersonation Level:            Impersonation

New Logon:
```

Log Name:	Security		
Source:	Microsoft Windows security a	Logged:	26-01-2026 23:54:50
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	ATHUL
OpCode:	Info		

5.2 Detailed Event Fields Analysis

- **SubjectUserSid:** S-1-5-18
(Security Identifier for the local SYSTEM account)

- **SubjectUserName:** ATHUL$
(Machine account initiating the logon)

- **SubjectDomainName:** WORKGROUP
(Local system domain)

- **TargetUserSid:** S-1-5-18
(SYSTEM account being logged in)

- **TargetUserName:** SYSTEM
(Built-in Windows system account)

- **TargetDomainName:** NT AUTHORITY
(Windows internal authority domain)

- **LogonId:** 0x3E7
(Unique identifier for this logon session)

5.3 Logon Characteristics

- **LogonType:** 5
(Service logon – triggered when a Windows service starts)

- **LogonProcessName:** Advapi
(Windows API responsible for authentication processes)

- **AuthenticationPackageName:** Negotiate
(Windows automatically selected Kerberos or NTLM)

- **ImpersonationLevel:** Impersonation
(Process can act on behalf of the security context)

5.4 Process Information

- **ProcessName:** C:\Windows\System32\services.exe
(Windows Service Control Manager – legitimate system process)

- **ProcessId:** 0x638
(Unique identifier for the process during execution)

5.5 Network-Related Fields

- **IpAddress:** -
(No network access involved)

- **IpPort:** -
(No remote connection used)

- **WorkstationName:** -
(Local system activity)

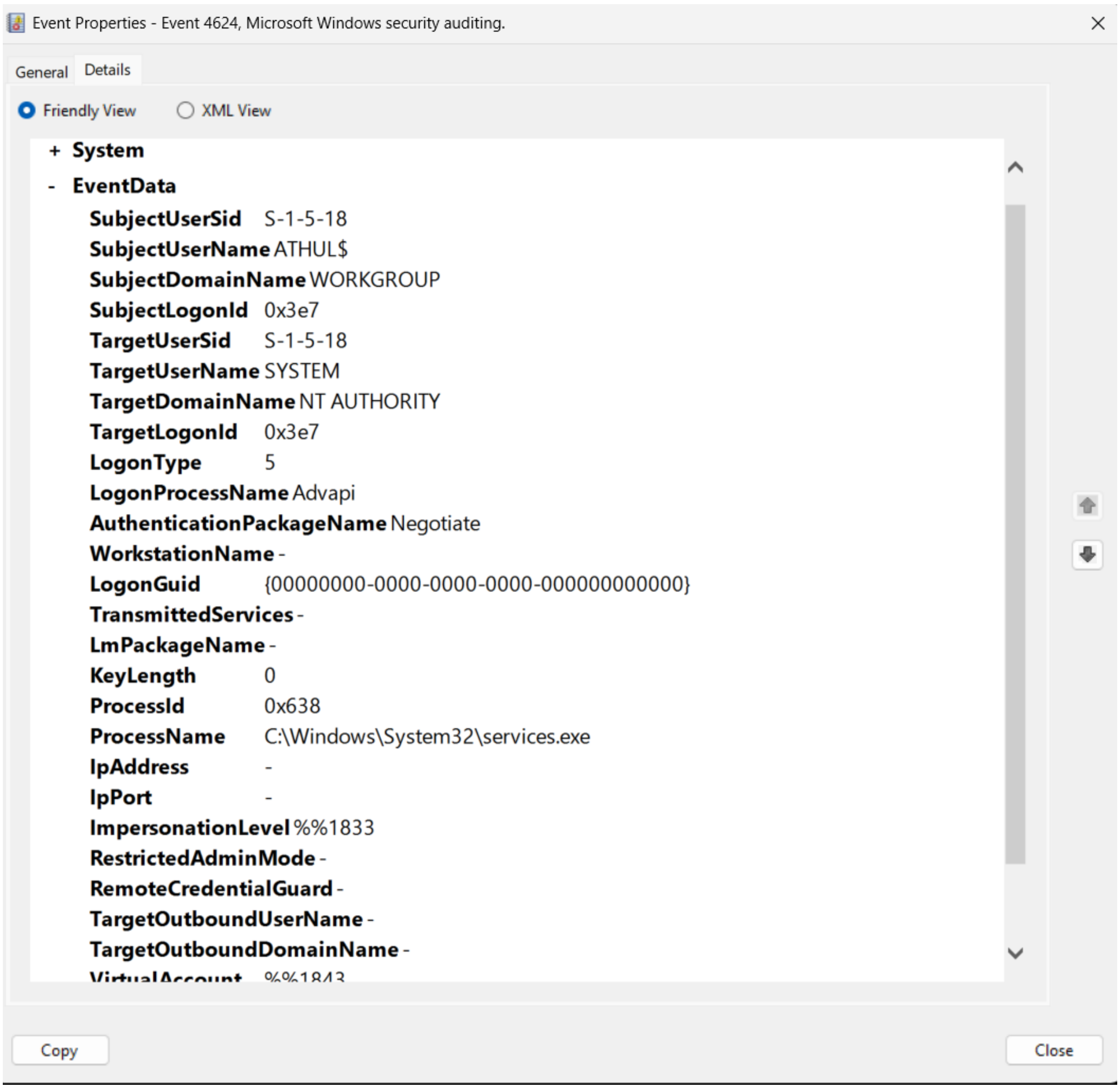
5.6 Privilege Information

- **ElevatedToken:** Yes
(Process ran with elevated privileges – expected for SYSTEM services)

- **VirtualAccount:** No
(Service did not use a virtual account)

- **RestrictedAdminMode:** -
(Not applicable)

- **RemoteCredentialGuard:** -
(Not applicable)


Event Properties - Event 4624, Microsoft Windows security auditing.
General
Details
● Friendly View
○ XML View
Copy
Close

```
+ System
- EventData
    SubjectUserSid    S-1-5-18
    SubjectUserName ATHUL$
    SubjectDomainName WORKGROUP
    SubjectLogonId    0x3e7
    TargetUserSid     S-1-5-18
    TargetUserName SYSTEM
    TargetDomainName NT AUTHORITY
    TargetLogonId     0x3e7
    LogonType         5
    LogonProcessName Advapi
    AuthenticationPackageName Negotiate
    WorkstationName -
    LogonGuid         {00000000-0000-0000-0000-000000000000}
    TransmittedServices -
    LmPackageName -
    KeyLength         0
    ProcessId         0x638
    ProcessName       C:\Windows\System32\services.exe
    IpAddress         -
    IpPort            -
    ImpersonationLevel %%1833
    RestrictedAdminMode -
    RemoteCredentialGuard -
    TargetOutboundUserName -
    TargetOutboundDomainName -
    VirtualAccount    %%1843
```

6. Event Interpretation

- The event represents a normal service logon performed by the operating system.
- The SYSTEM account authenticated locally to start a Windows service.
- No user interaction or remote access was involved.
- The process responsible (services.exe) is a trusted Windows component.
- This logon was initiated automatically by Windows service management.

7. Security Assessment

- The event is non-suspicious.

Reasons:

o Service logon (Logon Type 5)

o Legitimate SYSTEM account
o Initiated by trusted process (services.exe)
o No IP address or remote access
o No failed authentication attempts related to this event

---

8. Importance of This Analysis

• Understanding normal authentication events helps distinguish between legitimate system activity and malicious behavior.
• Service logons are often abused by attackers for persistence; therefore, recognizing legitimate service activity is critical.
• This analysis establishes a baseline for future detection and incident response tasks.
• Event ID 4624 is essential for tracking successful authentication events in Windows systems.

---

9. Outcome of Part A

- Successfully collected host and network logs.
- Gained understanding of Windows authentication events.
- Learned how to interpret detailed event fields.
- Established normal system behavior for future comparison

Additional Windows Security Log Analysis

Event ID 5058 – (Key File Operation)

---

9. Windows Security Event Analysis (Event ID 5058)

9.1 Event Overview

• Event ID: 5058 (Key File Operation)
(Indicates that a cryptographic key file was accessed by the system or an application)

• Event Type: Audit Success
(The cryptographic operation was completed successfully)

• Event Category: Other System Events
(Related to system-level cryptographic and security services)

• Log Name: Security
• Event Source: Microsoft Windows Security Auditing
• Date & Time: 27-01-2026 19:40:29
• Computer Name: ATHUL

9.2 Detailed Event Fields Analysis

- SubjectUserSid: Not displayed (User context shown)

- SubjectUserName: athul
(User account under which the cryptographic operation was performed)

- SubjectDomainName: ATHUL
(Local user account domain)

- LogonId: 0x681BFBE
(Unique identifier for the user logon session used to correlate related events)

9.3 Process Information

- ProcessId: 25708
(Unique identifier of the process that accessed the cryptographic key)

- ProcessCreationTime: 2026-01-21T04:01:53.963592300Z
(Time when the process responsible for the operation was created)

9.4 Cryptographic Parameters

- ProviderName: Microsoft Software Key Storage Provider
(Trusted Windows component responsible for managing cryptographic keys)

- AlgorithmName: UNKNOWN
(The specific cryptographic algorithm is not displayed for this operation)

- KeyName: 8cecc4f9-6862-4233-962e-c6c338e2c656
(Unique identifier assigned to the cryptographic key)

- KeyType: User key
(The key belongs to and is associated with the logged-in user account)

9.5 Key File Operation Information

- FilePath:
C:\Users\athul\AppData\Roaming\Microsoft\Crypto\Keys\675d48e919b96ab7d694d2e9e31b6b2a_7ea5ef41-13a5-4ab3-877e-c08612a01e9f
(Standard Windows location for storing user cryptographic private keys)

- Operation: Read persisted key from file
(The system accessed and loaded an existing stored cryptographic key)

- ReturnCode: 0x0
(The operation was successful with no errors)

10. Event Interpretation

- This event indicates that Windows or an application accessed a stored cryptographic key.
- The key was read from secure storage for use in encryption, authentication, or certificate-based operations.
- This activity is commonly triggered by secure applications, Windows authentication, or background security services.
- No modification or deletion of the key occurred.

---

11. Security Assessment

- The event is non-suspicious and represents normal system behavior.

Reasons:
o Operation performed by a legitimate user account (athul)
o Accessed a standard Windows cryptographic key storage directory
o Operation type was read-only (no key modification)
o Successful return code (0x0)
o Operation performed by a trusted Microsoft cryptographic provider

---

12. Importance of This Analysis

- Helps monitor access to sensitive cryptographic keys.
- Useful for detecting abnormal or unauthorized access to encryption material.
- Establishes a baseline for normal cryptographic behavior for the user account.
- Important in forensic and incident response investigations involving certificates, VPNs, and secure authentication.

Linux Authentication Log Analysis

- Linux authentication and privilege-related logs were accessed using the journalctl utility, as Kali Linux uses systemd-based logging instead of traditional log files such as /var/log/auth.log.
- Sudo-related logs were filtered to observe authentication and privilege escalation activities

---

Linux Commands Used (One-Line Explanation)

- **sudo** – Used to execute commands with administrative (root) privileges required to access system logs.
- **journalctl** – Used to view system and authentication logs stored by the systemd journal in Kali Linux.
- **sudo journalctl** – Used to access system logs that are restricted to root-level users.
- **sudo journalctl _COMM=sudo** – Used to filter and display only sudo-related authentication and privilege escalation logs.
- **sudo journalctl _COMM=sudo -n 10** – Used to display the most recent sudo log entries in a concise and readable format.

Analyzed Log Entry

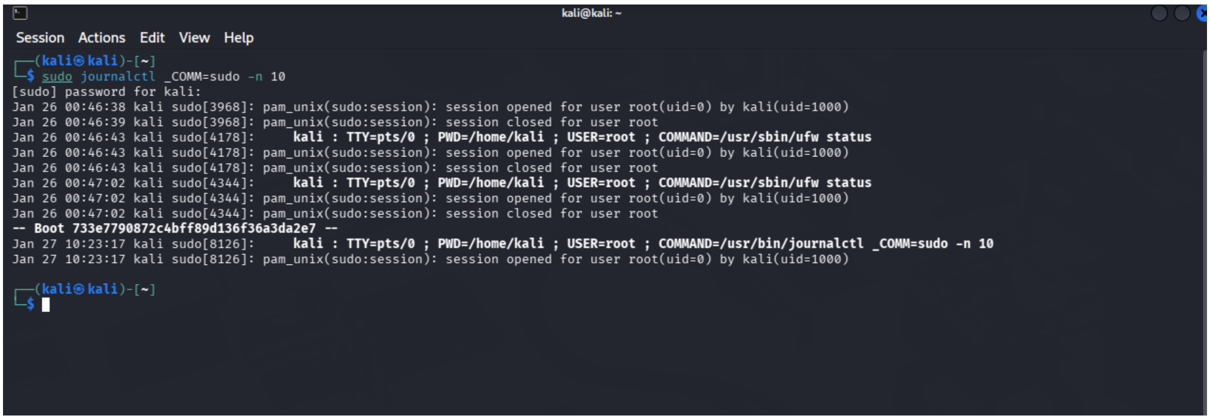
```
Jan 26 00:46:43 kali sudo[4178]:
kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/sbin/ufw status
```

Interpretation

• The log indicates that the user **kali** successfully executed a command with elevated privileges using **sudo**.
• The command was executed from a local terminal session (**TTY=pts/0**) and escalated to the **root** user.
• The user checked the status of the **UFW firewall**, which is a standard administrative task.

Security Significance

• This entry confirms legitimate administrative access to firewall settings.
• Monitoring firewall-related sudo commands is important to detect unauthorized changes to security controls.
• This activity appears to be **normal system administration** and does not indicate malicious behavior.



```
┌──(kali㉿kali)-[~]
└─$ sudo journalctl _COMM=sudo -n 10
[sudo] password for kali:
Jan 26 00:46:38 kali sudo[3968]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
Jan 26 00:46:39 kali sudo[3968]: pam_unix(sudo:session): session closed for user root
Jan 26 00:46:43 kali sudo[4178]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/sbin/ufw status
Jan 26 00:46:43 kali sudo[4178]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
Jan 26 00:46:43 kali sudo[4178]: pam_unix(sudo:session): session closed for user root
Jan 26 00:47:02 kali sudo[4344]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/sbin/ufw status
Jan 26 00:47:02 kali sudo[4344]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)
Jan 26 00:47:02 kali sudo[4344]: pam_unix(sudo:session): session closed for user root
-- Boot 733e7790872c4bff89d136f36a3da2e7 --
Jan 27 10:23:17 kali sudo[8126]:     kali : TTY=pts/0 ; PWD=/home/kali ; USER=root ; COMMAND=/usr/bin/journalctl _COMM=sudo -n 10
Jan 27 10:23:17 kali sudo[8126]: pam_unix(sudo:session): session opened for user root(uid=0) by kali(uid=1000)

┌──(kali㉿kali)-[~]
└─$ 
```

PART B: Detecting Suspicious Activity or Potential Intrusions

---

1. Objective

- To identify and analyze **failed authentication attempts** in Windows.
- To understand how Windows logs record login failures.
- To evaluate whether a failed logon event is normal or suspicious.
- To introduce the concept of **pattern-based detection**.

---

2. Tool Used

- **Windows Event Viewer**
  - Used to access and filter Windows Security logs.
  - Focused on authentication failure events.

---

3. Log Source

- **Windows Security Event Logs**
  - Location: Event Viewer → Windows Logs → Security
  - Contains authentication success and failure events.

---

4. Event Filtering Method

- The Security log contained a large number of events.
- To isolate relevant events, the **Filter Current Log** option was used.
- Event ID **4625** was applied as a filter to display only failed logon events.

---

5. Windows Failed Logon Event Analysis (Event ID 4625)

5.1 Event Details Observed

• **Event ID:** 4625
(Failed logon attempt (multiple times))

• **Logon Type:** 2
(Interactive local logon attempt using keyboard or login screen)

• **Account Name:** ATHUL$
(Machine account, not a human user account)

• **Account Domain:** WORKGROUP

• **Failure Reason:** An Error occurred during Logon
(Authentication failed during the logon process)

• **Status Code:** 0xC000006D
(Generic logon failure – bad username or password)

• **Sub Status Code:** 0xC0000380
(Account or logon process-related failure)

• **Source Network Address:** 127.0.0.1
(Login attempt originated from the local system itself)

• **Caller Process Name:** C:\Windows\System32\svchost.exe
(System service initiated the logon request)

• **Authentication Package:** Negotiate

---

6. Interpretation of the Event

• The event indicates a **local interactive login failure** on the system.
• The logon attempt was initiated by a **local system process (svchost.exe)**.
• The failure was related to **invalid credentials or a system/service-related authentication issue**.
• The attempt originated from **localhost (127.0.0.1)**, confirming it was not a remote attack.
• The account involved (**ATHUL$**) is a **machine account**, not a normal user account.

---

7. Security Assessment

• This failed logon event is considered **low risk and non-suspicious**.

Reasons:
o Local interactive logon attempt
o Originated from the same system (localhost)
o Machine account involved, not a human user
o No external IP address
o No privileged user account targeted

---

8. Detection Insight Gained

- Event ID 4625 is a key indicator for:
  - Failed authentication attempts
  - Brute-force attack detection (when repeated)
  - Misconfigured services or system processes

- A **single occurrence** is normal and often caused by:
  - Background services
  - Cached credentials
  - System startup processes
  - Temporary authentication issues

- Multiple repeated 4625 events within a short time window may indicate **brute-force or credential-stuffing attacks**.

---

9. Current Status of Part B

- Identified failed logon events in Windows Event Viewer
- Applied filtering to locate Event ID 4625
- Analyzed a failed authentication attempt
- Determined the logon source and process
- Distinguished between normal system behavior and potential threat indicators

---

Detection of suspicious activity depends on identifying abnormal patterns rather than isolated events.

False Positive Detection Analysis (Windows Authentication Events)

---

1. Incident Summary

During the analysis of Windows Security logs, a sequence of multiple failed logon events followed by successful logon events was identified. The observed pattern initially resembled a brute-force authentication attack. However, further contextual analysis confirmed that the activity was a **false positive**, originating from the local system rather than an external attacker.

---

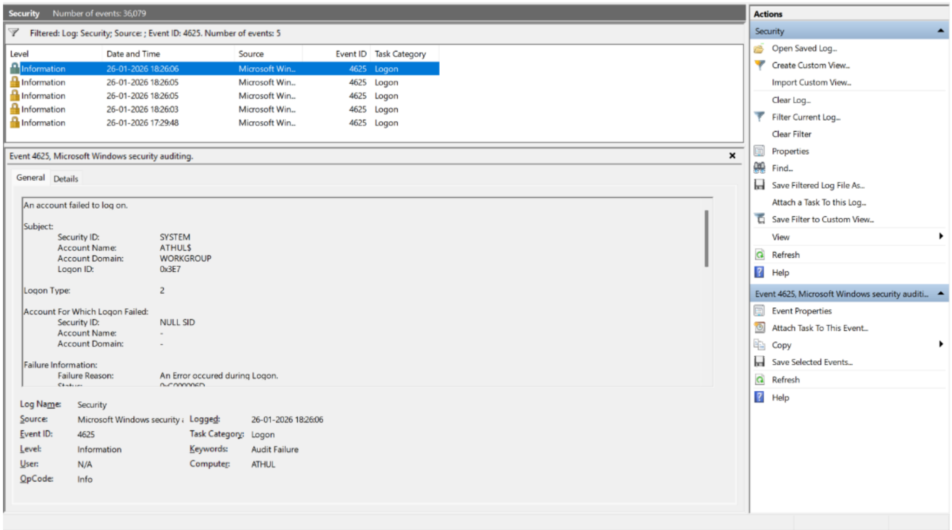
2. Events Observed

2.1 Failed Logon Events

- **Event ID:** 4625 (Audit Failure – Failed Logon)

- **Timestamps:**
  - 26-01-2026 18:26:03
  - 26-01-2026 18:26:05

o 26-01-2026 18:26:05
o 26-01-2026 18:26:06
o 26-01-2026 17:29:48



```
Security    Number of events: 36,079

Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 5

Level         Date and Time          Source            Event ID  Task Category
Information   26-01-2026 18:26:06    Microsoft Win...      4625  Logon
Information   26-01-2026 18:26:05    Microsoft Win...      4625  Logon
Information   26-01-2026 18:26:05    Microsoft Win...      4625  Logon
Information   26-01-2026 18:26:03    Microsoft Win...      4625  Logon
Information   26-01-2026 17:29:48    Microsoft Win...      4625  Logon

Event 4625, Microsoft Windows security auditing.

General  Details

An account failed to log on.

Subject:
        Security ID:            SYSTEM
        Account Name:           ATHUL$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Type:                     2

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -

Failure Information:
        Failure Reason:         An Error occured during Logon.
        Status:                 0xC000006D

Log Name:   Security
Source:     Microsoft Windows security a   Logged:         26-01-2026 18:26:06
Event ID:   4625                           Task Category:  Logon
Level:      Information                    Keywords:       Audit Failure
User:       N/A                            Computer:       ATHUL
OpCode:     Info
```

- **Characteristics:**

o Multiple failed logon attempts within a short time window
o Consistent logon category (Logon)
o Failure reason related to authentication error
o Status code indicates credential or logon process failure

2.2 Successful Logon Events

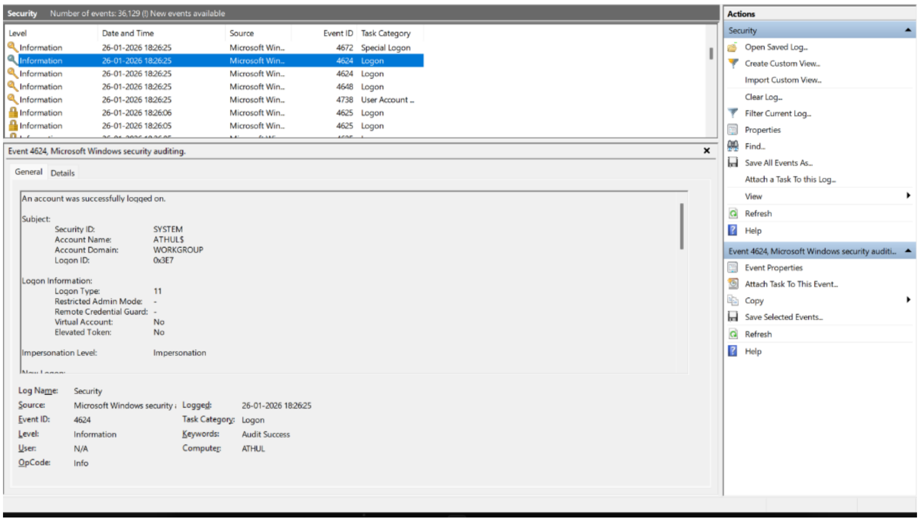
- **Event ID:** 4624 (Audit Success – Successful Logon)

- **Timestamp:**

o 26-01-2026 18:26:25 (multiple related logon events)

- **Observation:**

o Successful authentication occurred shortly after failed attempts
o Multiple 4624-related events observed at the same timestamp
o Behavior consistent with Windows session initialization and logon sequence



Security Number of events: 36,129 (!) New events available

Level	Date and Time	Source	Event ID	Task Category
Information	26-01-2026 18:26:25	Microsoft Win...	4672	Special Logon
Information	26-01-2026 18:26:25	Microsoft Win...	4624	Logon
Information	26-01-2026 18:26:25	Microsoft Win...	4624	Logon
Information	26-01-2026 18:26:25	Microsoft Win...	4648	Logon
Information	26-01-2026 18:26:25	Microsoft Win...	4738	User Account ...
Information	26-01-2026 18:26:06	Microsoft Win...	4625	Logon
Information	26-01-2026 18:26:05	Microsoft Win...	4625	Logon

Event 4624, Microsoft Windows security auditing.

```
An account was successfully logged on.

Subject:
        Security ID:                SYSTEM
        Account Name:               ATHUL$
        Account Domain:             WORKGROUP
        Logon ID:                   0x3E7

Logon Information:
        Logon Type:                 11
        Restricted Admin Mode:      -
        Remote Credential Guard:    -
        Virtual Account:            No
        Elevated Token:             No

Impersonation Level:                Impersonation
```

```
Log Name:   Security
Source:     Microsoft Windows security    Logged:         26-01-2026 18:26:25
Event ID:   4624                          Task Category:  Logon
Level:      Information                   Keywords:       Audit Success
User:       N/A                           Computer:       ATHUL
OpCode:     Info
```

3. Initial Detection Assessment

Based on event sequence alone, the following pattern was identified:

4625 → 4625 → 4625 → 4625 → 4624

This sequence typically indicates:
- Repeated authentication attempts
- Followed by a successful login
- Commonly associated with brute-force credential attack patterns

At this stage, the activity was flagged as **potentially suspicious** based on pattern recognition.

4. Contextual Analysis (Critical Step)

Further analysis of event details provided essential context that ruled out a real intrusion.

4.1 Source Network Address

- **Source IP:** 127.0.0.1

- **Interpretation:**

o Indicates localhost
o Authentication attempts originated from the same system
o No external or remote source involved

See screenshot showing Source Network Address = 127.0.0.1

4.2 Logon Type

- **Logon Type:** 2

- **Interpretation:**

o Interactive local logon (keyboard / console)

o Not a network-based or remote login
o Excludes RDP or external brute-force scenarios

4.3 Account Involved

- **Account Name:** ATHUL$

- **Interpretation:**
o Machine account (identified by $ suffix)
o Used internally by Windows for system operations
o Not a typical target for manual attacker login attempts

4.4 System Context

- The activity occurred on a personal/local system
- No evidence of:
o External IP addresses
o Privileged user targeting
o New user account creation
o Malware or security software alerts
o Lateral movement indicators

---

5. Final Determination

After correlating all indicators, the activity was determined to be a **false positive**.

Reasoning:
- All authentication attempts originated locally
- Logon type confirmed interactive local access
- Machine account involvement suggests internal system behavior
- No persistence or attacker-controlled access observed
- Behavior consistent with:
o Credential provider retries
o Cached credential mismatch
o Lock-screen or system service authentication behavior

---

6. Security Verdict

- **Threat Level:** None
- **Incident Type:** False Positive Authentication Detection
- **System Status:** Not Compromised
- **Action Required:** No remediation required

---

7. Cybersecurity Insight Gained

This analysis highlights an important cybersecurity principle:

Detection patterns must always be validated with contextual information before declaring an incident.

Key lessons:
- Not all brute-force-like patterns indicate real attacks
- Source IP, logon type, and account context are critical
- False positives are common in real SOC environments
- Proper analysis prevents unnecessary incident escalation

8. Relevance to Part B (Detection Phase)

This case demonstrates:
- Pattern-based detection using authentication logs
- Correlation of failed and successful logon events
- Importance of distinguishing real threats from false positives
- Practical SOC-level analytical decision-making

9. Conclusion

Although the observed authentication pattern matched known brute-force indicators, detailed contextual analysis confirmed that the activity was benign and system-generated. This case represents a clear example of a **false positive detection**, reinforcing the importance of correlating multiple log attributes in cybersecurity operations.