Windows Brute-Force Detection using Splunk

Subject: **Windows Brute-Force Detection using Splunk**

Incident ID: IR-2025-1220-006

PREPARED BY:

Vignesh K.

SOC Analyst / Security Researcher

CERTIFICATIONS: Google Cybersecurity Professional

REPORT DATE: December 20, 2025

1. Project Overview and Goal

- **Overview:**This project demonstrates detection of brute-force authentication attempts against a Windows 11 system using Splunk SIEM.

2. Technical Environment and Tools

The technical components and tools used for this assessment are detailed below.

Component	Description	Detail
Target System	The victim server.	Windows 11
Attacker System	The attacker machine.	Kali Linux.
Primary Tools	SIEM	Splunk Enterprise

3. Attack Simulation

- SMB authentication attempts from Kali
- Multiple failed login attempts generated
- Windows logged Event ID 4625

4. Detection

- Splunk was used to detect brute-force behavior by correlating multiple failed login events.- **Splunk Query Logic:** The provided Splunk Search Processing Language (SPL) query (`index=* EventCode=4625 | stats count by Account`) aggregates all failed logon events (Event ID 4625) across all indexes. The `stats count by Account` command then groups these events by the target `Account` name and counts the total number of failed attempts for each unique account within the search timeframe.
-

- - **Threshold Setting:** A security analyst would then review the counts. A high count (e.g., > 10 failed attempts within a short window like 5 minutes) for a single account is a strong indicator of a brute-force attack.
-
- - **Visualisation:** This data can be visualized in a Splunk dashboard (e.g., a bar chart or a single value panel) to provide real-time monitoring of failed login trends and quickly identify accounts under attack.
-
- - **Refinement for Alerting:** For operational security, this base query is typically refined to include time windows and a specific threshold to trigger an automated alert (as noted in the security recommendations). For example, `... | where count > 5` and scheduled to run every 5 minutes.
-

5. SPL Query

```
index=* EventCode=4625 | stats count by Account_
```

The core Search Processing Language (SPL) query used for detection is:

`index=* EventCode=4625 | stats count by Account`This query is a foundational step in identifying brute-force activity.

Detailed Explanation of SPL Components

`index=* EventCode=4625`

This is the initial filtering stage.

- **`index=*`**: Instructs Splunk to search across *all* configured indexes. In a production environment, this should be narrowed down (e.g., `index=windows_security`) for performance.
- **`EventCode=4625`**: This is the critical filter. Windows Security Event ID 4625 specifically corresponds to a **"An account failed to log on"** event. Filtering by this ID ensures that only failed authentication attempts are analyzed, which is the signature of a brute-force attack.

```
| stats count by Account
```

This is the command that performs the aggregation and statistical analysis.

- `|` **(Pipe)**: Used to pipe the results of the previous command (the filtered failed logon events) into the next command.
- **`stats`**: A reporting command used to calculate statistics on the search results.
- **`count`**: The specific statistical function used, which calculates the total number of events.
- **`by Account`**: Specifies that the `count` should be grouped by the unique value in the `Account` field. The `Account` field typically holds the name of the user account that the attacker was trying to log into.

Result Interpretation

The output of this query is a simple table showing every unique account that experienced a failed login attempt during the search time frame, along with the total number of attempts (`count`) associated with that account. A security analyst immediately looks for an unusually high `count` value associated with any single `Account`, as this strongly suggests a programmatic, rapid-fire brute-force attempt rather than typical user error. The time range of the search is implicitly critical to this interpretation.

6. **Security Recommendations (Next Steps)**

Based on the detection results, the following remediation measures and security enhancements are recommended:

- **HIGH: Enforce Account Lockout Policy:** Implement a strict Group Policy Object (GPO) to lock out user accounts after a small number of consecutive failed login attempts (e.g., 3-5).
- **HIGH: Monitor and Alert:** Refine the existing Splunk query into a scheduled alert that triggers a high-priority incident when the threshold of failed logins is met. This alert should notify the SOC team immediately.
- **MEDIUM: Implement Multi-Factor Authentication (MFA):** Where possible, deploy MFA for all critical accounts and services to mitigate the risk of password-based attacks.
- **MEDIUM: Network Segmentation:** Isolate critical servers using network segmentation to limit the attack surface and prevent attacker lateral movement.

7. Conclusion

This project successfully validated the capability of using Splunk to detect common Windows security threats such as SMB-based brute-force attacks. The correlation of Event ID 4625 is a foundational detection control. Immediate action on the security recommendations, particularly the automated alerting and account lockout policies, is essential to harden the system against this threat.

8. Evidence

8.1 Eventviewer_4625

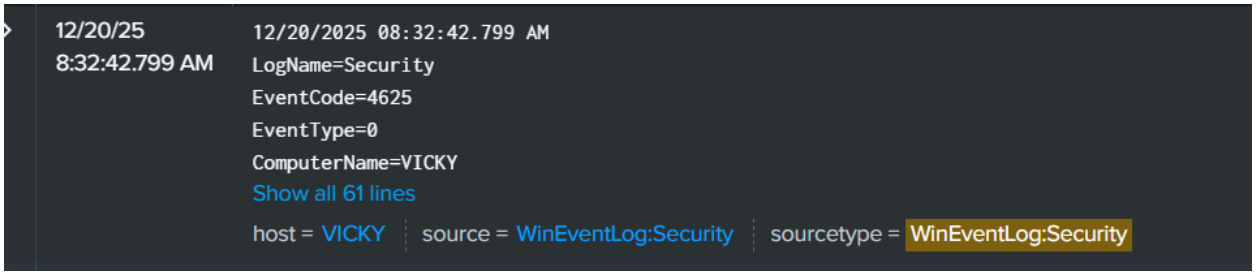
```
Account For Which Logon Failed:
        Security ID:            S-1-0-0
        Account Name:           fakeuser
        Account Domain:         WORKGROUP

Failure Information:
        Failure Reason:         Unknown user name or bad password.
        Status:                 0xC000006D
        Sub Status:             0xC0000064

Process Information:
        Caller Process ID:      0x0
        Caller Process Name:    -

Network Information:
        Workstation Name:       KALI
        Source Network Address: 192.168.31.110
        Source Port:            33932
```

8.2 Splunk_detection



8.3 Splunk_raw_logs