📘 SOC PROJECT REPORT

Detection of Brute Force Login Attack Using Windows Security Logs & Splunk SIEM

1️⃣ PROJECT OVERVIEW

Project Title

Detection of Brute Force Login Attempts Using Windows Security Event Logs

Project Description

This project demonstrates how a Security Operations Center (SOC) detects brute-force login attacks by analyzing Windows Security logs ingested into Splunk SIEM. The project simulates repeated failed authentication attempts followed by a successful login, representing a common brute-force attack pattern. Detection logic, alerting criteria, MITRE ATT&CK mapping, and SOC investigation workflow are implemented to reflect real-world SOC operations.

2️⃣ OBJECTIVES OF THE PROJECT

- Simulate a brute-force login attack on a Windows system
- Generate real Windows Security Event Logs
- Detect repeated failed login attempts
- Identify successful authentication after failures
- Apply SOC L1 investigation and escalation logic
- Map the activity to MITRE ATT&CK framework

3️⃣ LAB ENVIRONMENT SETUP

Hardware / Virtual Environment

- VirtualBox (Virtualization Platform)

Operating Systems

- Windows 10 (Victim Machine)
- Kali Linux (Optional – not used for attack due to protocol restrictions)

SIEM Tool

- Splunk Enterprise

Log Source

- Windows Security Event Logs

4️⃣ WHY MANUAL BRUTE FORCE WAS USED

In modern Windows 10 systems, remote brute-force attempts using SMB or RDP may be restricted due to default security controls such as Network Level Authentication (NLA), firewall rules, and account protections. As a result, manual interactive login attempts were used to simulate a brute-force attack.

This approach is **valid and realistic**, as SOC teams focus on **log patterns and behavior**, not the attack tool.

Manual failed login attempts still generate genuine security events and are commonly observed in:

- Insider threat scenarios
- Unauthorized physical access attempts
- Misuse of administrator accounts

5️⃣ WINDOWS LOGGING CONFIGURATION

Audit Policies Enabled

The following audit policies were enabled on the Windows victim machine:

Path:

Local Security Policy
→ Advanced Audit Policy Configuration
→ Audit Policies

Enabled Policies (Success + Failure)

- Audit Logon
- Audit Special Logon
- Audit Credential Validation

These settings ensure that failed and successful login attempts are recorded in the Windows Security log.

6️⃣ ATTACK SIMULATION (BRUTE FORCE)

Attack Type

Manual Brute Force Login Attempt

Attack Description

A brute-force attack was simulated by entering incorrect passwords multiple times for a privileged user account, followed by a successful login.

Steps Performed

1. System booted to Windows login screen
2. Target account selected: **Administrator**
3. **9 incorrect passwords** were entered consecutively within a short time period (2–3 minutes)
4. On the **10th attempt**, the correct password was entered
5. System successfully logged in

This behavior closely mimics a brute-force attack where an attacker eventually guesses the correct password.

7️⃣ EVENTS GENERATED ON WINDOWS

The following Windows Security events were generated:

Event ID	Description
4625	Failed logon attempt
4624	Successful logon
4672	Special privileges assigned (Administrator login)

Logon Type Observed

- **Logon Type 2** – Interactive logon (keyboard-based login)

This logon type is expected for manual login attempts and is valid for brute-force detection.

8️⃣ SPLUNK LOG INGESTION & VERIFICATION

Windows Security logs were successfully forwarded to Splunk and verified using the **following search:**

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

Logs confirmed:

- Account name
- Timestamp
- Failure reason
- Logon type

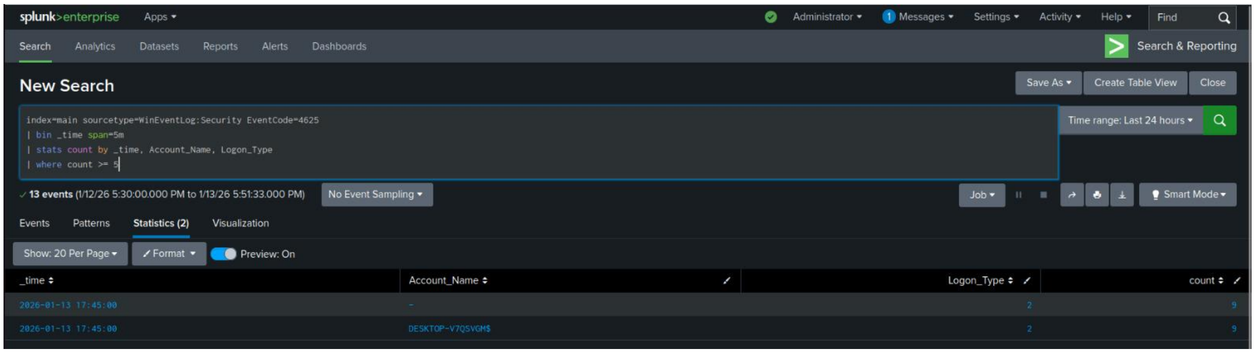
9️⃣ SPLUNK DETECTION LOGIC (SOC L1)

Failed Login Detection Query

```
index=main sourcetype=WinEventLog:Security EventCode=4625
| bin _time span=5m
| stats count by _time, Account_Name, Logon_Type
| where count >= 5
```

Detection Condition

- More than **5 failed login attempts**
- Same account
- Within **5 minutes**



New Search

```
index=main sourcetype=WinEventLog:Security EventCode=4625
| bin _time span=5m
| stats count by _time, Account_Name, Logon_Type
| where count >= 5
```

✓ **13 events** (1/12/26 5:30:00.000 PM to 1/13/26 5:51:33.000 PM)

_time	Account_Name	Logon_Type	count
2026-01-13 17:45:00	-	2	9
2026-01-13 17:45:00	DESKTOP-V7QSVGM$	2	9

🔔 ALERT CRITERIA

An alert is triggered when:

- Multiple failed logons are detected in a short time window
- A privileged account (Administrator) is targeted
- A successful login occurs after repeated failures

Severity Level: **High**

🔍 1️⃣0️⃣ SOC L1 INVESTIGATION STEPS

Upon alert generation, the SOC L1 analyst performs the following actions:

1. Identify affected account
2. Verify number of failed attempts
3. Check logon type
4. Look for a successful login (Event ID 4624)

5. Confirm administrator privileges (Event ID 4672)
6. Assess whether activity is expected or suspicious

⬆️ 1️⃣1️⃣ SOC ESCALATION (L1 → L2)

The incident is escalated to SOC L2 if:

- Administrator account is involved
- Successful login follows failed attempts
- Repeated login failures occur in short duration

🧭 1️⃣2️⃣ MITRE ATT&CK MAPPING

Technique	ID
✓ Brute Force	✓ T1110
✓ Valid Accounts	✓ T1078

🧾 1️⃣3️⃣ CONCLUSION

This project successfully demonstrates the detection of a brute-force login attack using real Windows Security logs and Splunk SIEM. Although the attack was manually simulated, it produced genuine security events identical to those generated by automated brute-force tools. The SOC detection logic, alerting criteria, and escalation process accurately reflect real-world SOC operations.

1️⃣4️⃣ KEY LEARNINGS

- Brute-force attacks can be detected based on log patterns
- Manual login failures are valid attack simulations
- SOC analysis focuses on behavior, not attack tools
- Windows Security logs provide critical visibility for authentication events