SOC Incident Investigation: Brute Force Attack Analysis Using SIEM

Hands-on SOC investigation using realistic log data
in a simulated bootcamp SOC lab environment

Tri Hamdani HN. Husuna
SOC Analyst Junior

Incident Type : Brute Force Attack
Tools : Splunk, Windows Event Log, Sysmon
Environment : Bootcamp Lab

1. Background & Objective

Background

This report documents a security incident identified during routine security monitoring activities using a SIEM platform. During monitoring, multiple failed authentication attempts were observed, followed by a successful login from the same source. This pattern raised suspicion of a potential brute force attack.

Objective

- Analyze failed and successful authentication events
- Identify indicators of brute force attack
- Assess potential security impact
- Provide security recommendations

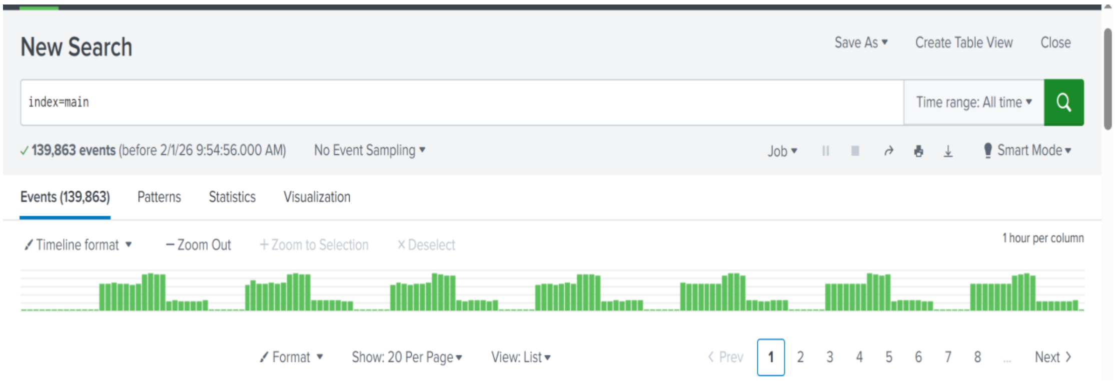
2. Lab Environment

Environment Setup

- **Operating System:** Windows
- **Log Sources:** Windows Security Log, Sysmon
- **SIEM Platform:** Splunk
- **Environment Type:** Bootcamp SOC Lab

Architecture / Flow

Logs generated from the Windows system were collected and analyzed using the Splunk SIEM platform to support security monitoring and incident investigation.



New Search

```
index=main
```

Time range: All time ▾

✓ 139,863 events (before 2/1/26 9:54:56.000 AM)   No Event Sampling ▾

Events (139,863)

1 hour per column

Show: 20 Per Page ▾   View: List ▾

Figure 1. Splunk SIEM environment used for log collection and analysis.

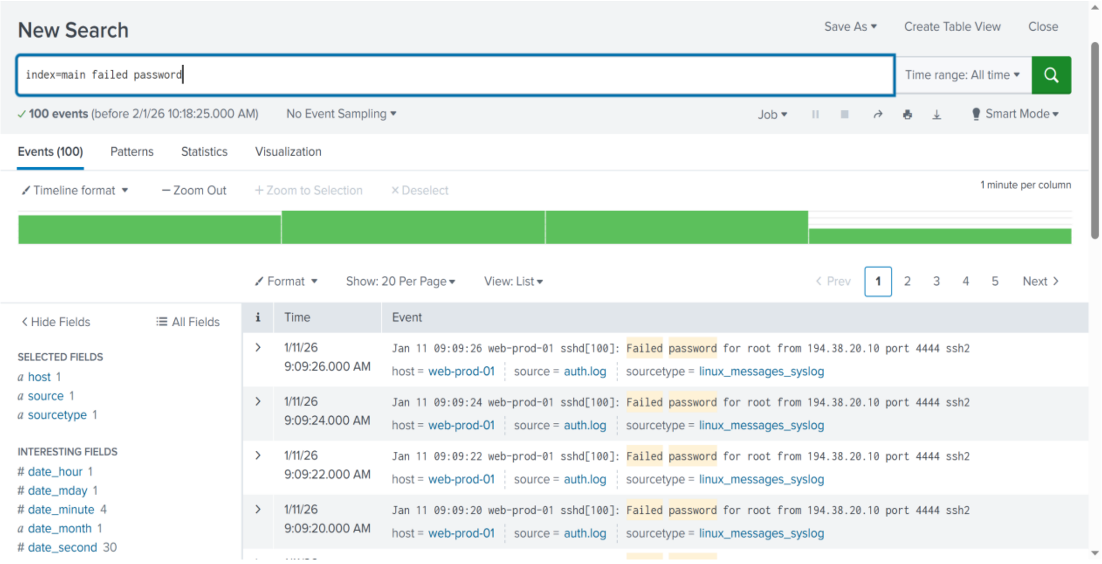
3. incident identification

Initial Detection

During routine monitoring activities in the SIEM platform, an unusual number of failed authentication events were detected within a short time period. The repeated failures originating from the same source raised an alert for further investigation.

Indicators Observed

- High volume of failed login attempts
- Repeated attempts within a short time window
- Same source involved in multiple authentication failures



```
index=main failed password
```

✓ 100 events (before 2/1/26 10:18:25.000 AM)   No Event Sampling

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 1
# date_mday 1
# date_minute 4
a date_month 1
# date_second 30

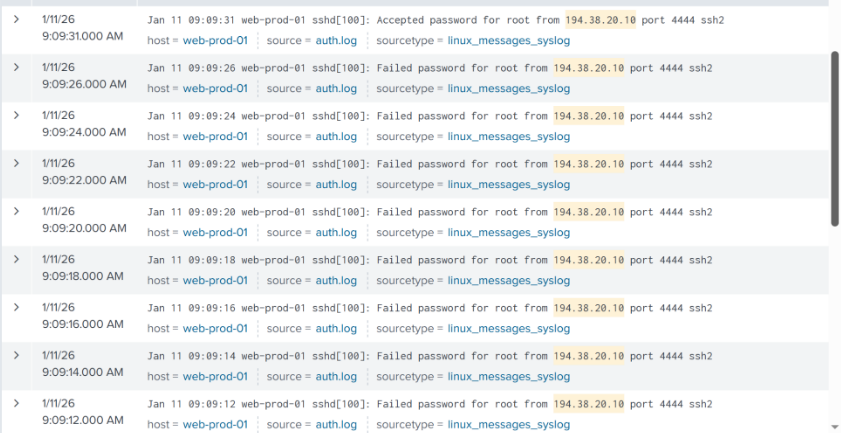
Time	Event
1/11/26 9:09:26.000 AM	Jan 11 09:09:26 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2 host = web-prod-01 source = auth.log sourcetype = linux_messages_syslog
1/11/26 9:09:24.000 AM	Jan 11 09:09:24 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2 host = web-prod-01 source = auth.log sourcetype = linux_messages_syslog
1/11/26 9:09:22.000 AM	Jan 11 09:09:22 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2 host = web-prod-01 source = auth.log sourcetype = linux_messages_syslog
1/11/26 9:09:20.000 AM	Jan 11 09:09:20 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2 host = web-prod-01 source = auth.log sourcetype = linux_messages_syslog

Figure 2. Detection of multiple failed authentication events during SIEM monitoring.

4. Log Analysis

Analysis Summary

- Total failed authentication events: ~100
- Successful authentication events: 1
- Failed attempts occurred before the successful login
- Pattern indicates systematic credential guessing

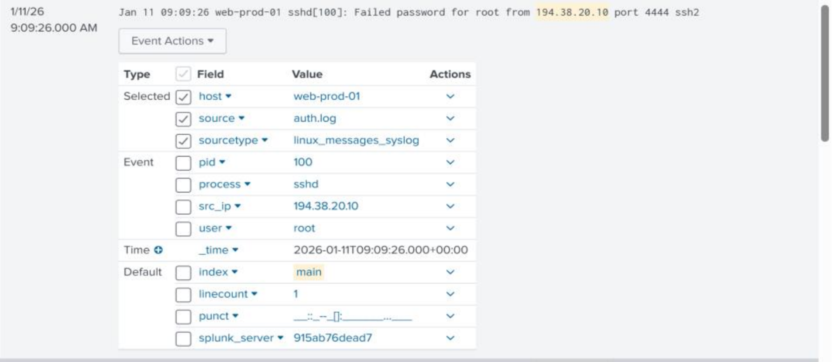


```
1/11/26            Jan 11 09:09:31 web-prod-01 sshd[100]: Accepted password for root from 194.38.20.10 port 4444 ssh2
9:09:31.000 AM     host = web-prod-01 | source = auth.log | sourcetype = linux_messages_syslog
1/11/26            Jan 11 09:09:26 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2
9:09:26.000 AM     host = web-prod-01 | source = auth.log | sourcetype = linux_messages_syslog
1/11/26            Jan 11 09:09:24 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2
9:09:24.000 AM     host = web-prod-01 | source = auth.log | sourcetype = linux_messages_syslog
1/11/26            Jan 11 09:09:22 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2
9:09:22.000 AM     host = web-prod-01 | source = auth.log | sourcetype = linux_messages_syslog
1/11/26            Jan 11 09:09:20 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2
9:09:20.000 AM     host = web-prod-01 | source = auth.log | sourcetype = linux_messages_syslog
1/11/26            Jan 11 09:09:18 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2
9:09:18.000 AM     host = web-prod-01 | source = auth.log | sourcetype = linux_messages_syslog
1/11/26            Jan 11 09:09:16 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2
9:09:16.000 AM     host = web-prod-01 | source = auth.log | sourcetype = linux_messages_syslog
1/11/26            Jan 11 09:09:14 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2
9:09:14.000 AM     host = web-prod-01 | source = auth.log | sourcetype = linux_messages_syslog
1/11/26            Jan 11 09:09:12 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2
9:09:12.000 AM     host = web-prod-01 | source = auth.log | sourcetype = linux_messages_syslog
```

Figure 3. *Overview of authentication events showing multiple failed login attempts followed by one successful login.*

Log Fields Analyzed

- EventCode
- Username
- Source IP
- Timestamp



```
1/11/26            Jan 11 09:09:26 web-prod-01 sshd[100]: Failed password for root from 194.38.20.10 port 4444 ssh2
9:09:26.000 AM
```

Type	☑ Field	Value	Actions
Selected	☑ host ▾	web-prod-01	⌄
	☑ source ▾	auth.log	⌄
	☑ sourcetype ▾	linux_messages_syslog	⌄
Event	□ pid ▾	100	⌄
	□ process ▾	sshd	⌄
	□ src_ip ▾	194.38.20.10	⌄
	□ user ▾	root	⌄
Time ⊕	_time ▾	2026-01-11T09:09:26.000+00:00	
Default	□ index ▾	main	⌄
	□ linecount ▾	1	⌄
	□ punct ▾	__::_--_[]:________...____	⌄
	□ splunk_server ▾	915ab76dead7	⌄

Figure 4. *Detailed analysis of a single authentication event, highlighting source host information and related log fields.*

5. Attack Confirmation & Risk Assessment

Attack Classification

- **Attack Type:** Brute Force Authentication Attack
- **Target:** User authentication mechanism
- **Status:** Successful (unauthorized access achieved)

Justification

- High number of failed authentication attempts observed
- Failed attempts occurred before a successful login
- Repeated attempts originated from the same source
- Pattern matches common brute force behavior

Potential Impact

- Unauthorized system access
- Credential compromise
- Lateral movement risk

Risk Level

Overall Risk: Medium–High

Risk level is classified as Medium–High due to successful authentication but limited evidence of post-exploitation activity.

6. Recommendations & Skills Demonstration

Security Recommendations

- Implement account lockout policy after multiple failed login attempts
- Enable multi-factor authentication (MFA) for critical accounts
- Monitor repeated authentication failures from the same source IP
- Block or rate-limit suspicious IP addresses at firewall level
- Improve alerting rules for authentication anomalies

Analyst Actions

- Collected authentication logs from Splunk
- Identified abnormal login behavior
- Correlated failed and successful login events
- Analyzed source host and attack pattern
- Determined attack classification and risk level
- Documented findings and recommendations

Tools & Technologies Used

- SIEM: Splunk
- Log Source: Windows Security Logs
- Analysis Method: Log correlation & pattern analysis
- Operating System: Windows
- Attack Type: Brute Force Authentication

Skills Demonstrated

- Log analysis & event correlation
- Brute force attack detection

- Windows authentication analysis
- SIEM querying (Splunk)
- Incident documentation
- Security mindset & risk assessment

Closing Statement

This portfolio demonstrates my ability to analyze security logs, identify suspicious activities, and perform initial incident analysis as a SOC Analyst Level 1.