📘 SOC INCIDENT REPORT

SOAR-Lite-Splunk-SSH-Bruteforce

1. Executive Summary (Management View)

During routine security monitoring, multiple failed SSH authentication attempts were detected on a Linux system. The activity originated from a single source IP and exceeded normal baseline behavior.
The event was identified using Splunk SIEM, enriched using threat intelligence (AbuseIPDB), and analyzed via a Python-based SOAR-Lite automation pipeline.

Based on enrichment results and contextual analysis, the activity was classified as **low-severity brute-force behavior in a controlled lab environment**, requiring no immediate containment. This incident demonstrates effective detection, validation, and analyst decision-making while avoiding unnecessary escalation.

2. Why This Alert Matters (Analyst Thinking)

SSH is a **high-value access vector** in Linux environments.
Repeated authentication failures can indicate:

- Credential stuffing
- Password brute-force attempts
- Unauthorized access attempts

However, **not every failed login is malicious**.
As a analyst i must determine **intent, risk, and impact** before escalation.

3. Detection Source & Data Collection

Log Source

- System: Ubuntu Linux
- Log file: /var/log/auth.log
- Service monitored: sshd

SIEM Tool

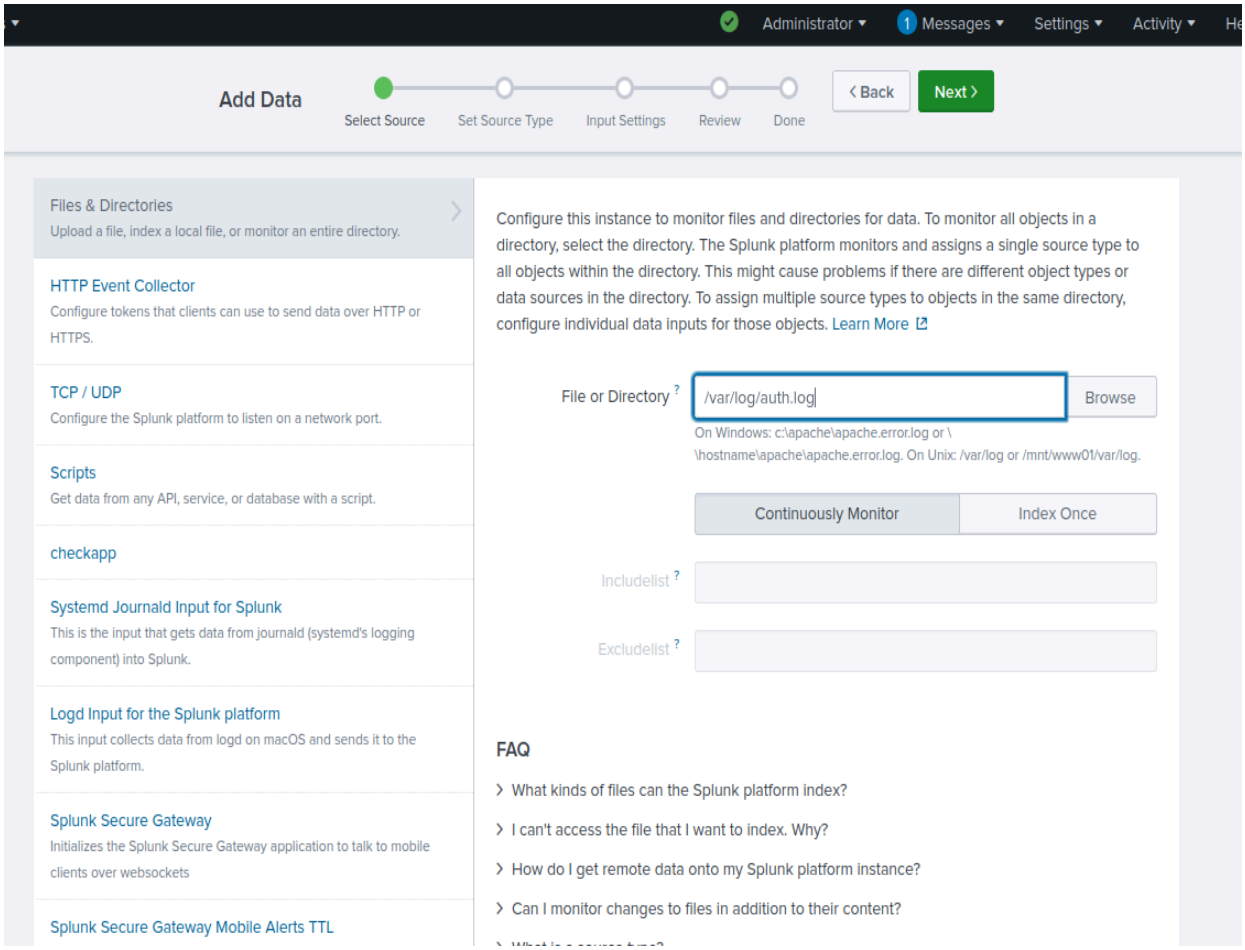
- Splunk Enterprise (Free)

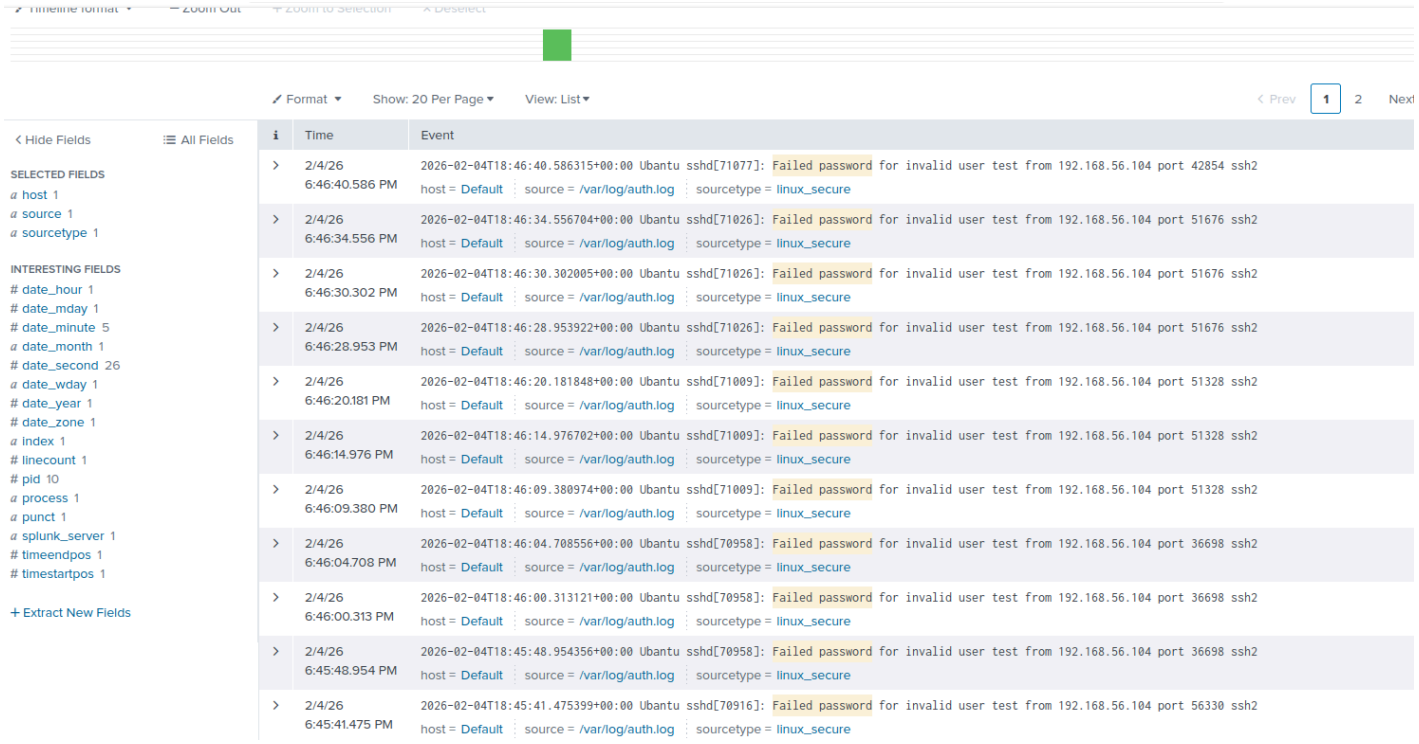
Detection Logic

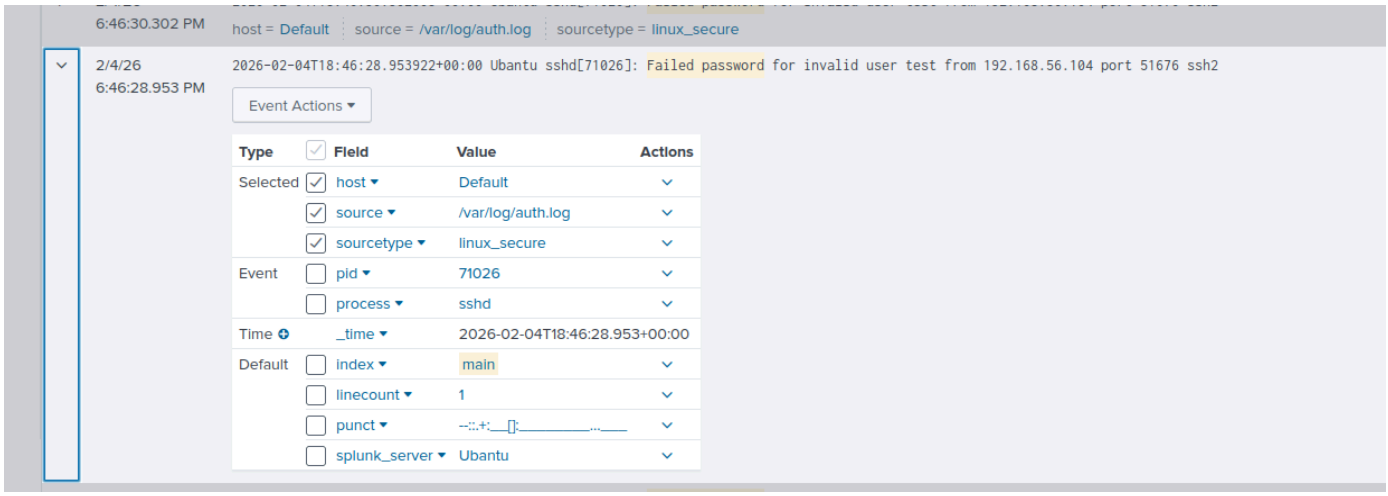
- Failed SSH authentication events (Failed password)
- Aggregation of failures by source IP

Evidence:

- Log ingestion configuration
- Failed SSH log entries
- Event-level details
- Aggregated statistics by attacker IP


Administrator
1 Messages
Settings
Activity
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
Files & Directories
Upload a file, index a local file, or monitor an entire directory.
HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.
TCP / UDP
Configure the Splunk platform to listen on a network port.
Scripts
Get data from any API, service, or database with a script.
checkapp
Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.
Logd Input for the Splunk platform
This input collects data from logd on macOS and sends it to the Splunk platform.
Splunk Secure Gateway
Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets
Splunk Secure Gateway Mobile Alerts TTL
Configure this instance to monitor files and directories for data. To monitor all objects in a directory, select the directory. The Splunk platform monitors and assigns a single source type to all objects within the directory. This might cause problems if there are different object types or data sources in the directory. To assign multiple source types to objects in the same directory, configure individual data inputs for those objects. Learn More
File or Directory
/var/log/auth.log
Browse
On Windows: c:\apache\apache.error.log or \\hostname\apache\apache.error.log. On Unix: /var/log or /mnt/www01/var/log.
Continuously Monitor
Index Once
Includelist
Excludelist
FAQ
What kinds of files can the Splunk platform index?
I can't access the file that I want to index. Why?
How do I get remote data onto my Splunk platform instance?
Can I monitor changes to files in addition to their content?





4. Noise vs Risk Analysis

Observed Behavior

- Multiple failed login attempts
- Single source IP
- Short time window

Potential Noise Indicators

- No successful authentication
- No lateral movement
- No privilege escalation
- IP not previously flagged

Potential Risk Indicators

- Repeated authentication attempts
- Use of SSH (remote access service)

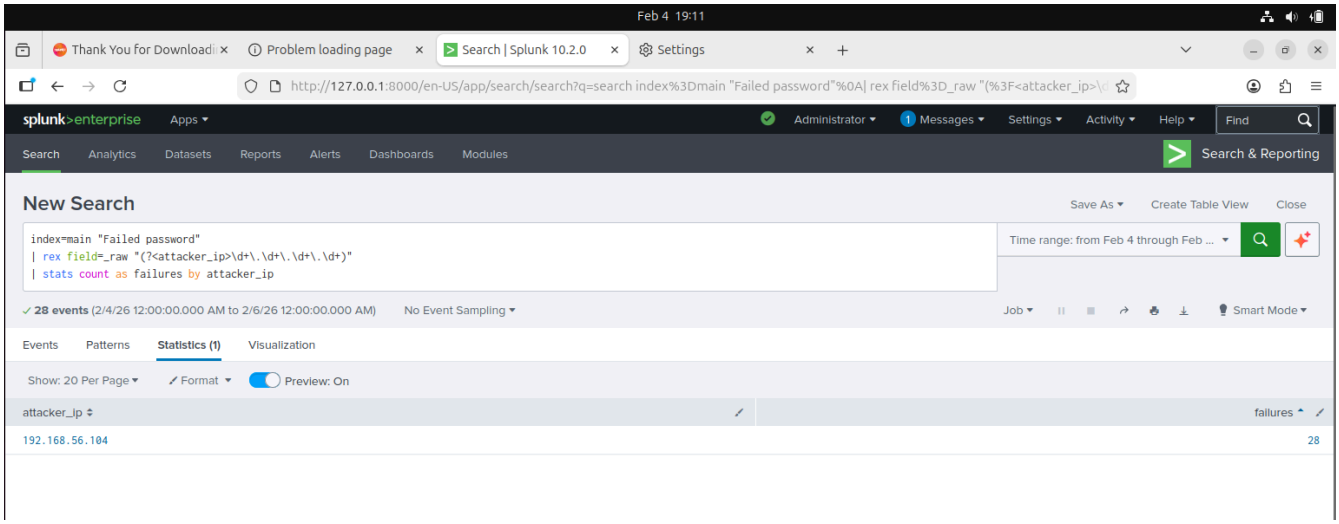
5. Event Aggregation & Alert Review in Splunk

Splunk was used to:

- Identify failed SSH attempts
- Group events by attacker IP
- Quantify attack volume

Detection Query (Conceptual)

- Failed authentication events
- Count by source IP
- Threshold-based review



6. Incident Context Enrichment (Why SOAR Is Required)

SIEM answers:

“What happened?”

SOAR + Threat Intel answers:

“How dangerous is it?”

Enrichment Objective

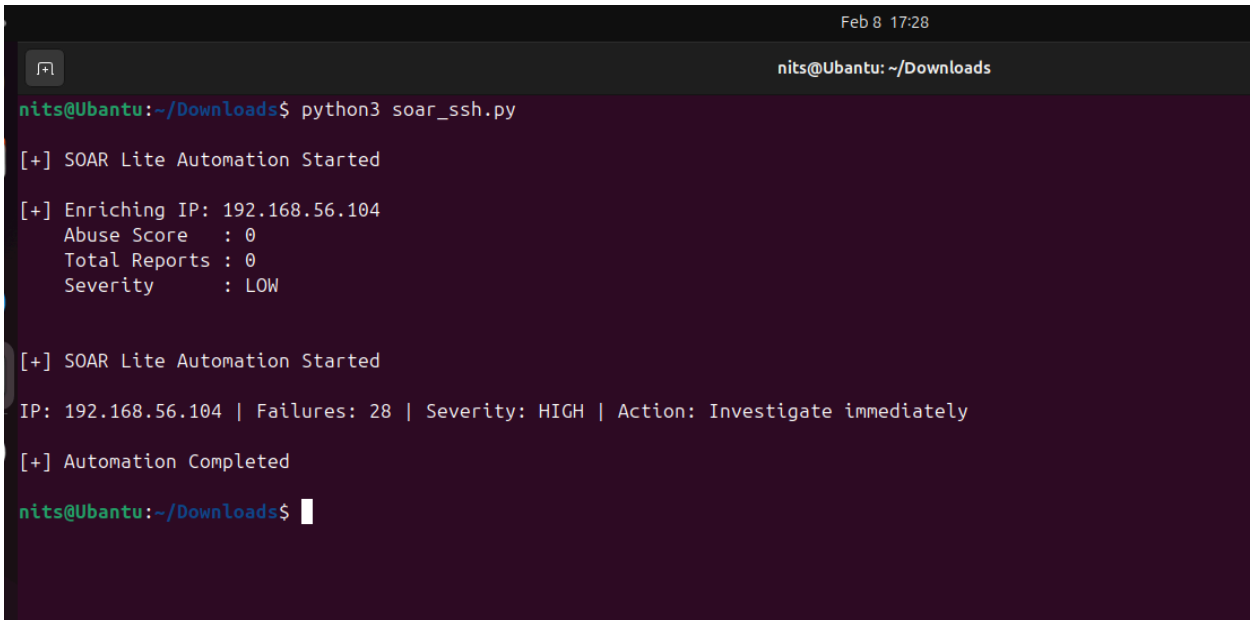
- Validate whether the attacking IP is **known malicious**
- Reduce false positives
- Support analyst decision-making

Threat Intelligence Source

- AbuseIPDB

Enrichment Data Retrieved

- Abuse confidence score
- Number of reports
- Reputation status



7. SOAR-Lite Automation (Analyst Efficiency)

A Python automation script was used to:

- Ingest SIEM-exported CSV alerts
- Extract attacker IPs
- Query AbuseIPDB API
- Assign severity based on reputation

- Produce analyst-readable output

Why Automation Matters in SOC

- Reduces manual lookups
- Ensures consistency
- Saves analyst time
- Prevents alert fatigue

8. Severity Classification & Decision Logic

Enrichment Results

- Abuse Confidence Score: Low
- Total Reports: None / Minimal
- IP Reputation: Clean

Final Severity

LOW

Justification

- No malicious reputation
- Lab-generated activity
- No signs of compromise

As analyst Decision:

No escalation required. Monitor for recurrence.

9. Incident Handling & Response Actions

Actions Taken

- Alert investigated
- IP behavior validated
- Severity assigned
- Incident documented

Actions Not Taken (Justified)

- No IP blocking
- No account lockout
- No escalation to IR team

Reason:

Response must be proportional to risk.

10. Communication & Escalation Evidence

Internal SOC Communication (Simulated)

Status Update (Tier-1 → Tier-2):

"Repeated SSH authentication failures detected from a single IP. Threat intelligence enrichment shows no malicious reputation. Severity classified as LOW. No further action required unless behavior persists."

11. Lessons Learned (As Analyst)

- Detection alone is insufficient

- Context determines severity
- Threat intelligence reduces noise
- Automation enhances analyst effectiveness
- Not every alert is an incident

12. Limitations & Future Improvements

Current Limitations

- Single-IP lab environment
- No real external attackers

Future Enhancements

- VirusTotal enrichment
- GeoIP analysis
- Automated response actions
- Case management integration
- Multi-source correlation

---

13. Conclusion

This project demonstrates an end-to-end **SOC detection and response workflow**, integrating SIEM monitoring, automation, threat intelligence enrichment, and analyst decision-making.
It reflects how modern SOC teams balance alert volume, accuracy, and operational efficiency.