TryHackMe Advent of Cyber 2025
Day 3 Challenge Report

Log Analysis with Splunk

1. Executive Summary

This report documents the completion of Day 3 of the TryHackMe Advent of Cyber 2025 event. The challenge focused on Security Information and Event Management (SIEM) using Splunk to analyze web traffic logs and firewall logs. Through systematic log analysis and correlation, successfully identified a multi-stage cyber attack including reconnaissance, exploitation, payload delivery, and command-and-control (C2) communication.

2. Challenge Overview

Objective: Use Splunk to analyze web traffic and firewall logs, identify anomalous behavior, trace an attack chain from reconnaissance through exploitation to C2 communication.

Tools: Splunk SIEM platform for log aggregation, searching, and visualization

3. Initial Data Exploration

3.1 Understanding Splunk Fields

Splunk automatically extracts and categorizes fields from ingested logs:

Selected Fields:

Basic metadata fields currently displayed in the event summary: host, source, sourcetype. These represent fundamental information about the log file origin.

Interesting Fields:

Fields automatically extracted or manually added by Splunk. Fields prefixed with # (e.g., #date_hour) are automatically generated by Splunk's time commands. Key fields identified:

- **user_agent** - Browser/client identification string
- **client_ip** - Source IP address of requests
- **path** - URL paths being accessed

3.2 Time-Based Analysis

Created a time chart to visualize traffic patterns and identify anomalous days:

```
index=main sourcetype="web_traffic"
| timechart span=1d count
| sort by count
| reverse
```

Result: Graph visualization revealed a significant traffic spike on **October 12, 2025**, indicating potential malicious activity.

4. Anomaly Detection & Investigation

4.1 Field-Based Anomaly Analysis

Analyzed key fields to identify suspicious patterns:

- **User Agent field:** 993 events recorded
- **Client IP field:** 198.51.100.55 showed unusually high activity
- **Path field:** 658 events with suspicious path patterns

4.2 Non-Standard User Agent Filtering

Filtered out legitimate browser user agents to isolate potentially malicious automation tools:

```
index=main sourcetype=web_traffic user_agent!=*Mozilla* user_agent!=*Chrome*
user_agent!=*Safari* user_agent!=*Firefox*
```

This query removed legitimate browser traffic, exposing automated tools like cURL, Wget, and scanning software.

4.3 Top Malicious IP Identification

Identified top 5 sources of non-browser traffic:

```
sourcetype=web_traffic user_agent!=*Mozilla* user_agent!=*Chrome* user_agent!=*Safari*
user_agent!=*Firefox*
| stats count by client_ip
| sort -count
| head 5
```

Primary Attacker Identified: 198.51.100.55 - Highest volume of suspicious activity

5. Attack Chain Analysis

5.1 Reconnaissance Phase

Investigated common reconnaissance patterns - probing for configuration files and testing path traversal:

```
sourcetype=web_traffic client_ip="198.51.100.55" AND path IN ("/.env", "/*phpinfo*",
"/.git*") | table _time, path, user_agent, status
```

Findings: Attacker probed for sensitive files including environment configuration files (.env), PHP info pages, and Git repositories - classic information gathering techniques.

Path Traversal Detection:

```
sourcetype=web_traffic client_ip="198.51.100.55" AND path="*..*" OR path="*redirect*"
sourcetype=web_traffic client_ip="198.51.100.55" AND path="*..\/..\/\*" OR
path="*redirect*" | stats count by path
```

Result: Multiple directory traversal attempts detected using ../ and ..\ patterns, attempting to access files outside the web root.

5.2 Exploitation Phase - SQL Injection

Searched for SQL injection tool signatures:

```
sourcetype=web_traffic client_ip="198.51.100.55" AND user_agent IN ("*sqlmap*", "*Havij*")
| table _time, path, status
```

Findings: SQLmap and Havij user agents detected - automated SQL injection tools. Presence of SLEEP(5) payloads confirmed successful exploitation attempts.

5.3 Data Exfiltration Attempts

Investigated attempts to download backup files and archives:

```
sourcetype=web_traffic client_ip="198.51.100.55" AND path IN ("*backup.zip*",
"*logs.tar.gz*") | table _time path, user_agent
```

Result: Attacker attempted to locate and download backup files, potentially containing sensitive data or credentials.

5.4 Remote Code Execution (RCE)

Identified the critical payload delivery phase:

```
sourcetype=web_traffic client_ip="198.51.100.55" AND path IN ("*bunnylock.bin*",
"*shell.php?cmd=*") | table _time, path, user_agent, status
```

Critical Finding: Execution of **/shell.php?cmd=./bunnylock.bin** detected.

Attack Classification: Remote Code Execution (RCE). The webshell execution of bunnylock.bin indicates a ransomware-like program was successfully executed on the compromised server.

6. Command & Control Communication

6.1 Firewall Log Analysis

Pivoted to firewall logs to identify post-exploitation C2 communication:

```
sourcetype=firewall_logs src_ip="10.10.1.5" AND dest_ip="198.51.100.55" AND
action="ALLOWED" | table _time, action, protocol, src_ip, dest_ip, dest_port, reason
```

Findings: Outbound connections from the compromised internal server (10.10.1.5) to the attacker's external IP (198.51.100.55) were successfully established.

6.2 Data Transfer Volume Analysis

Calculated total data transferred to attacker infrastructure:

```
sourcetype=firewall_logs src_ip="10.10.1.5" AND dest_ip="198.51.100.55" AND
action="ALLOWED" | stats sum(bytes_transferred) by src_ip
```

Critical Result: 126,167 bytes transferred from compromised web server to C2 server - confirming successful data exfiltration and ongoing command-and-control communication.

7. Attack Timeline & Kill Chain

Phase 1: Reconnaissance

- Automated probes using cURL/Wget
- Searched for configuration files (/.env)
- Tested path traversal vulnerabilities

Phase 2: Exploitation

- Deployed SQLmap for SQL injection attacks
- Confirmed exploitation with SLEEP(5) payloads
- Successfully compromised web application

Phase 3: Payload Delivery

- Uploaded webshell (shell.php)
- Deployed ransomware binary (bunnylock.bin)
- Executed malicious payload via RCE

Phase 4: Command & Control

- Established outbound connection from compromised server (10.10.1.5)
- Connected to attacker C2 infrastructure (198.51.100.55)
- Exfiltrated 126,167 bytes of data

8. Key Indicators of Compromise (IOCs)

Network Indicators:

- **Attacker IP:** 198.51.100.55
- **Compromised Server:** 10.10.1.5
- **Attack Date:** October 12, 2025

File Indicators:

- shell.php - Webshell for remote command execution
- bunnylock.bin - Ransomware payload

Tool Signatures:

- SQLmap - SQL injection automation
- Havij - SQL injection tool
- cURL/Wget - Non-browser automation
- SLEEP(5) payloads - SQL injection testing

9. Key Skills & Techniques Learned

9.1 Splunk Query Language (SPL)

- Time-based analysis with timechart
- Statistical aggregation with stats command
- Field filtering and boolean operations
- Wildcard pattern matching
- Data visualization and sorting

9.2 Log Analysis Methodology

- Baseline establishment through time-series analysis
- Anomaly detection using statistical thresholds
- Field-based correlation across multiple log sources
- Pivot analysis between web and firewall logs
- Attack chain reconstruction

9.3 Attack Pattern Recognition

- Reconnaissance techniques identification
- SQL injection tool signatures
- Path traversal attack patterns
- Webshell deployment indicators
- Remote Code Execution (RCE) detection
- C2 communication patterns

9.4 SIEM Best Practices

- Multi-source log correlation
- Automated field extraction and parsing
- Graph-based visualization for pattern identification
- Systematic investigation methodology

10. Key Takeaways

- SIEM platforms like Splunk are essential for detecting sophisticated attacks
- Time-series analysis reveals anomalous behavior patterns
- User-agent filtering helps isolate automated attack tools
- Attack chains follow predictable patterns:
  reconnaissance → exploitation → payload → C2
- Multi-source correlation provides complete attack visibility
- Early detection of reconnaissance activity can prevent full compromise
- Graph visualization accelerates anomaly identification

11. Conclusion

Day 3 of the TryHackMe Advent of Cyber 2025 provided comprehensive training in Security Information and Event Management using Splunk. Successfully traced a complete attack chain from initial reconnaissance through exploitation to command-and-control communication.

The investigation revealed a sophisticated multi-stage attack executed by IP 198.51.100.55 on October 12, 2025, culminating in the deployment of ransomware (bunnylock.bin) and the establishment of C2 communication with 126,167 bytes of data exfiltrated. The systematic use of Splunk's search capabilities, field analysis, and log correlation demonstrated the critical importance of SIEM platforms in modern cybersecurity operations.

Challenge Status: **COMPLETED ✓**