TryHackMe Advent of Cyber 2025
Day 15 Challenge Report

Web Attack Forensics with Splunk

1. Executive Summary

This report documents the completion of Day 15 of the TryHackMe Advent of Cyber 2025 event. The challenge focused on web attack forensics using Splunk to investigate command injection attacks against TBFC's drone scheduler. Successfully detected malicious web activity through Apache logs, investigated OS-level attacker actions using Sysmon data, decoded Base64-encoded PowerShell payloads, and reconstructed the full attack chain from initial compromise through post-exploitation reconnaissance.

2. Incident Overview

Scenario: TBFC's drone scheduler web UI receiving suspicious HTTP requests containing Base64-encoded chunks

Alert: "Apache spawned an unusual process"

Attack Type: Command Injection through vulnerable CGI script (hello.bat)

Investigation Goal: Triage incident, identify compromised hosts, decode payloads, determine scope

3. Investigation Methodology

Utilized Splunk to pivot between:

- **Web Layer:** Apache access and error logs
- **Host Layer:** Sysmon telemetry for process creation

4. Investigation Steps

4.1 Step 1: Detect Suspicious Web Commands

Objective:

Search HTTP requests for command execution attempts (cmd.exe, PowerShell, Invoke-Expression)

Splunk Query:

```
index=windows_apache_access (cmd.exe OR powershell OR "powershell.exe" OR "Invoke-Expression") | table _time host clientip uri_path uri_query status
```

Findings:

- Identified Base64-encoded PowerShell commands
- Vulnerable CGI script: hello.bat
- Command injection attempts present

Payload Analysis:

Encoded String

```
VABoAGkAcwAgAGkAcwAgAG4AbwB3ACAATQBpAG4AZQAhACAATQBVAEEASABBAEEASABBAEEA
```

Decoded Output:

This is now Mine! MUAHAAHAA

4.2 Step 2: Server-Side Errors & Command Execution

Objective:

Inspect Apache error logs for execution attempts or internal failures

Splunk Query:

```
index=windows_apache_error ("cmd.exe" OR "powershell" OR "Internal Server Error")
```

Key Indicators:

- HTTP 500 Internal Server Error responses
- Requests like /cgi-bin/hello.bat?cmd=powershell triggering errors
- Confirms attacker input processed by server but failed during execution

4.3 Step 3: Trace Suspicious Process Creation

Objective:

Explore Sysmon for malicious executables spawned by Apache web server

Splunk Query:

```
index=windows_sysmon ParentImage="*httpd.exe"
```

Critical Finding:

```
ParentImage = C:\\Apache24\\bin\\httpd.exe Image        = C:\\Windows\\System32\\cmd.exe
```

Analysis: Apache should only spawn worker threads, NOT system processes. Finding cmd.exe as child process indicates successful command injection penetrating the OS.

Significance: Strongest indicator that web attack penetrated the operating system

4.4 Step 4: Confirm Attacker Enumeration

Objective:

Discover post-exploitation reconnaissance activities

Splunk Query:

```
index=windows_sysmon *cmd.exe* *whoami*
```

Findings:

- Located: whoami.exe execution
- Found in: Interesting files → originalfile
- Purpose: Determine user account context

Analysis: Attackers commonly use 'whoami' immediately after gaining code execution. This confirms post-exploitation reconnaissance and successful command execution on host.

4.5 Step 5: Identify Base64-Encoded PowerShell Payloads

Objective:

Find all successfully encoded PowerShell commands

Splunk Query:

```
index=windows_sysmon Image="*powershell.exe" (CommandLine="*enc*" OR CommandLine="*-EncodedCommand*" OR CommandLine="*Base64*")
```

Expected Result:

With proper defenses: No results (encoded payload never executed)

If results appear: Decode Base64 to inspect attacker's true intent

5. Challenge Answers

5.1 Question 1: Reconnaissance Executable

Question: What is the reconnaissance executable file name?

Location:

Interesting files → originalfile

Answer: whoami.exe

5.2 Question 2: Command Injection Executable

Question: What executable did the attacker attempt to run through the command injection?

Answer: powershell.exe

6. Attack Chain Reconstruction

6.1 Initial Access

1. Attacker identified vulnerable CGI script (hello.bat)
2. Crafted HTTP requests with command injection payloads
3. Used Base64 encoding to obfuscate malicious commands

6.2 Exploitation

4. Sent malicious requests to /cgi-bin/hello.bat
5. Server processed attacker input
6. Apache (httpd.exe) spawned cmd.exe - successful OS penetration
7. Some attempts triggered Internal Server Errors

6.3 Post-Exploitation

8. Executed whoami.exe for reconnaissance
9. Determined user account context
10. Attempted PowerShell execution with encoded commands

7. Key Skills Developed

- Splunk query construction and optimization
- Apache log analysis (access and error logs)
- Sysmon process creation telemetry analysis
- Base64 payload decoding and analysis
- Command injection attack detection
- Parent-child process relationship analysis
- Web-to-OS attack chain reconstruction
- Blue Team incident response methodology

8. Conclusion

Day 15 of the TryHackMe Advent of Cyber 2025 provided comprehensive training in web attack forensics using Splunk. Successfully investigated command injection attacks by pivoting between web server logs (Apache) and host-level telemetry (Sysmon), demonstrating the critical importance of multi-layer visibility in Blue Team operations.

The investigation revealed a complete attack chain from initial command injection through vulnerable CGI script, successful OS penetration via spawned system processes, to post-exploitation reconnaissance. Key findings included Base64-encoded PowerShell commands, Apache spawning cmd.exe (strongest OS penetration indicator), and whoami.exe execution confirming attacker enumeration activities. This challenge highlighted the power of SIEM correlation in detecting and analyzing multi-stage web attacks.

Challenge Status: **COMPLETED ✓**