**Investigating with Splunk**

## Investigating with Splunk – Challenge Notes

### Scenario Overview

* You step into the shoes of SOC Analyst Johny.
* Anomalous behavior is believed to be happening on some Windows machines.
* Your task: Analyze ingested logs in the main index using Splunk and uncover what occurred.

### Key Investigation Steps & Findings

| **Question** | **Query Example (index="main" ...)** | **What to Look For** | **Answer** |
| --- | --- | --- | --- |
| **1. Total events in index "main"** | index="main" | Total count of logs (ensure time filter is set to “All time”) | **12,256** [mattheweaton.net](https://mattheweaton.net/posts/investigating-with-splunk-tryhackme-walkthrough/?utm_source=chatgpt.com)[Patryk Łabuz](https://hexseven.pl/articles/investigating-with-splunk/?utm_source=chatgpt.com) |
| **2. New backdoor username created** | EventID=4720 | Sysmon logs new user creation events | **A1berto** [Patryk Łabuz](https://hexseven.pl/articles/investigating-with-splunk/?utm_source=chatgpt.com)[mattheweaton.net](https://mattheweaton.net/posts/investigating-with-splunk-tryhackme-walkthrough/?utm_source=chatgpt.com) |
| **3. Registry key path modified for backdoor user** | EventID=13 A1berto maybe Hostname filter | Registry create/delete events relating to A1berto | **HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto** [Patryk Łabuz](https://hexseven.pl/articles/investigating-with-splunk/?utm_source=chatgpt.com)[mattheweaton.net](https://mattheweaton.net/posts/investigating-with-splunk-tryhackme-walkthrough/?utm_source=chatgpt.com) |
| **4. Impersonated (original) user** | index="main" then check User field | Identify intended legitimate target | **Alberto** [Patryk Łabuz](https://hexseven.pl/articles/investigating-with-splunk/?utm_source=chatgpt.com)[mattheweaton.net](https://mattheweaton.net/posts/investigating-with-splunk-tryhackme-walkthrough/?utm_source=chatgpt.com) |
| **5. Command used to add backdoor user** | EventID=1 or 4688 + filter A1berto | Process creation events with command string | **WMIC.exe /node:WORKSTATION6 process call create “net user /add A1berto paw0rd1”** [Patryk Łabuz](https://hexseven.pl/articles/investigating-with-splunk/?utm_source=chatgpt.com)[mattheweaton.net](https://mattheweaton.net/posts/investigating-with-splunk-tryhackme-walkthrough/?utm_source=chatgpt.com) |
| **6. Login attempts by backdoor user** | EventID=4624 OR 4625 A1berto | Look for successful or failed login attempts | **0** [Patryk Łabuz](https://hexseven.pl/articles/investigating-with-splunk/?utm_source=chatgpt.com)[mattheweaton.net](https://mattheweaton.net/posts/investigating-with-splunk-tryhackme-walkthrough/?utm_source=chatgpt.com) |
| **7. Host with suspicious PowerShell execution** | PowerShell | Check Hostname field for systems executing PS | **James.browne** [Patryk Łabuz](https://hexseven.pl/articles/investigating-with-splunk/?utm_source=chatgpt.com)[mattheweaton.net](https://mattheweaton.net/posts/investigating-with-splunk-tryhackme-walkthrough/?utm_source=chatgpt.com) |
| **8. PowerShell logging event count** | EventID=4103 (PS logging) | Count how many PS commands were logged | **79** [Patryk Łabuz](https://hexseven.pl/articles/investigating-with-splunk/?utm_source=chatgpt.com)[mattheweaton.net](https://mattheweaton.net/posts/investigating-with-splunk-tryhackme-walkthrough/?utm_source=chatgpt.com) |
| **9. Full URL from encoded PowerShell script** | Decode base64 from logs, identify string | Often embedded in CommandLine or ContextInfo | **hxxp[://]10[.]10[.]10[.]5/news[.]php** [Patryk Łabuz](https://hexseven.pl/articles/investigating-with-splunk/?utm_source=chatgpt.com)[mattheweaton.net](https://mattheweaton.net/posts/investigating-with-splunk-tryhackme-walkthrough/?utm_source=chatgpt.com) |

### Summary of Insights

* The attacker created a backdoor user **A1berto**, likely targeting the real user **Alberto**.
* A registry key was created to support persistence.
* The backdoor user **did not successfully log in** (0 login attempts detected).
* Host **James.browne** executed malicious PowerShell payloads.
* A PowerShell script containing a base64-encoded C2 URL was found and successfully decoded to retrieve the flag URL.

### Why This Worked & What It Demonstrates

* **Filtering by EventID** is a powerful way to focus on relevant log entries.
* **Field pivots** (exploring usernames, hostnames, command lines) lead to deeper context.
* Combining Splunk search with **external tools (e.g., CyberChef)** to decode payloads is invaluable.
* This challenge showcases real SOC analyst skills: **log engineering**, **threat detection**, and **incident reconstruction**.

