Lucas McMahon
9/24/23

Investigating a Compromised Host: Analyzing Process Execution and Payload Delivery Using Splunk

Table of Contents

- Introduction
- Objectives
- Lab Environment
- Tools and Technologies Used
- Step-by-Step Process
- Results and Analysis
- Challenges Faced
- Conclusion
- References

Introduction

This lab focuses on investigating a suspicious process execution detected in the HR department of a client's network. The investigation begins after one of the Intrusion Detection Systems (IDS) flagged potentially malicious activity. By analyzing process execution logs ingested into Splunk, we aim to identify a compromised host, examine the actions taken, and trace the attack to its root cause. The compromised system is suspected of running unauthorized scheduled tasks and downloading malicious payloads using system processes (LOLBins).

Objective

The primary objective of this lab is to:

1. Investigate suspicious activity flagged by the IDS.
2. Identify compromised accounts and malicious actions.
3. Determine the LOLBins used to bypass security controls and download payloads.
4. Trace the source of the malicious payload.
5. Analyze and **retrieve the flag** to complete the investigation.

Lab Environment

- The network is segmented into three logical groups: IT, HR, and Marketing departments.
- The investigation is focused on Event ID 4688 logs, related to process execution, gathered from HR hosts and ingested into Splunk.
- Splunk was used to search and filter through process execution logs, focusing on specific users and activity within the HR department.
- Hosted on TryHackMe, a CyberSecurity Training Site

Lucas McMahon
9/24/23

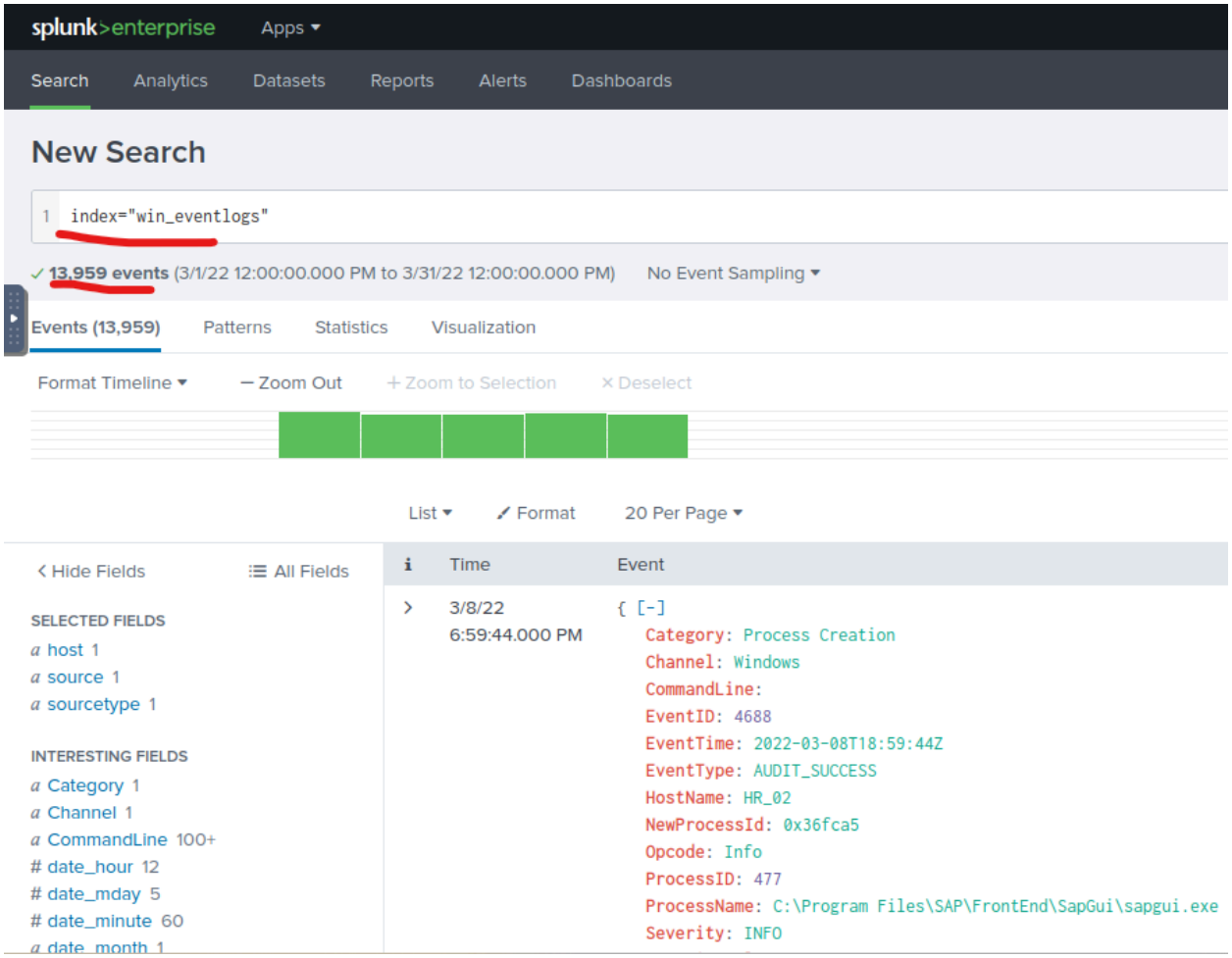
Tools and Technologies

- Splunk: Used for log analysis and filtering. Ingested Event ID 4688 logs are explored to trace suspicious activities.
- Windows Event Logs (Event ID: 4688): Logs related to process creation and execution.
- CertUtil: A built-in Windows utility used as a system process (LOLBIN) to download payloads.
- File-sharing platforms: Investigated for hosting the payloads used in the attack**.**

Step-by-Step Process

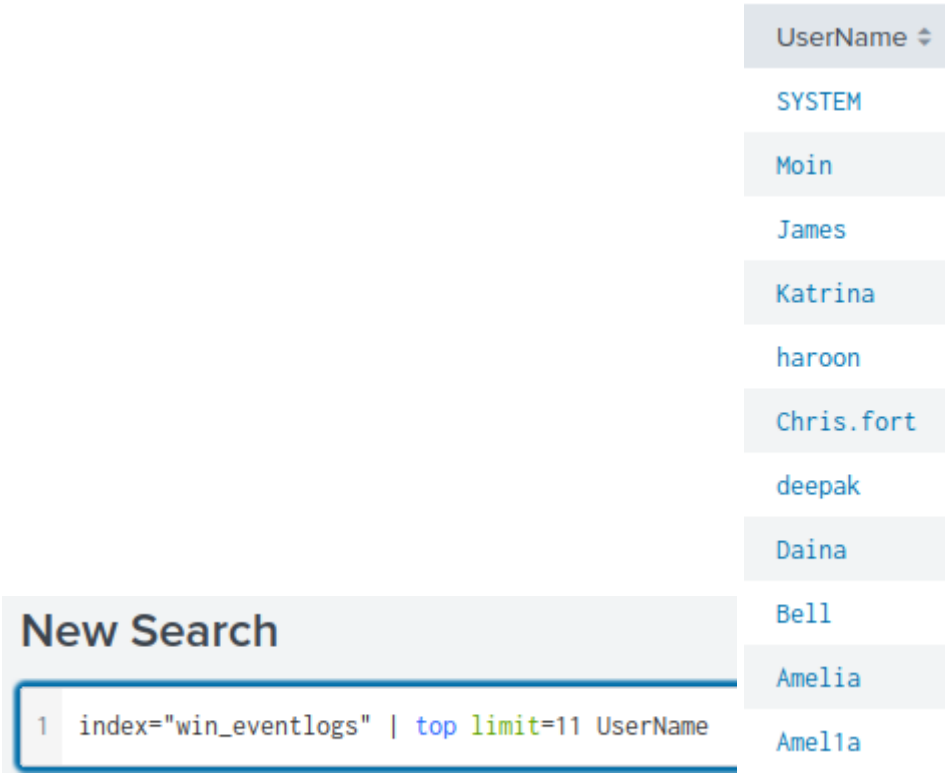
Step One

Logging into the Splunk account and setting our search query to March 2022, with the search index *win_eventlogs*, we can see a large number of matching logs giving us a plethora of information.



Lucas McMahon
9/24/23

The first task was to identify an imposter account. Using Splunk's filtering capabilities, I listed all 11 usernames with activity in the specified timeframe.



Among them, there is a duplicate account with the alias **Amel1a**, which likely attempted to conceal activity by mimicking the real account.

Step Two

The next task is to find someone in the HR department who has been running scheduled tasks. I am going to filter through all logs that use *Schtasks.exe* and list out all the usernames from the HR department referencing the employee sheet from before..

```
1  index=win_eventlogs (UserName="haroon" OR "Chris.fort" OR "Daina") AND "Schtasks.exe"
2  | stats count by CommandLine
```

✓ **1 event** (3/1/22 9:00:00.000 PM to 3/31/22 9:27:13.000 PM) No Event Sampling

Events Patterns **Statistics (1)** Visualization

20 Per Page ▾ Format Preview ▾

CommandLine
/create /tn OfficUpdater /tr "C:\Users\Chris.fort\AppData\Local\Temp\update.exe" /sc onstart

Splunk gives us the ability to view all usernames associated through the filtered logs and their number of occurrences sorted. We can see *Chris.fort* is the only HR member here using scheduled tasks.

Step Three

Step three asks to investigate an HR user executing a system process to download a payload from a file sharing host. Doing some research on the windows security forum I can find that the event ID of 4688 references a process creation/execution.

[Ultimate Windows Security]

Building off the filter from before, I can remove the scheduled tasks part and replace it with the EventID, and find my result.

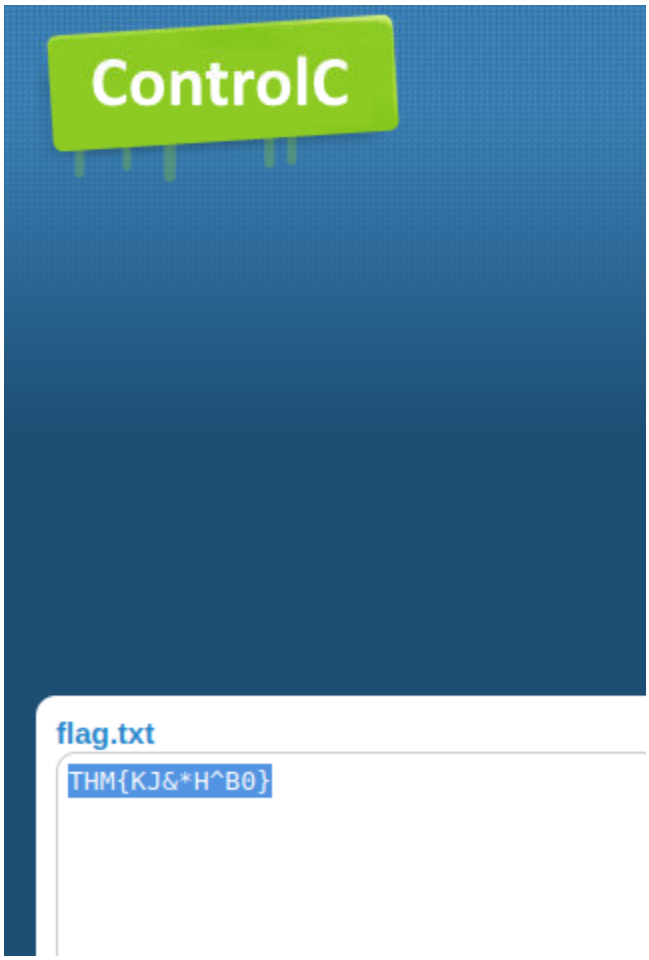
Lucas McMahon
9/24/23

This log gives us a ton of information. From the command line, *certutil.exe* was run to download a payload named *benign.exe* from a website called *controlc[.]com*. This occurred on March 3rd 2022 around 10:30 from the host *HR_01*. And it looks like the user *Haroon* is who we are looking for.

Lucas McMahon
9/24/23

Step Four

Finally, I investigated the URL https://controlc[.]com/e4d11035 used to download the payload. The analysis revealed the content of the payload and the flag required for the investigation.



Results and Analysis

Through log filtering and detailed analysis, the following key points were identified:

- An imposter account (Amel1a) was actively mimicking a real user to evade detection.
- Chris.fort from the HR department was running scheduled tasks, indicating potential unauthorized system maintenance or exploitation.
- Haroon used certutil.exe to download a malicious payload, indicating a breach of security controls through a known LOLBIN technique.

- The payload hosted on controlc[.]com was retrieved and found to contain malicious content, confirming the attack on the HR department's host.

Challenges Faced

One of the challenges was ensuring accurate filtering within Splunk to isolate relevant logs. Searching through large volumes of data required precise queries, especially when identifying specific users and processes. Additionally, the use of system processes like certutil.exe (a legitimate tool) for malicious activity made it difficult to immediately flag the activity as suspicious.

Conclusion

The investigation successfully identified a compromised host within the HR department and traced malicious activities back to specific users and actions. The use of LOLBINs like certutil.exe to bypass security controls and download a payload was confirmed. By leveraging Splunk's log analysis capabilities, we were able to pinpoint the imposter account, scheduled tasks, and malicious downloads that contributed to the compromise.

References

- Splunk Documentation: Splunk Event Search Reference
- Ultimate Windows Security: Event ID 4688 - Process Creation
- Windows CertUtil Documentation: CertUtil
- LOLBAS Documentation: LOLBAS