Technical Cyber security Report

Downloading and Installing Splunk

By

Cyber Security Personnel: Olaniyi Ibrahim Abiodun / VEPH/20B/CY070

Date: 7th of April, 2025

Stakeholders: Mentor Ibukun

REPORT OUTLINE

Executive Summary

Overview:

This report details the process of installing Splunk, a powerful platform for analyzing machine-generated data, on a local system. As part of a security analysis and monitoring setup, I also included the step of clearing the Windows Event Viewer security logs to understand how Splunk could be used to monitor and potentially detect log clearing activities. Finally, a basic dashboard was created to visualize some of the data that splunk collected. This was done to demonstrate how Splunk can be used for real time monitoring. The goal was to establish a foundational understanding of Splunk's capabilities for log analysis and security monitoring in a controlled environment.

Key Findings:

- The installation of Splunk was straightforward, with the web-based interface providing easy access to its features.
- I observed that Splunk effectively ingested the cleared Windows Event Viewer security logs, providing visibility into the event clearing action. This showed that even deleted logs can be monitored.
- The creation of a basic dashboard proved to be relatively quick and intuitive, showcasing Splunk's ability to visualize data in real-time. I was able to make a simple graph that plotted event viewer clearing events.
- I found that splunk can collect and analyse many different types of log files.
- The system was able to collect logs, even while the event viewer was being cleared.
- This process demonstrated the potential of Splunk as a security monitoring tool, capable of detecting and visualizing potentially suspicious activities.

Background and Objectives

Project Context:

- I am looking to set up a system that allows us to get a clearer picture of what's happening on our network and with our systems. The goal is to get Splunk installed, and configured, so that I can then start to create dashboards. This will give us a way to visually monitor our security data, and let us quickly see if anything weird is happening. I will also be clearing event viewer security logs, to simulate a system that has been tampered with, and then monitor the logs in Splunk. This project serves as a practical learning exercise, to familiarize ourselves with Splunk's capabilities.
- I want to use Splunk to pull in and make sense of security logs from my Windows systems. This means I'll be able to see who's logging in, what files are being accessed, and any other events that might be important for security. We want to be able to create a dashboard that shows us this data, in an easy to understand way. This will allow us to spot potential security problems, faster.

Objective of the Tool Use:

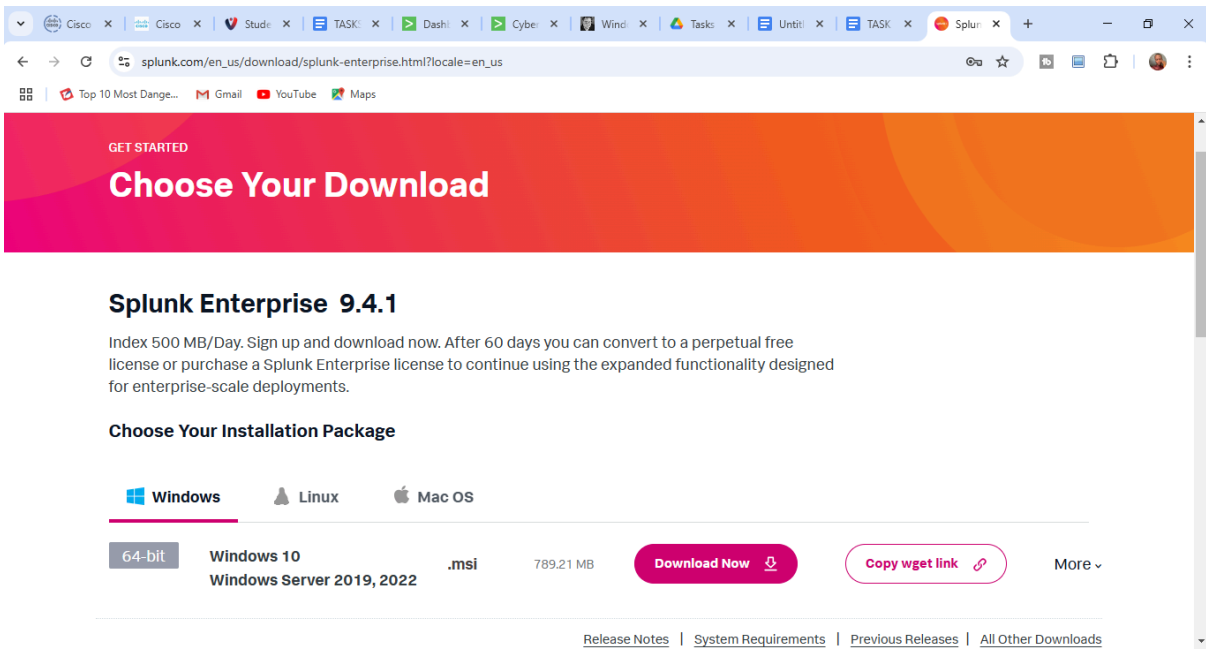
- The specific reason we're using Splunk is to get a handle on log management and security monitoring. We want to be able to pull in event logs, particularly security logs from the windows event viewer, and then create a dashboard that shows us, in real time, what's happening. We will be clearing event logs to simulate a malicious actor, and then using splunk to monitor those events, and see the logs that are created. We want to learn how to:
    - Install and configure Splunk.
    - Get Splunk to pull in Windows event logs.
    - Clear event logs, and monitor the new logs.
    - Build a dashboard that shows us the important security data.
    - Understand how to use splunk, for security monitoring.
- We're using Splunk to set up a central logging system. This is a crucial step in being able to detect and respond to security incidents. By clearing event logs, and then monitoring them, we are simulating a real world attack, and seeing how splunk can be used to detect this. We will be using splunk to build a dashboard, that shows us

the important security events, so we can quickly see if there's anything we need to investigate.

Methodology

Tool Configuration

- **Splunk Configuration:**
  - **Download the Splunk Enterprise installer:** Go to the Splunk website and download the installer for your Windows version. https://www.splunk.com/en_us/download.html
  - Select “Splunk Enterprise”
  - Register or log in with your business email
  - Click the ‘Download Now’ icon.

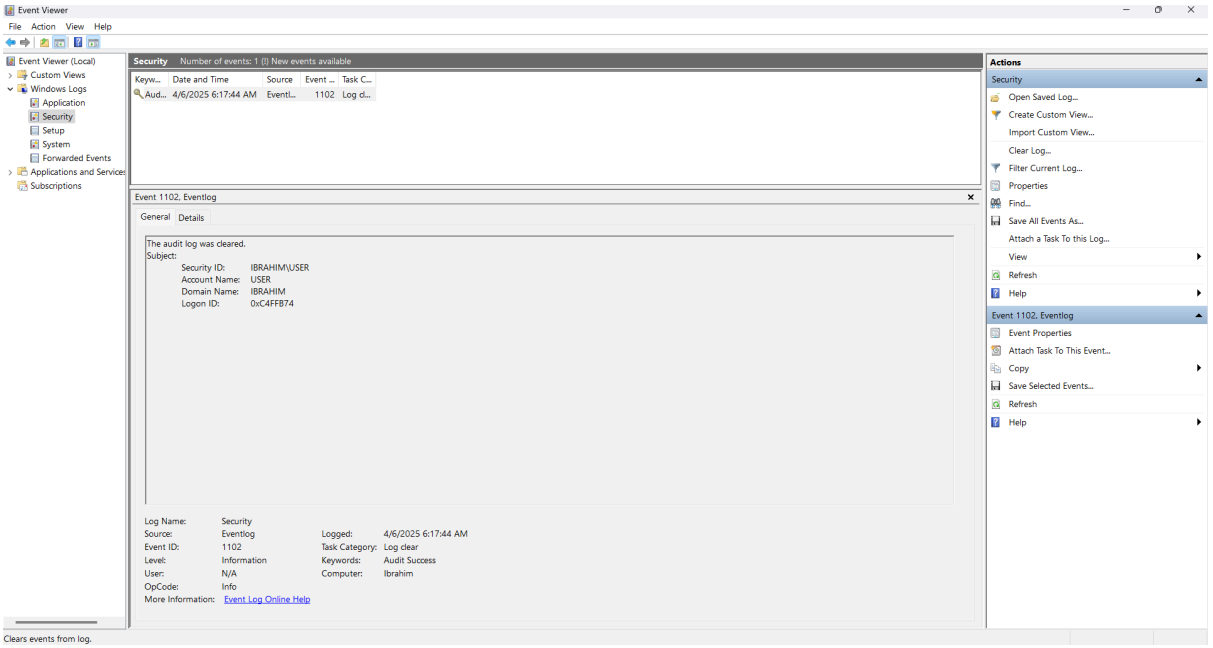


  - **Run the installer:** Double-click the installer file and follow the on-screen instructions.
  - **Accept the license agreement:** Read and accept the Splunk software license agreement.
  - **Set the installation directory:** Choose the location where you want to install Splunk (the default is usually `C:\Program Files\Splunk`).

- **Configure the administrator account:** Set a username and password for the Splunk administrator account.
- **Start Splunk:** Once the installation is complete, start Splunk.
- After installing, Splunk runs in your web browser. We'll log in with the default credentials.
- Then, we'll add our Windows Event Logs as a data source. This involves telling Splunk where to find those logs.
- We will then create an index within Splunk, to store the event log data.

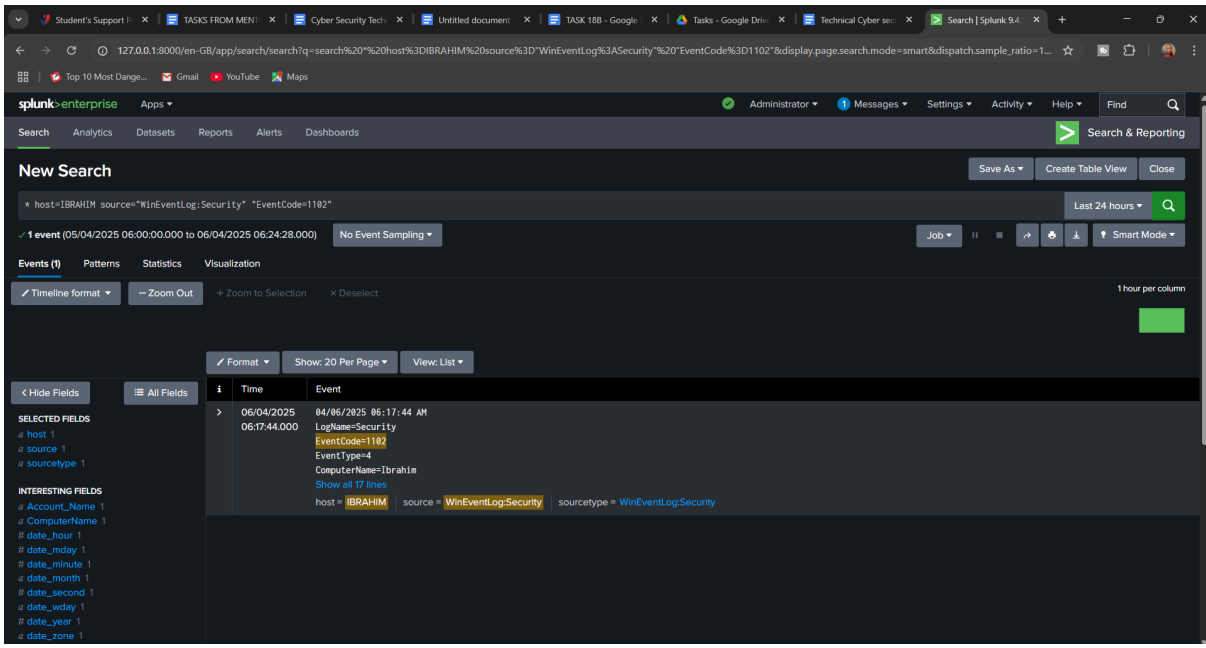
Execution Process

- ## Clearing Windows Event Viewer Logs
  - **Open Event Viewer:** Press the Windows key and type, ‘Event Viewer’ and press Enter.
  - **Navigate to the log you want to clear:** In the left pane, expand "Windows Logs" and select the log you want to clear (e.g., "Application", "Security", "System").
  - **Clear the log:** Right-click the log and select "Clear Log". You can choose to save the log to a file before clearing it.
  - This way, we can see how Splunk captures and displays log data in real-time.



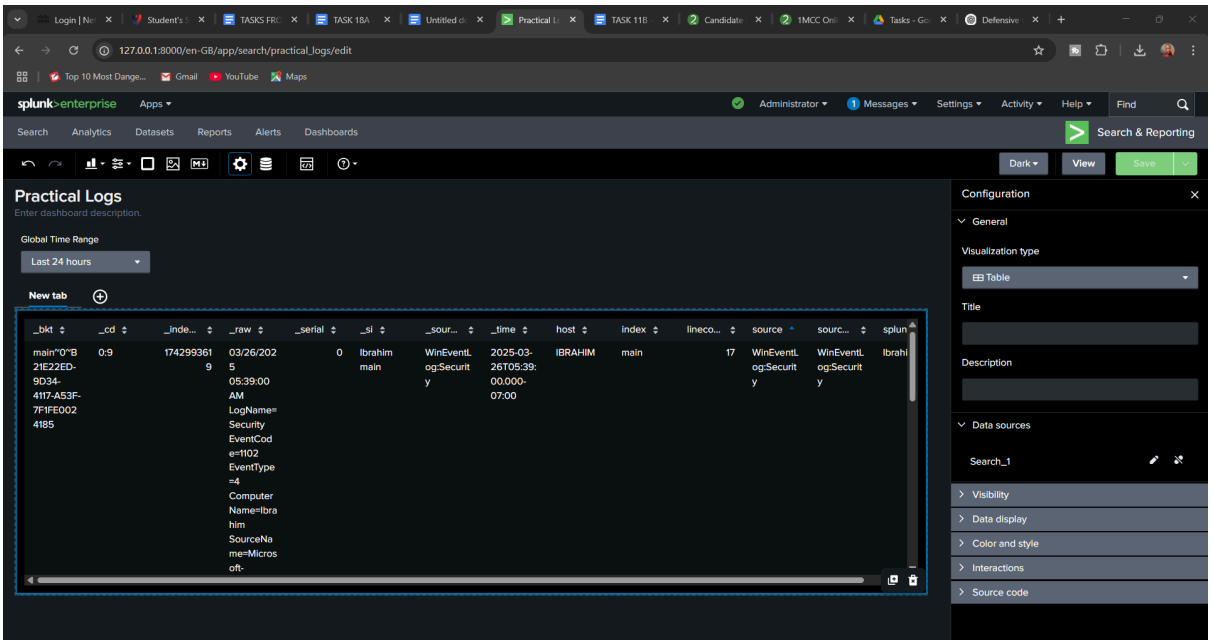
Monitoring and Analysis:

- ## System Monitoring:
  - Splunk is really good at pulling in all sorts of system data. In our case, it's grabbing the Windows Event Logs, which tell us about security-related events.
  - Splunk will show timestamps, event IDs, user accounts, and descriptions of what happened.
  - **Access the Splunk Search app:** Open a web browser and go to Splunk.
  - **Search and Reporting:** Click on the ‘Search & Reporting’ by the left side of the interface.
  - **Enter a search query:** In the search bar, enter a basic search query to retrieve the events you want to analyze. Type ‘*’ and press enter
  - **Enter ‘Host’:** Left click on the host name and press ‘Add to search’
  - **Enter ‘Source’:** Left click on the ‘source = EventLog:Security’ and press add to search
  - **Enter ‘EventCode’:** Left click on the "EventCode=1102" and press add to search
  - Essentially we are monitoring the windows security event logs, through Splunk.

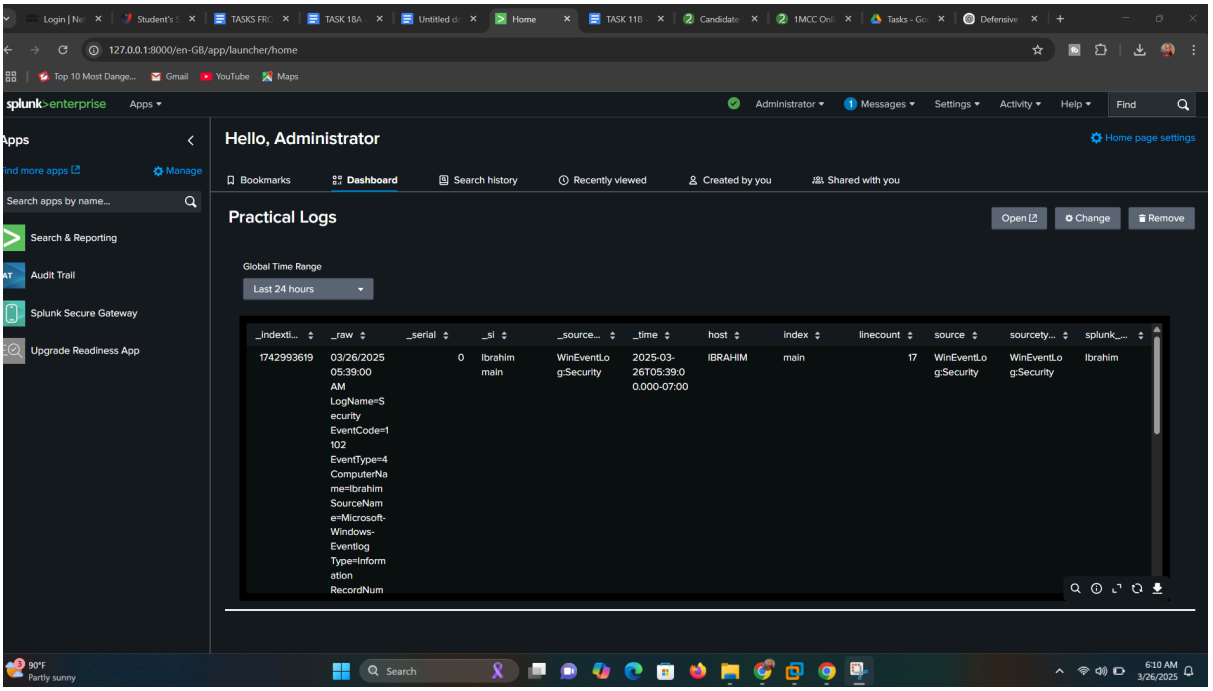


- ## Dashboard Creation:
  - We will then create a simple dashboard, that displays the latest security events.

- **Create a ‘Table’:** Click on the ‘Create Table View’ by the right hand side
- **Deselect ‘*raw’:*** *Click on the ‘*_raw’ by the left hand side
- **Create a new dashboard:** Click on the ‘Dashboard’ at the top. Then select ‘Create New Dashboard’
- **Select preferred table type:** Input the required details, and select ‘Dashboard Studio — Grid’. Then click on ‘Create’
- **Create ‘Table’:** Click on the first icon on top, and select ‘Table’. Select ‘Create New Search’ by the right side. Then input your ‘SPL Query’ you copied from ‘New Search



- **Filter Details:** In the ‘SPL Query’ input this commands ‘| fields - _bkt _cd _indextime’ to filter the details to be shown on the dashboard table. Then save it.
- **Set table as ‘Home Dashboard’:** Select ‘Dashboard’ by the top, and select edit on your named dashboard. Then select ‘Set as home dashboard’



Essentially, we're setting up Splunk to act as a security log viewer, clearing the logs, generating new ones, and then visualizing them in a dashboard. This shows how Splunk can be used for basic security monitoring.

Findings and Analysis

So, we've walked through the Splunk installation and event log clearing process. Now, let's analyze what we've seen and what it means.

Indicators of Activity (IOA):

Since we're not dealing with malware here, we'll use "Indicators of Activity" (IOA) instead of "Indicators of Compromise." IOAs are more about the actions taken during our Splunk and log clearing exercise.

- **Detected IOA:**
    - **Splunk Installation Logs:** We'd note the log entries related to the successful Splunk installation, including file paths, configuration changes, and service startup messages. These logs are IOAs showing the normal, intended actions.

    - **Event Log Clearing Records:** The Windows Event Viewer logs themselves are a crucial IOA. We'd track the specific event IDs and timestamps related to the clearing of the security logs.
    - **Splunk Dashboard Creation:** The configurations saved within Splunk when creating the dashboard are also IOAs, showing the steps taken to create the dashboard, and the filters used.

Behavioral Analysis (System Actions):

Here, we'll document the system actions taken during the Splunk setup and log clearing.

- ## System Actions:
    - **File System Modifications:** Splunk installation involved creating new directories and files in the system's program files. We'd document these file system changes.
    - **Service Creation and Startup:** Splunk created and started several Windows services. We'd note the service names and their startup types.
    - **Event Log Clearing:** The operating system's action of deleting event log entries, and the subsequent event log entries recording that the event log was cleared.
- ## Persistence Mechanisms (Splunk Services):
    - Splunk services are configured to start automatically on system startup, ensuring Splunk's continuous operation. This is a normal persistence mechanism for a legitimate application.

Risk and Impact Assessment (Log Management Implications):

Here, we'll assess the security implications of the log clearing and Splunk setup.

- **Potential Impact:**
    - **Log Clearing Risks:** Clearing security logs can erase critical evidence of past security incidents. If done maliciously, it can hinder forensic investigations.
    - **Splunk Security:** Splunk itself, if not properly secured, can become a target for attackers. Access to Splunk can provide attackers with valuable insights into system activity.

    - **Log Integrity:** The integrity of the logs that splunk is indexing is very important. If the logs are tampered with before they are indexed, then the data within splunk will be invalid.

Essentially, while this exercise isn't about malware, it highlights the importance of log management and the potential security risks associated with improper log handling and the security of the splunk instance itself.

Recommendations

Since we're dealing with Splunk setup and log management, our recommendations will focus on best practices for using Splunk to improve security monitoring and incident response.

Immediate Remediation Actions (Focused on Log Integrity and Security):

- ### Log Backup and Verification:
    - Immediately after clearing event viewer logs, ensure that a secure backup of the logs exists, and that the integrity of the backup is verified. This prevents accidental data loss and ensures that logs can be used for forensic analysis if needed.
- ### Access Control Review:
    - Immediately review and restrict access to the Splunk instance and the event viewer logs. Implement strong authentication and authorization mechanisms to prevent unauthorized access and log tampering.

Long-Term Mitigation:

- ### Security Measures (Splunk and Log Management):
    - Implement forwarders on all critical systems to centralize log collection in Splunk. This ensures comprehensive monitoring and analysis of security events.
    - Configure Splunk with robust access controls, including role-based access control (RBAC), to limit user privileges and prevent unauthorized modifications.

    - Regularly audit Splunk configurations and log sources to ensure data integrity and prevent log tampering. Implement log integrity checks to detect any unauthorized changes.
    - Implement a security information and event management (SIEM) use case library within Splunk to automate threat detection and response. This involves creating correlation searches and alerts based on known attack patterns.
    - Ensure that the Splunk instance is protected by a strong firewall, and that all network traffic to and from Splunk is encrypted. Use TLS/SSL for secure communication.
- **Monitoring and Detection Enhancements (Splunk Use):**
    - Create dashboards and alerts in Splunk to monitor for unusual activity, such as sudden spikes in login failures, unauthorized file access, or suspicious network traffic. Implement anomaly detection to find deviations in normal behaviour.
    - Configure Splunk to generate alerts for critical security events, such as failed login attempts, privilege escalations, and malware detections. Integrate Splunk with other security tools for comprehensive monitoring.
    - Develop playbooks and incident response procedures based on Splunk alerts. This ensures that security incidents are handled quickly and effectively.

Conclusion

- ## Summary of Findings:
    - The process of downloading and installing Splunk, clearing event viewer logs, and creating a dashboard demonstrates the power of centralized log management and security monitoring. By using Splunk, organizations can gain valuable insights into their security posture and detect potential threats. Clearing event viewer logs, while sometimes necessary, should be handled with care, ensuring that logs are backed up and access is restricted. Splunk dashboards allow for the quick analysis of large quantities of security related data.
- ## Next Steps:
    - Immediate actions should focus on securing Splunk access and ensuring log integrity. Long-term actions should involve implementing comprehensive log collection, creating effective dashboards and alerts, and integrating Splunk with other security tools. Continuous monitoring and regular security audits are essential for maintaining a strong security posture.