**Splunk Internship Task Report**

**1. Introduction**

This report documents the steps performed during the Splunk internship task as part of the Future Interns Program. The objective of this task was to ingest log data into Splunk, configure the data source, and then perform searches to identify potential security threats. Splunk is a powerful SIEM (Security Information and Event Management) tool that helps security analysts collect, index, and analyze machine-generated data for detecting anomalies and threats.

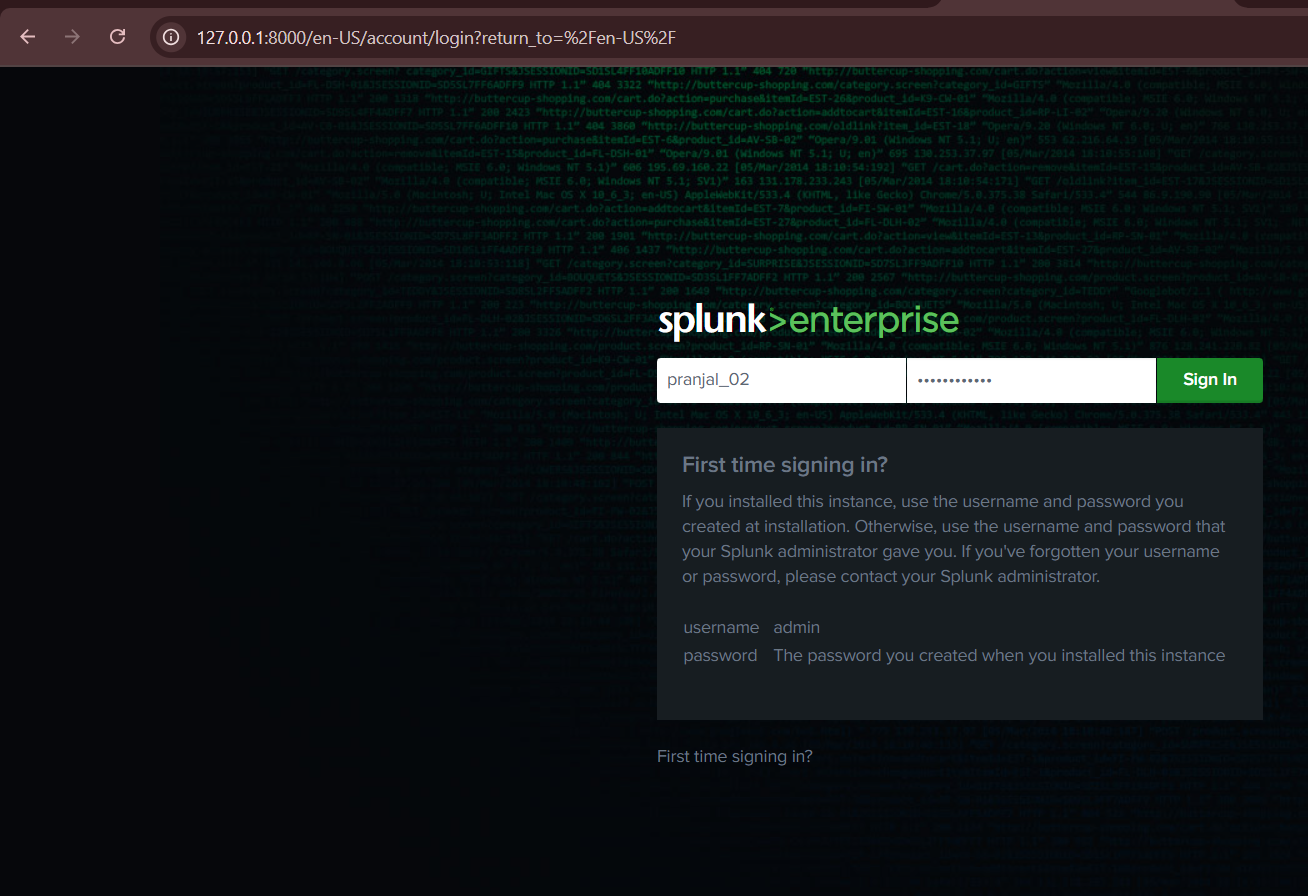
The task involved:

* Installing and logging into the Splunk Enterprise platform.
* Uploading a sample log file.
* Defining a source type and configuring input settings.
* Reviewing and indexing data.
* Executing a search query to detect malware-related events.

**2. Installation & Login**

Splunk Enterprise was installed and accessed locally on the system.

* **Website used for login:**
* http://127.0.0.1:8000
* The login page requires valid administrator credentials. Once authenticated, the user gains access to the Splunk Enterprise dashboard.



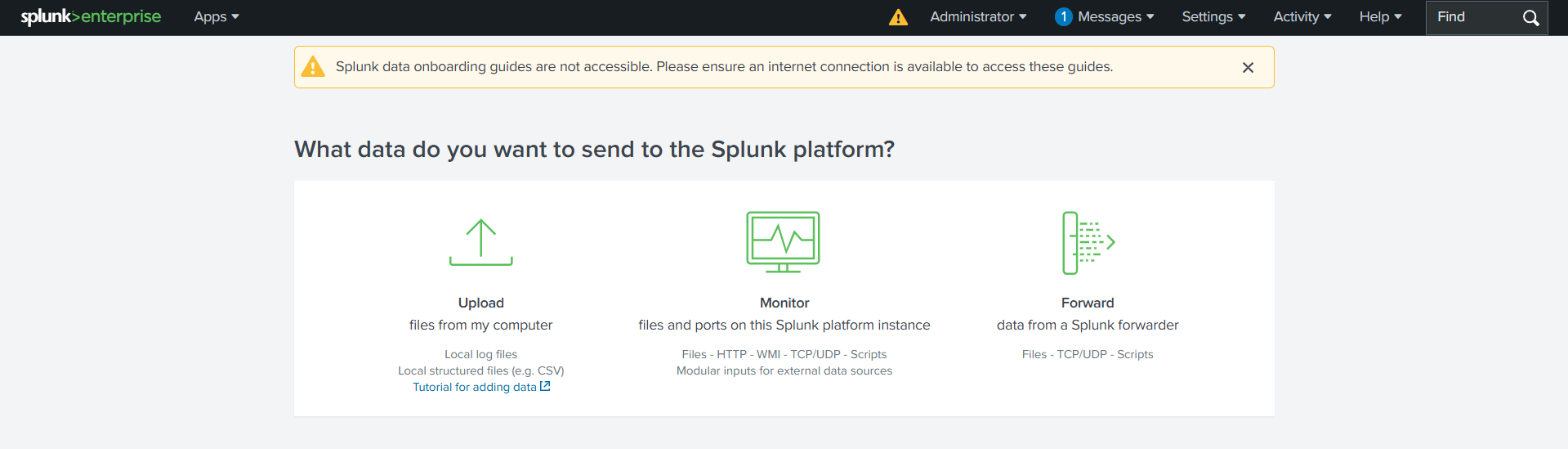
**3. Adding Data to Splunk**

**Step 1: Choosing Data Input Method**

After logging in, the “Add Data” section was used to upload logs. Splunk provides multiple options for data ingestion:

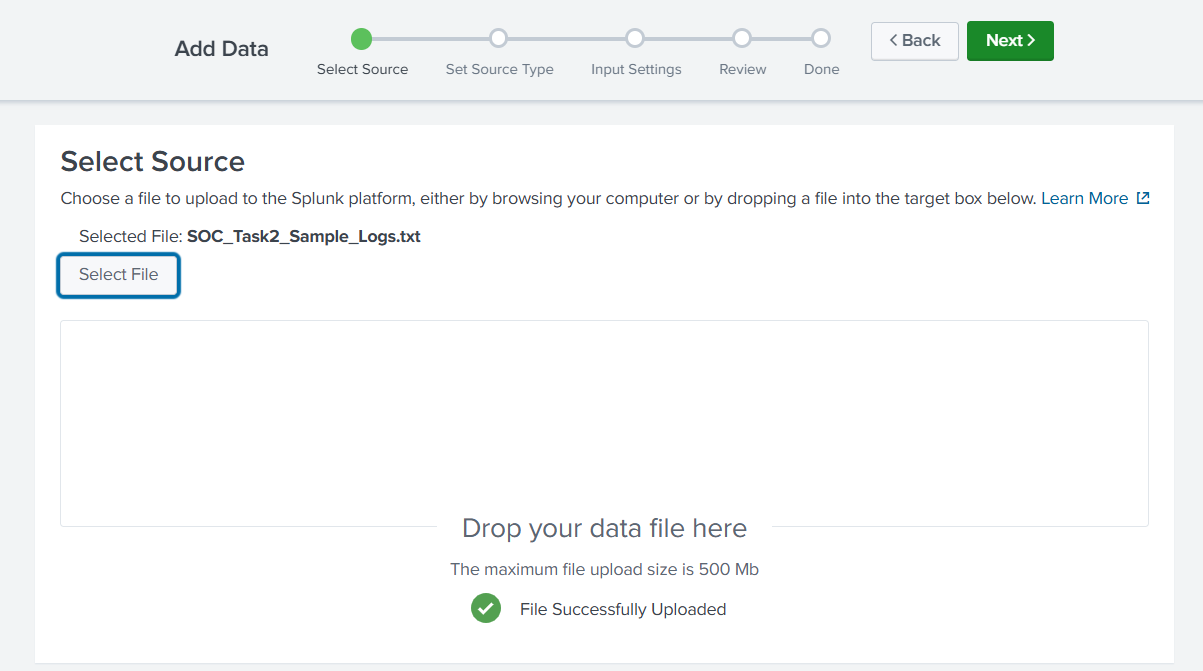
* **Upload:** Files directly from the computer.
* **Monitor:** Continuous monitoring of files, ports, or scripts.
* **Forward:** Data received from a Splunk forwarder.

For this task, the **Upload** option was selected to add a local log file.



**Step 2: Uploading the Log File**

A sample log file named **SOC\_Task2\_Sample\_Logs.txt** was uploaded successfully. The maximum supported upload size is 500 MB.

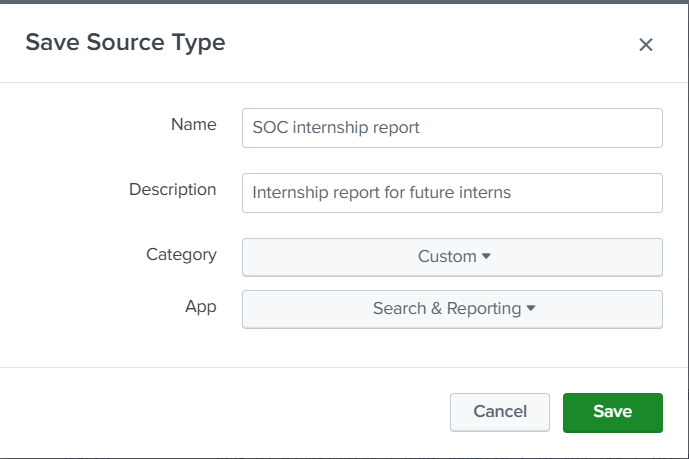


**Step 3: Setting Source Type**

Splunk automatically parsed the uploaded log file and displayed events in structured format. Each log entry contained fields such as **timestamp, user, IP address, action, and threat details**.

At this stage:

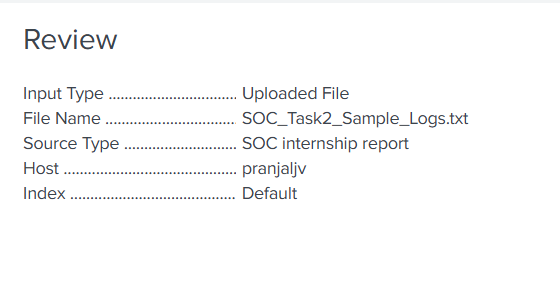
* The **Source Type** was set.
* Timestamps were verified to ensure accurate event indexing.
* Event breaks were properly identified to separate individual log entries.



**Step 4: Input Settings & Review**

In the **Input Settings** step:

* A suitable **source name** and **description** were provided (e.g., “SOC internship logs”).
* The default input settings were kept unchanged.
* A final review screen summarized all configurations before indexing.



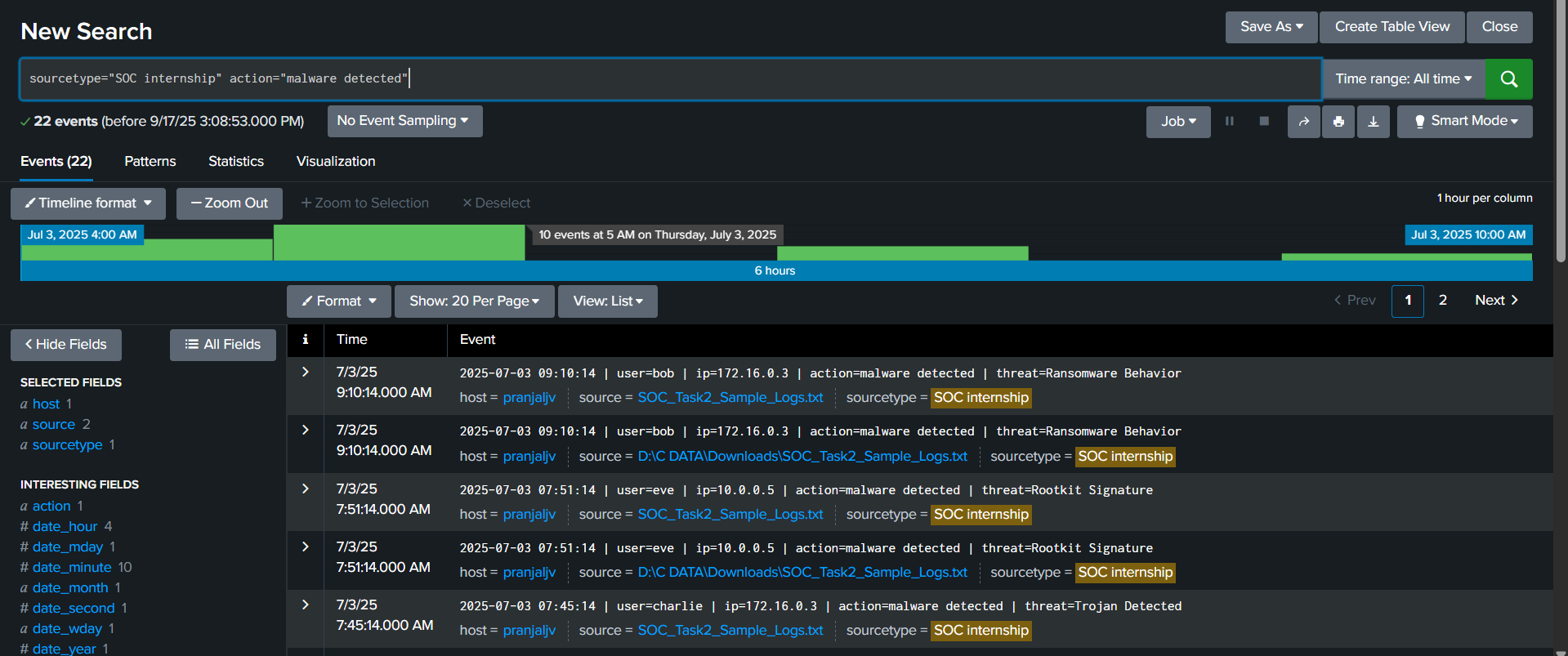
Once confirmed, the file was indexed successfully into Splunk.

**4. Searching the Logs**

After indexing, Splunk’s **Search & Reporting** app was used to query the logs. A filter was applied to detect malware events:

sourcetype="SOC internship" action="malware detected"

This search query ensured that only those events tagged as **malware detected** were retrieved, which is crucial for SOC (Security Operations Centre) monitoring and analysis.



**5. Findings**

The uploaded log file revealed multiple security-related events, including:

* **Connection Attempts** from different IP addresses.
* **Login Success/Failures** for various users.
* **File Accessed Events** indicating user activity.
* **Malware Detection Alerts**, where the logs flagged **Trojan threats**.

These findings highlight how Splunk helps identify suspicious activities and potential compromises in a network environment.

**6. Conclusion**

The task successfully demonstrated the process of ingesting log data into Splunk, configuring sources, and running queries for threat detection. By applying the search filter, malware detection events were isolated and reviewed. This exercise shows the importance of Splunk in cybersecurity operations, especially for SOC teams who need real-time monitoring, investigation, and incident response.