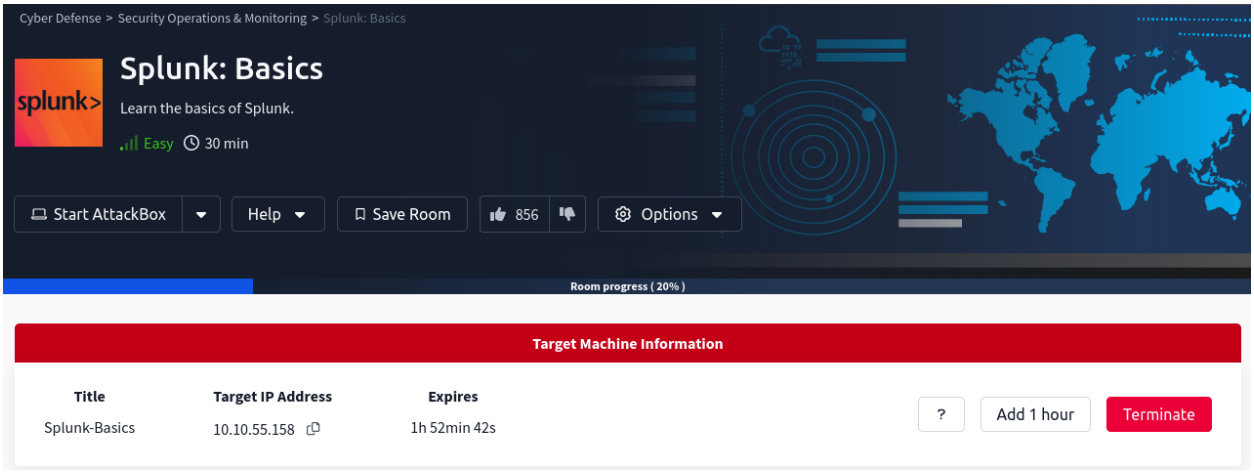
Splunk: Basics



Introduction

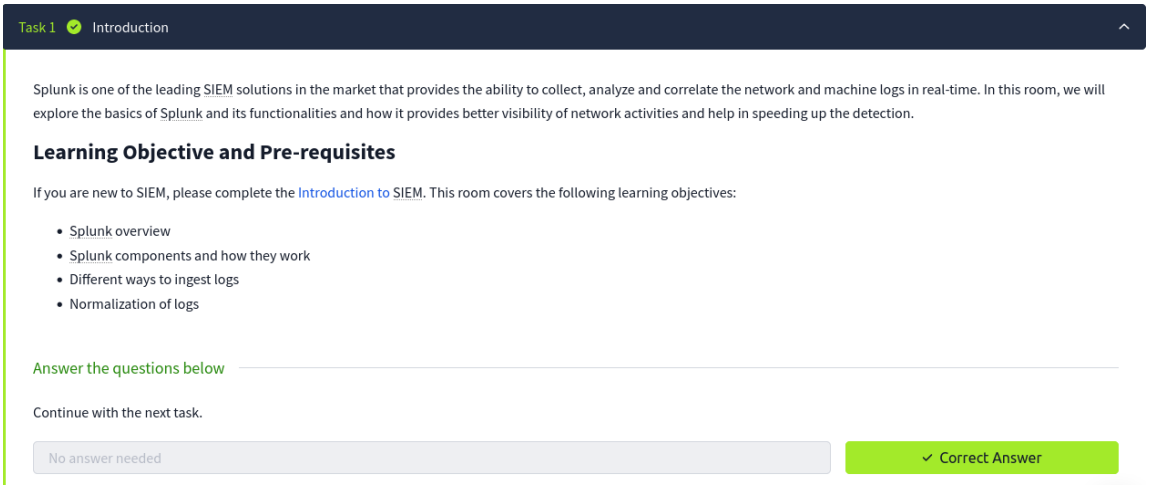
This repository showcases my work using Splunk to analyze and derive insights from event data. This project involves creating specific queries to filter and count events, helping to identify patterns and anomalies in the data. It demonstrates my ability to manipulate and extract valuable information from large datasets using Splunk.

Objectives

The primary objectives of this project were to:

1. Count the number of events originating from all countries except France.
2. Determine the number of VPN events observed by a specific IP address.

Task 1: Introduction



Task 2: Connect with the Lab

Task 2 Connect with the Lab

Room Machine

Start Machine

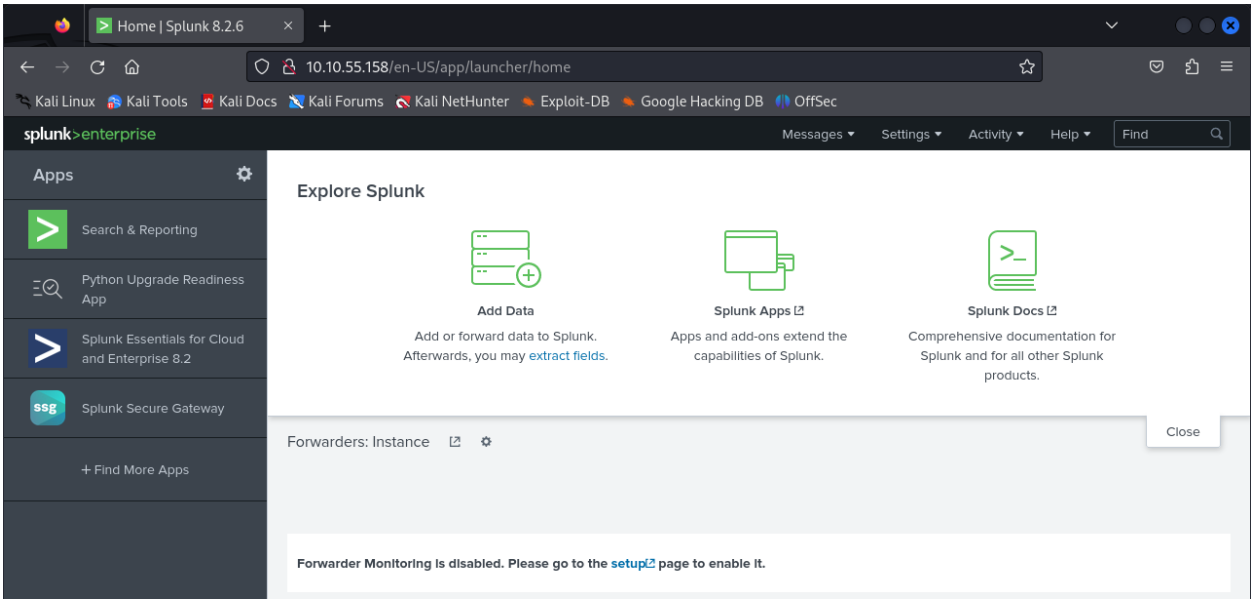
Before moving forward, deploy the machine. When you deploy the machine, it will be assigned an IP. Access this room in a web browser on the AttackBox, or via the VPN at `http://10.10.55.158`. The machine will take up to 3-5 minutes to start.

Answer the questions below

Connect with the lab.

No answer needed

✓ Correct Answer



Task 3: Splunk Components

Task 3 Splunk Components

Splunk has three main components, namely Forwarder, Indexer, and Search Head. These components are explained below:

Answer the questions below

Which component is used to collect and send data over the Splunk instance?

Forwarder

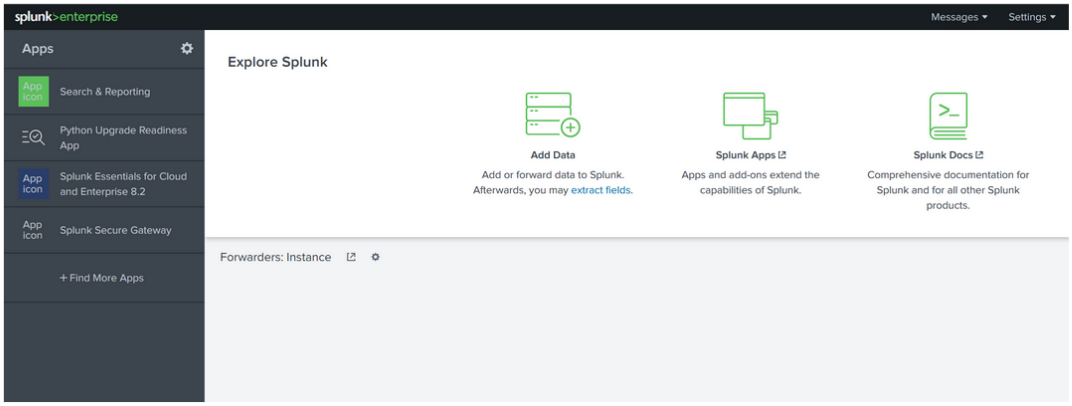
✓ Correct Answer

Task 4: Navigating Splunk

Task 4 ✓ Navigating Splunk

Splunk Bar

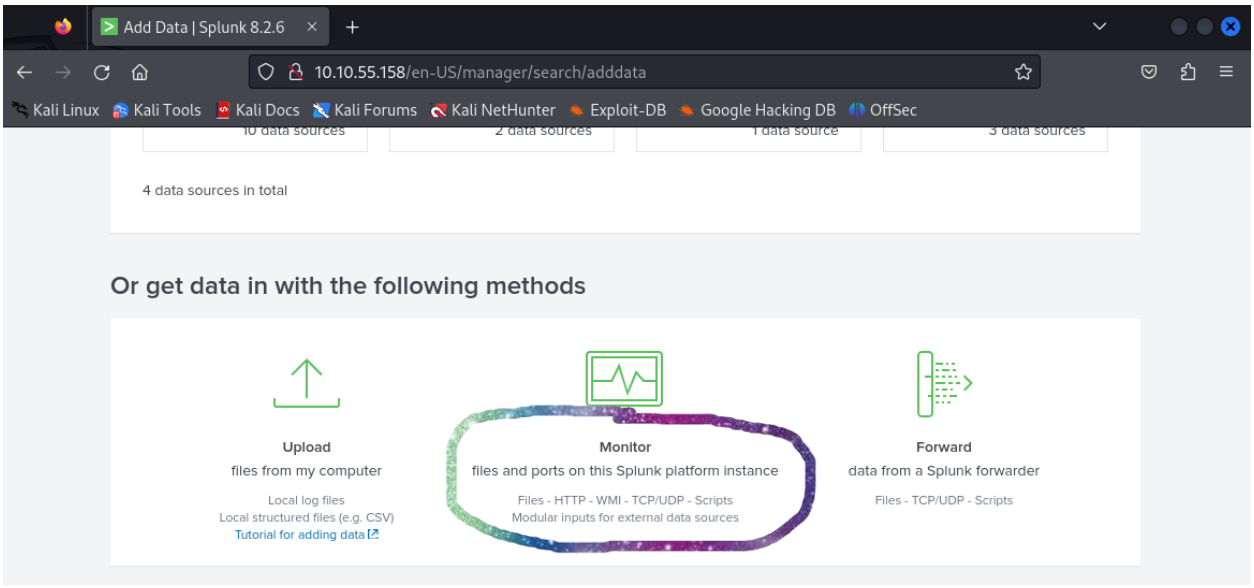
When you access Splunk, you will see the default home screen identical to the screenshot below.



Answer the questions below

In the Add Data tab, which option is used to collect data from files and ports?

Monitor ✓ Correct Answer Hint



Task 5: Adding Data

Task 5 Adding Data

Splunk can ingest any data. As per the Splunk documentation, when data is added to Splunk, the data is processed and transformed into a series of individual events.

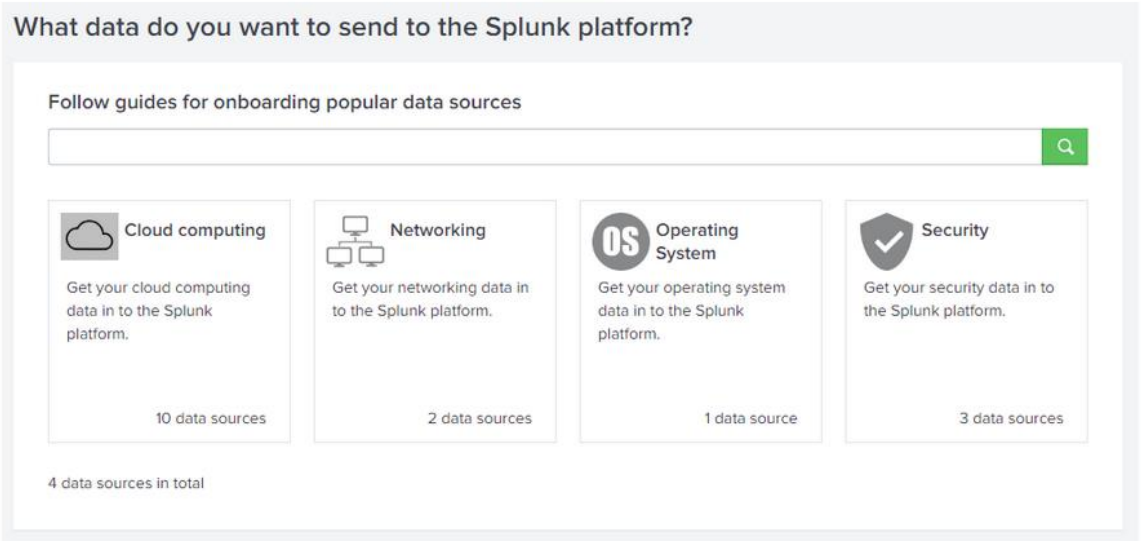
Download Task Files

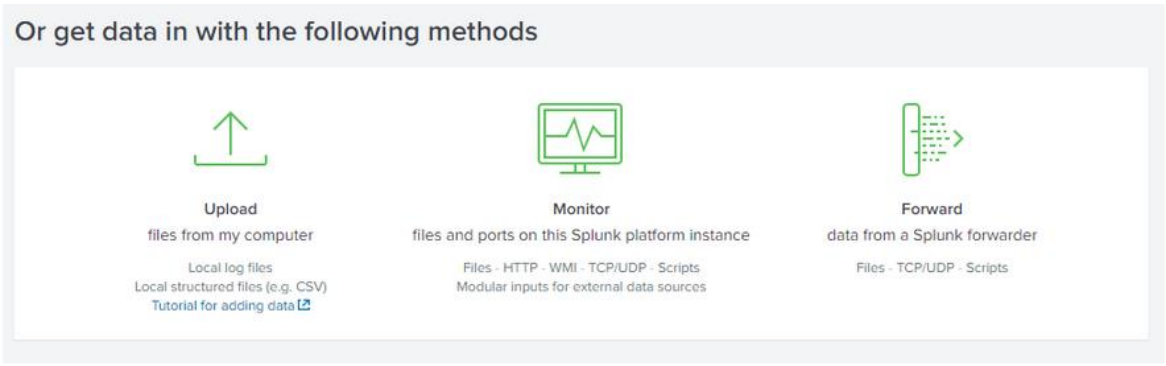
The data sources can be event logs, website logs, firewall logs, etc.

Data sources are grouped into categories. Below is a chart listing from the Splunk documentation detailing each data source category.

Data source	Description
Files and directories	Most data that you might be interested in comes directly from files and directories.
Network events	The Splunk software can index remote data from any network port and SNMP events from remote devices.
IT Operations	Data from IT Ops, such as Nagios, NetApp, and Cisco.
Cloud services	Data from Cloud services, such as AWS and Kinesis.
Database services	Data from databases such as Oracle, MySQL, and Microsoft SQL Server.
Security services	Data from security services such as McAfee, Microsoft Active Directory, and Symantec Endpoint Protection.
Virtualization services	Data from virtualization services such as VMWare and XenApp.
Application servers	Data from application servers such as JMX & JMS, WebLogic, and WebSphere.
Windows sources	The Windows version of Splunk software accepts a wide range of Windows-specific inputs, including Windows Event Log, Windows Registry, WMI, Active Directory, and Performance monitoring.
Other sources	Other input sources are supported, such as FIFO queues and scripted inputs for getting data from APIs, and other remote data interfaces.

In this room, we're going to focus on **VPN logs**. When we click on the `Add Data` link (from the Splunk home screen), we're presented with the following screen.



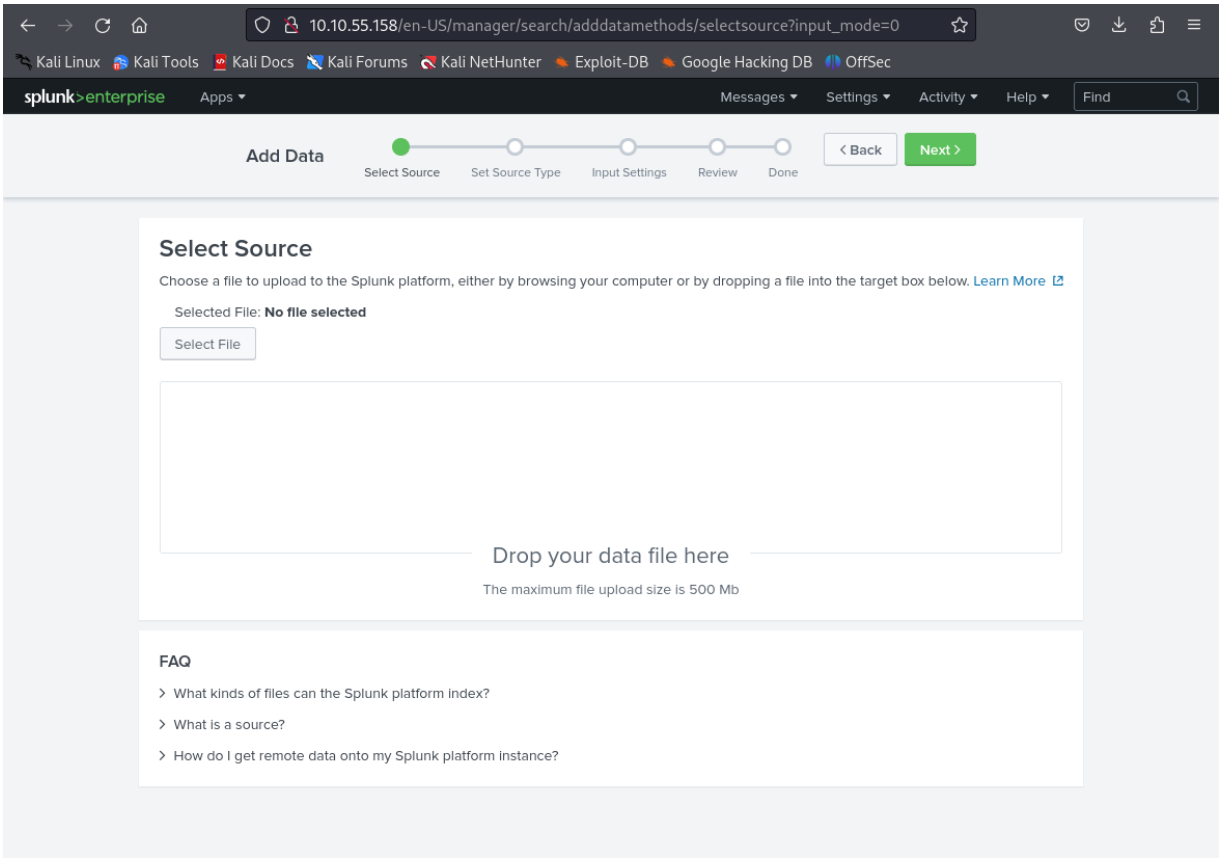


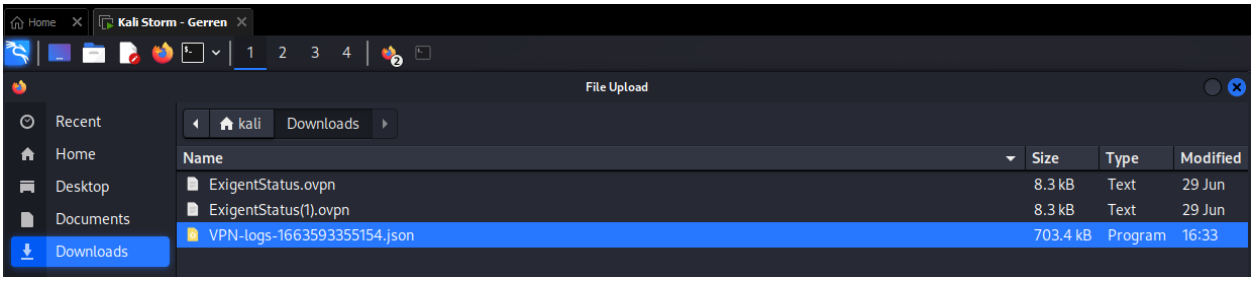
We will use the Upload Option to upload the data from our local machine. Download the attached log file and upload it on Splunk.

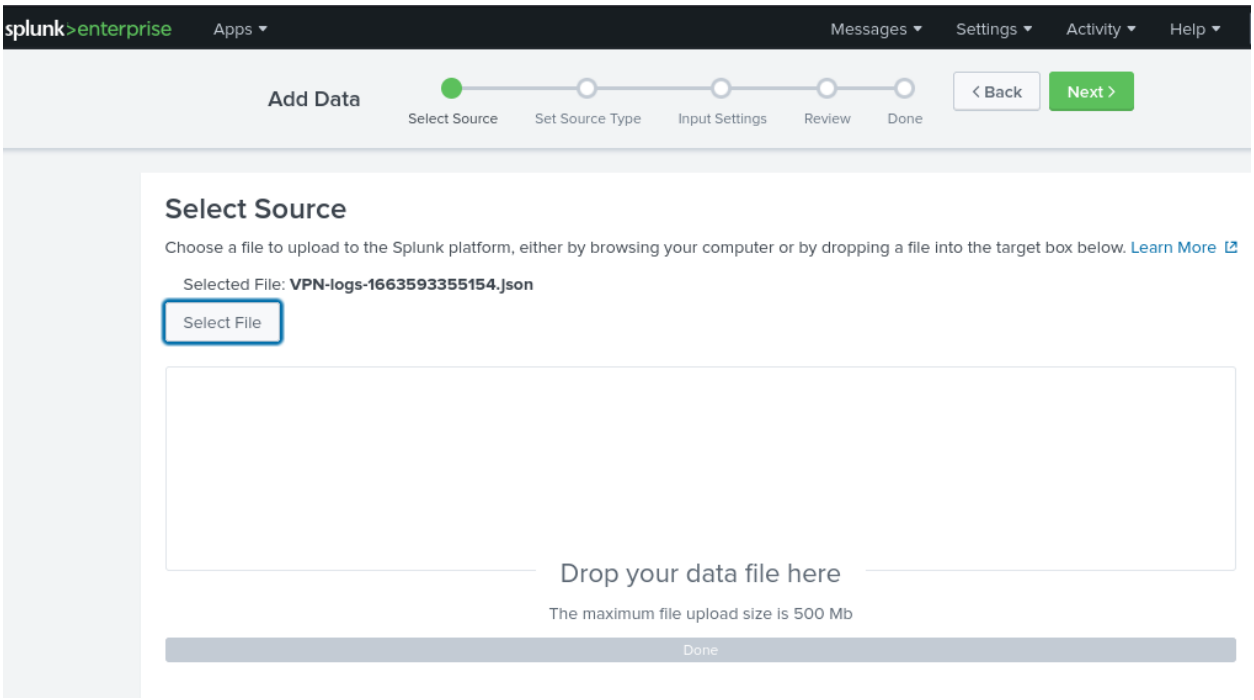
As shown above, it has a total of 5 steps to successfully upload the data.

1. **Select Source** -> Where we select the Log source.
2. **Select Source Type** -> Select what type of logs are being ingested.
3. **Input Settings** ->Select the index where these logs will be dumped and hostName to be associated with the logs.
4. **Review** -> Review all the gif
5. **Done** -> Final step, where the data is uploaded successfully and ready to be analyzed.

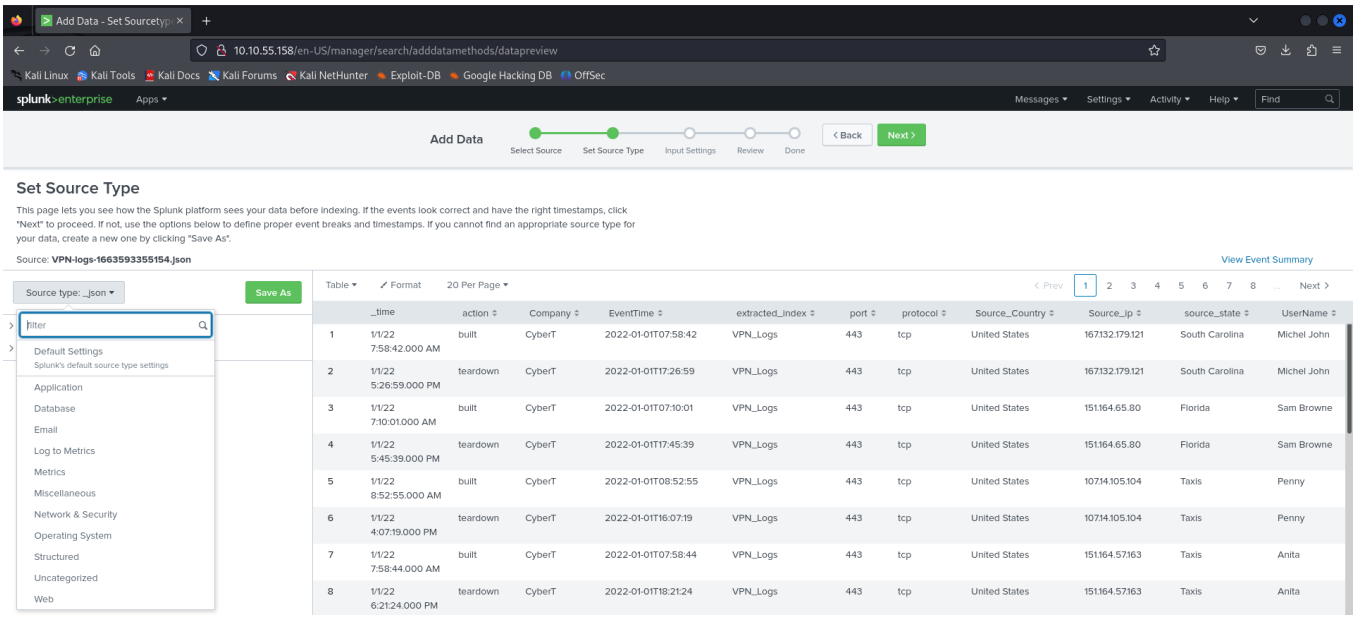
Step 1. Select Source



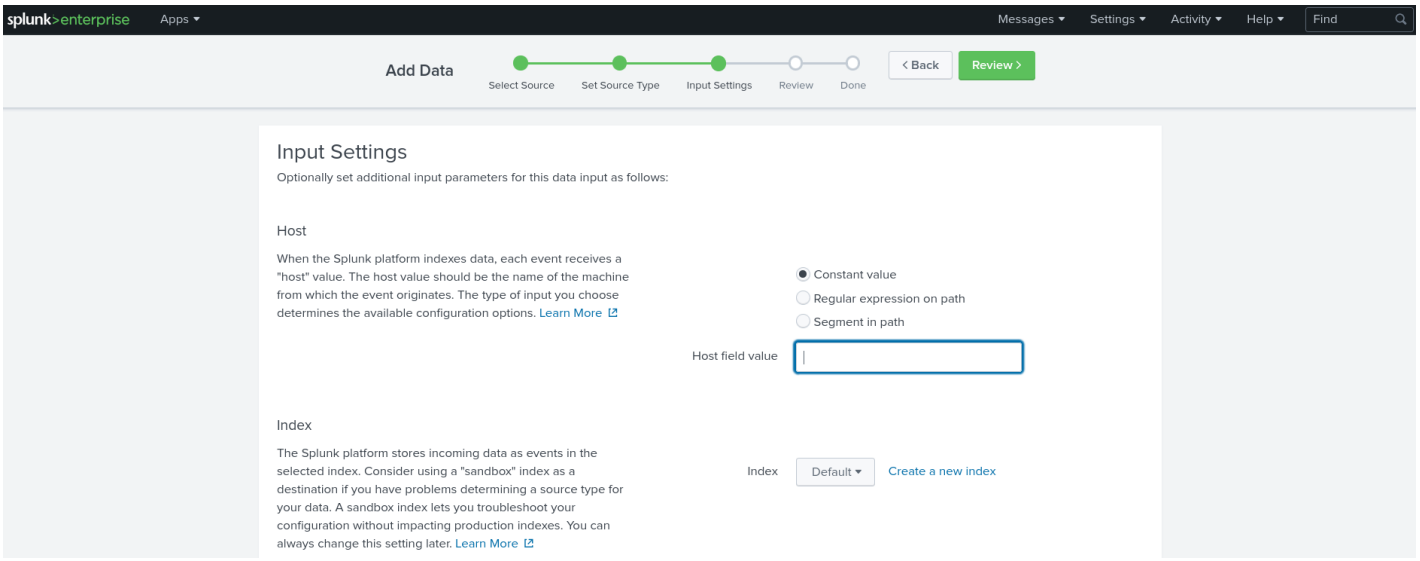


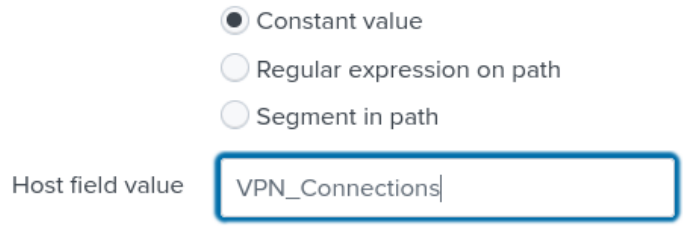


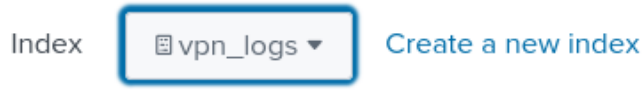
Step 2. Set Source Type

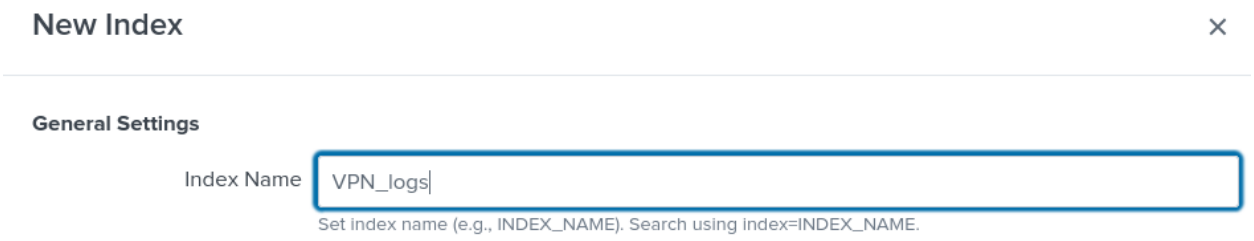


Step 3. Input Settings

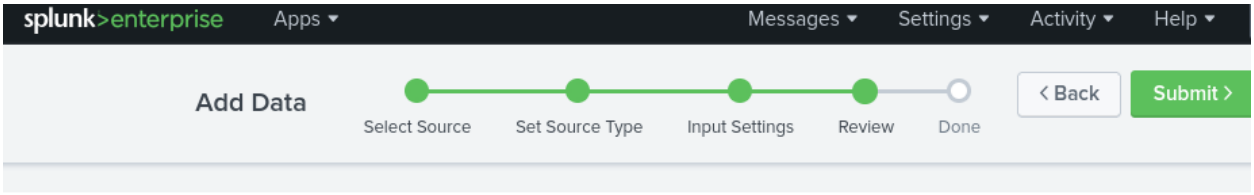








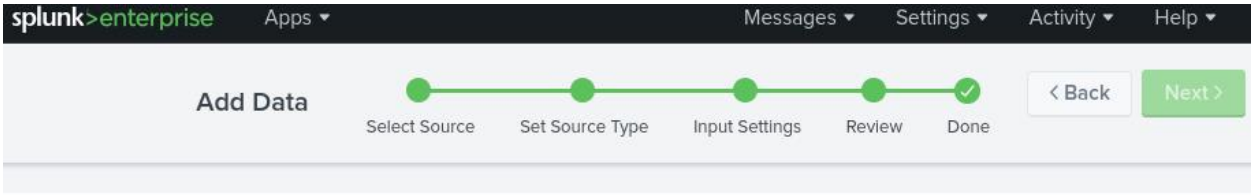
Step 4. Review



Review

Input Type ..... Uploaded File
File Name VPN-logs-1663593355154.json
Source Type ..... _json
Host ..... VPN_Connections
Index ..... vpn_logs

Step 5. File has been uploaded successfully



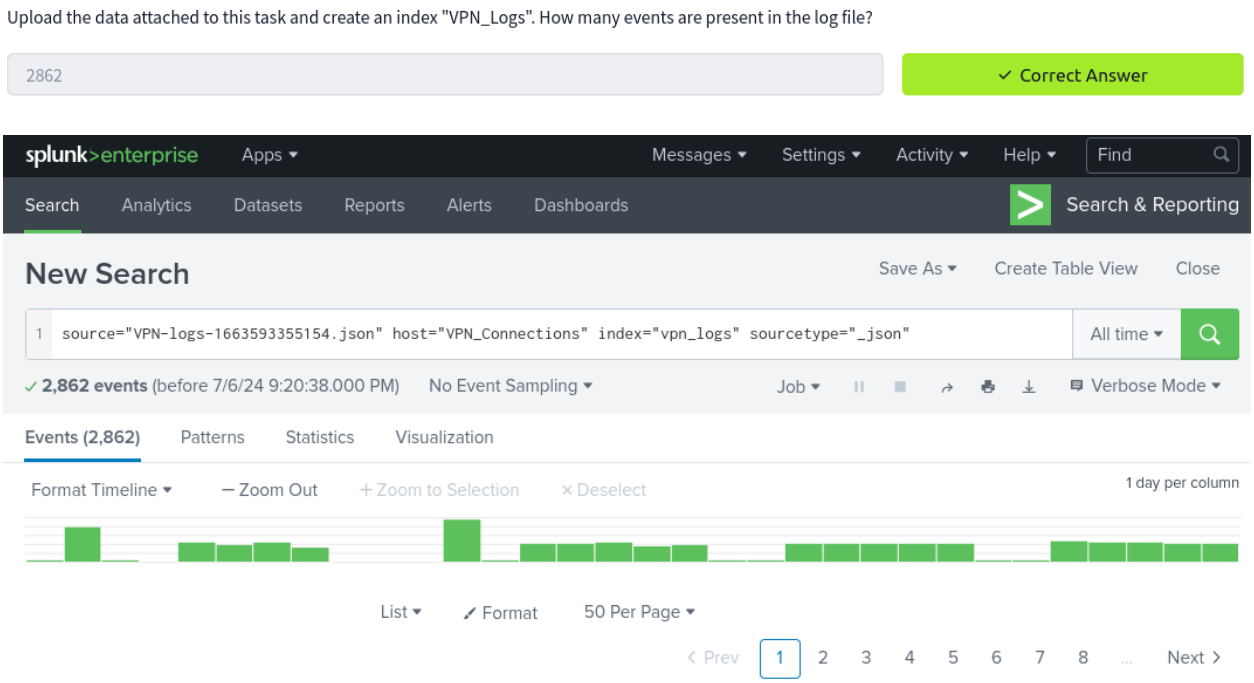
File has been uploaded successfully.

Configure your inputs by going to Settings > Data Inputs

Start Searching	Search your data now or see examples and tutorials.
Extract Fields	Create search-time field extractions. Learn more about fields.
Add More Data	Add more data inputs now or see examples and tutorials.
Download Apps	Apps help you do more with your data. Learn more.
Build Dashboards	Visualize your searches. Learn more.

Review Questions

1.



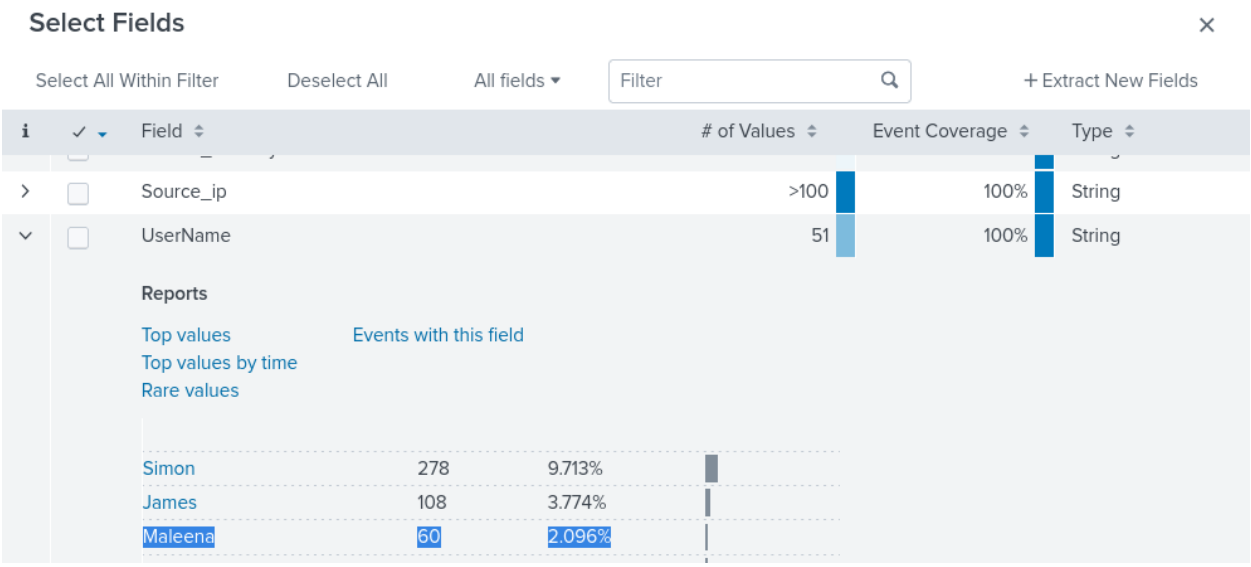
Splunk Search Query Breakdown:

1. **source ="VPN-logs-168539355154.json"**
   - This part of the query specifies the source file for the events. In this case, it is a JSON file named VPN-logs-168539355154.json.
2. **host ="VPN_Connections":**
   - This filter restricts the search to events from a specific host named VPN_Connections. The host can represent the machine or system that generated the log data.
3. **Index ="vpn_logs":**
   - This specifies the index where the data is stored. In Splunk, an index is a repository for data, and vpn_logs are the names of the index containing VPN connection logs.
4. **sourcetype ="_json":**
   - This indicates the type of data being searched, which in this case is JSON format. Sourcetype helps Splunk understand how to parse the incoming data.

2.

How many log events by the user **Maleena** are captured?

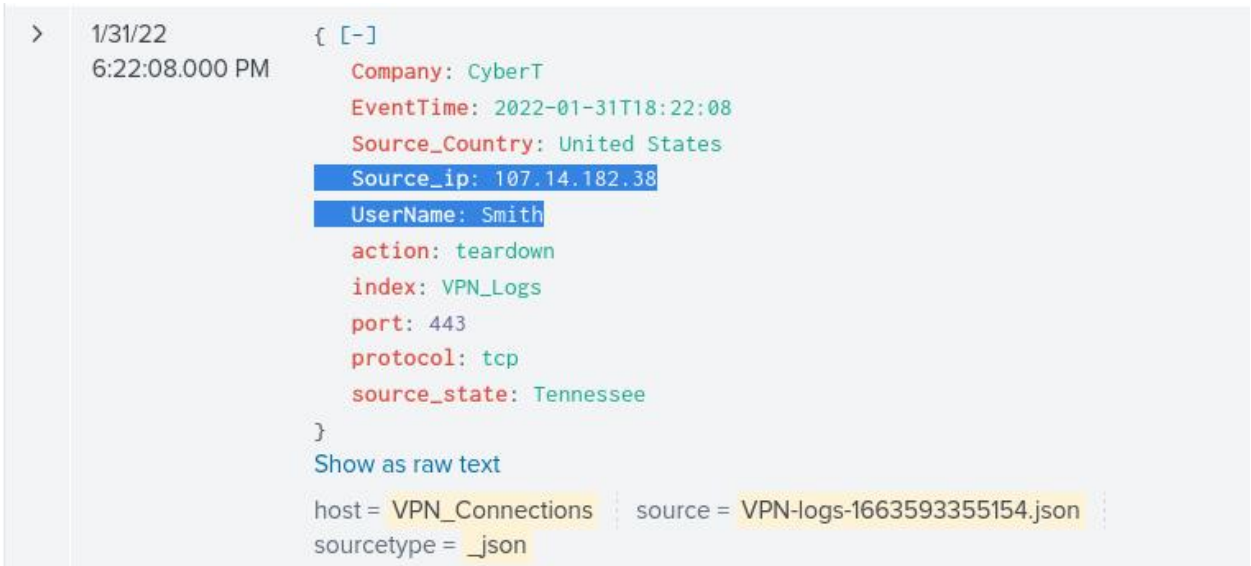
60 ✓ Correct Answer



3.

What is the name associated with IP 107.14.182.38?

Smith ✓ Correct Answer

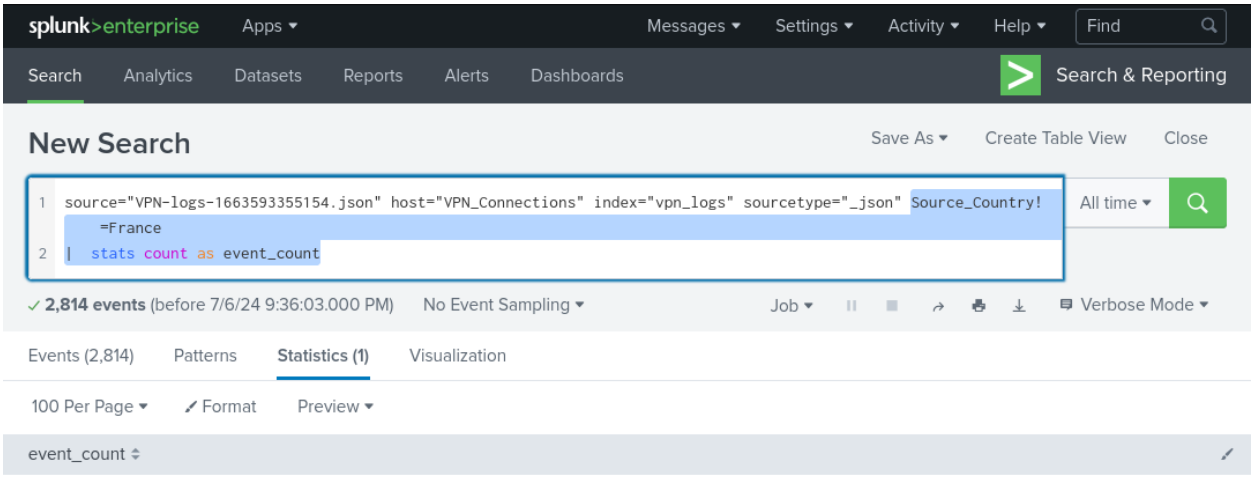


4.

What is the number of events that originated from all countries except France?

2814 ✓ Correct Answer

Source_Country!=France | stats count as event_count

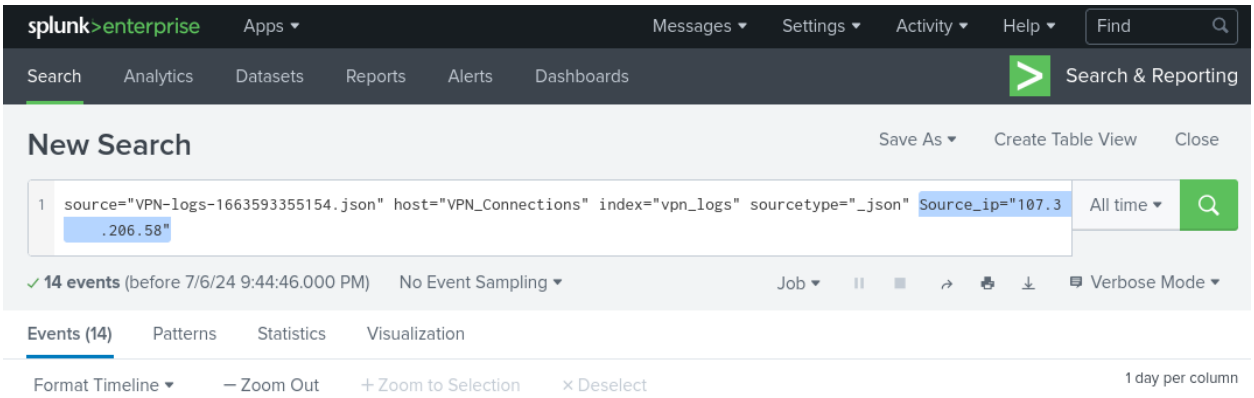


5.

How many VPN Events were observed by the IP 107.3.206.58?

14 ✓ Correct Answer

Source_ip="107.3.206.58"



Reflection

Working on this Splunk project has enhanced my skills in data manipulation and event analysis. Understanding how to filter and count events based on various criteria is essential for cybersecurity and IT operations. This project highlights my proficiency in using Splunk to gain valuable insights from data and improve overall system security.