Learn the following:

- Splunk components
- Navigating Splunk Interface
- Uploading data (adding data) to Splunk (VPN logs)
- Basic search commands

Splunk: The Basics

Understand how SOC analysts use Splunk for log investigations.

Task 1 Introduction

Splunk is one of the leading SIEM solutions in the market. It allows users to collect, analyze, and correlate network and machine logs in real time. In this room, we will explore the basics of Splunk and its functionalities, and how it provides better visibility of network activities and helps speed up detection.

Learning Objectives

This room covers the following learning objectives:

- Understanding the components of Splunk
- Exploring some available options in Splunk
- Understanding log ingestion in Splunk
- Practically ingesting some Logs in Splunk and analyzing them

Room Prerequisites

If you are new to SIEM, please complete the Introduction to SIEM room.

Answer the questions below

No answer needed

Task 2 Connect with the Lab

Before proceeding with the following tasks, start the attached virtual machine by clicking the **Start Machine** below.

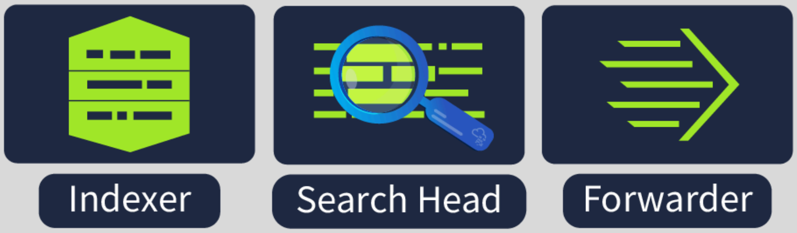
The machine may take up to 3-5 minutes to start. After the machine starts, the Splunk Instance can be accessed at `http://10.66.171.93` either directly on the AttackBox or via the TryHackMe VPN.

Answer the questions below

No answer needed

Task 3 Splunk Components

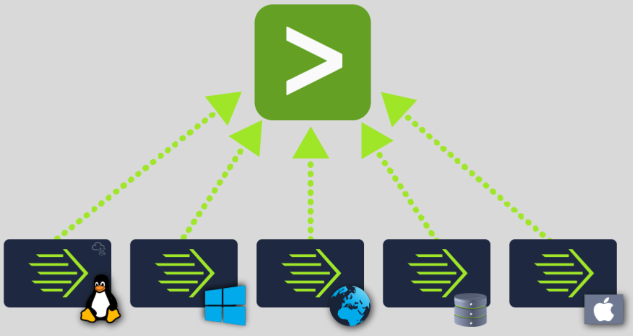
Splunk has three main components: Forwarder, Indexer, and Search Head. These components work together to help us search and analyze the data. These components are explained below:



Splunk Forwarder

Splunk Forwarder is a lightweight agent installed on the endpoint intended to be monitored, and its main task is to collect the data and send it to the Splunk instance. It does not affect the endpoint's performance as it takes a few resources to process. Some of the key data sources are:

- Web server generating web traffic.
- Windows machine generating Windows Event Logs, PowerShell, and Sysmon data.
- Linux host generating host-centric logs.
- Database generating DB connection requests, responses, and errors.



The forwarder collects the data from the log sources and sends it to the Splunk Indexer.

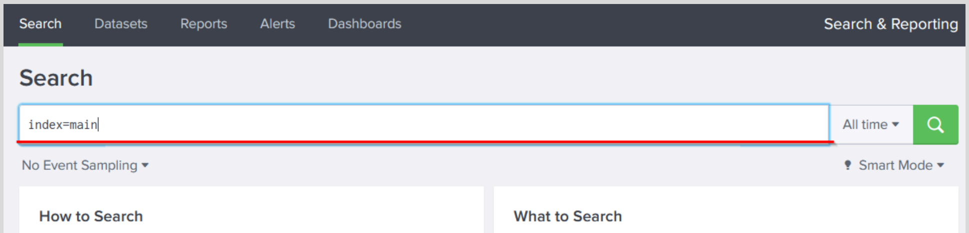
Splunk Indexer

Splunk Indexer plays the main role in processing the data it receives from forwarders. It parses and normalizes the data into field-value pairs, categorizes it, and stores the results as events, making the processed data easy to search and analyze.

Now, the data, which is normalized and stored by the indexer, can be searched by the Search Head, as explained below.

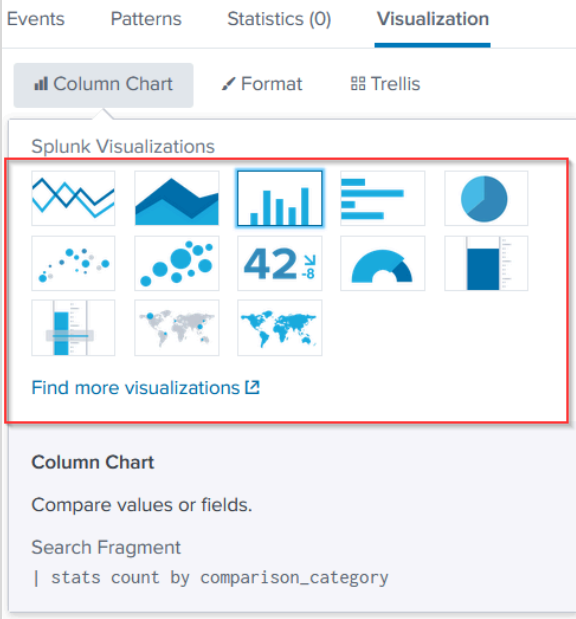
Search Head

Splunk Search Head is the place within the Search & Reporting App where users can search the indexed logs, as shown below. The searches are done using the SPL (Search Processing Language), a powerful query language for searching indexed data. When the user performs a search, the request is sent to the indexer, and the relevant events are returned as field-value pairs.



```
index=main
```

The Search Head also allows you to transform results into presentable tables and visualizations such as pie, bar, and column charts, as shown below:



Column Chart

Compare values or fields.

Search Fragment

```
| stats count by comparison_category
```

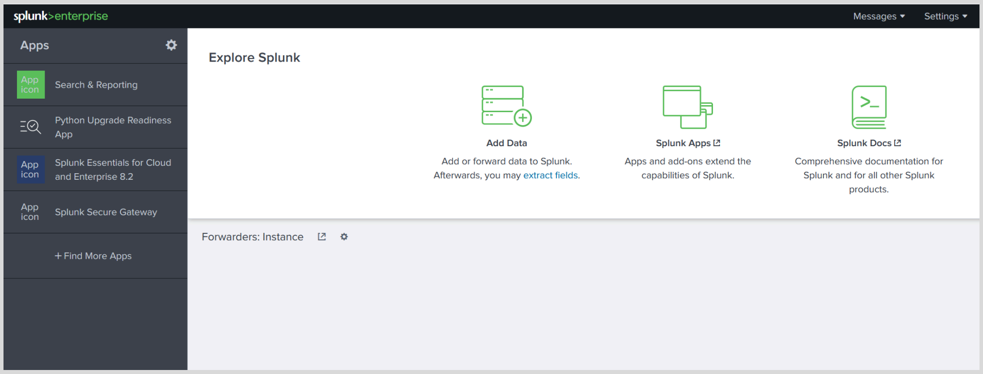
Answer the questions below

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

Forwarder

Task 4 Navigating Splunk

When you access Splunk, you will see the default **home screen** as shown below:



Add or forward data to Splunk. Afterwards, you may extract fields.

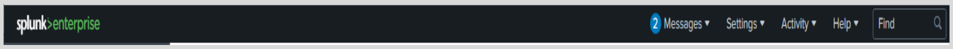
Apps and add-ons extend the capabilities of Splunk.

Comprehensive documentation for Splunk and for all other Splunk products.

Let's look at each section of this home screen.

Splunk Bar

The top panel is the **Splunk Bar** as shown below:



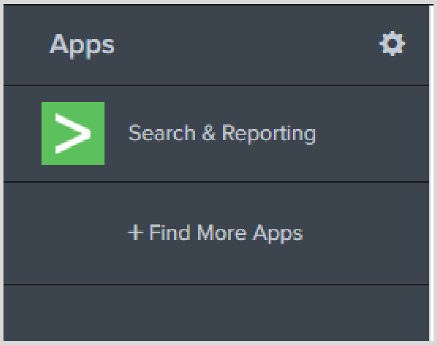
In the Splunk Bar, we have the following options available:

- **Messages:** View system-level notifications and messages.
- **Settings:** Configure Splunk instance settings.
- **Activity:** Review the progress of search jobs and processes.
- **Help:** View tutorials and documentation.
- **Find:** Search across the App.

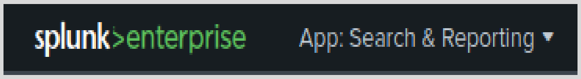
The Splunk Bar, allows users to switch between installed Splunk apps instead of using the Apps panel.

Apps Panel

Next is the **Apps Panel**. This panel shows the apps installed for the Splunk instance. The default app for every Splunk installation is **Search & Reporting**.

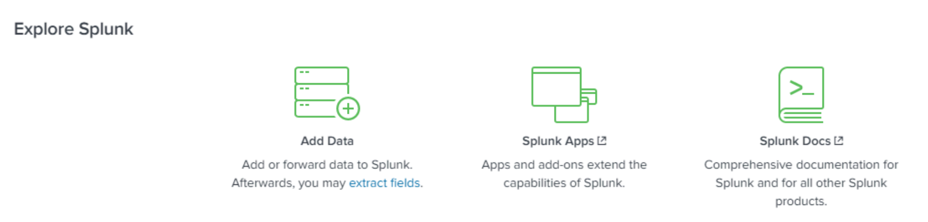


You can also switch between the Splunk Apps directly from the Splunk Bar, as shown below, without using the Apps Panel.



Explore Splunk

The next section is **Explore Splunk** . This panel contains quick links to add data to the Splunk instance, add new Splunk apps, and access the Splunk documentation.



Explore Splunk

Add Data

Add or forward data to Splunk. Afterwards, you may extract fields.

Splunk Apps

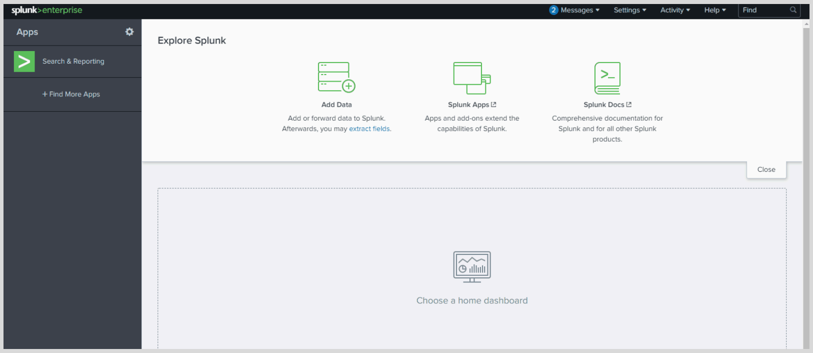
Apps and add-ons extend the capabilities of Splunk.

Splunk Docs

Comprehensive documentation for Splunk and for all other Splunk products.

Splunk Dashboard

The last section is the **Home Dashboard**. By default, no dashboards are displayed. You can choose from a range of dashboards readily available within your Splunk instance. You can select a dashboard from the dropdown menu or by visiting the **dashboards listing page**.



Explore Splunk

Add Data

Add or forward data to Splunk. Afterwards, you may extract fields.

Splunk Apps

Apps and add-ons extend the capabilities of Splunk.

Splunk Docs

Comprehensive documentation for Splunk and for all other Splunk products.

Choose a home dashboard

You can also create dashboards and add them to the Home Dashboard. The dashboards you create can be viewed separately from the other dashboards by clicking on the **Yours** tab.

Please review the Splunk documentation on Navigating Splunk here.

Answer the questions below

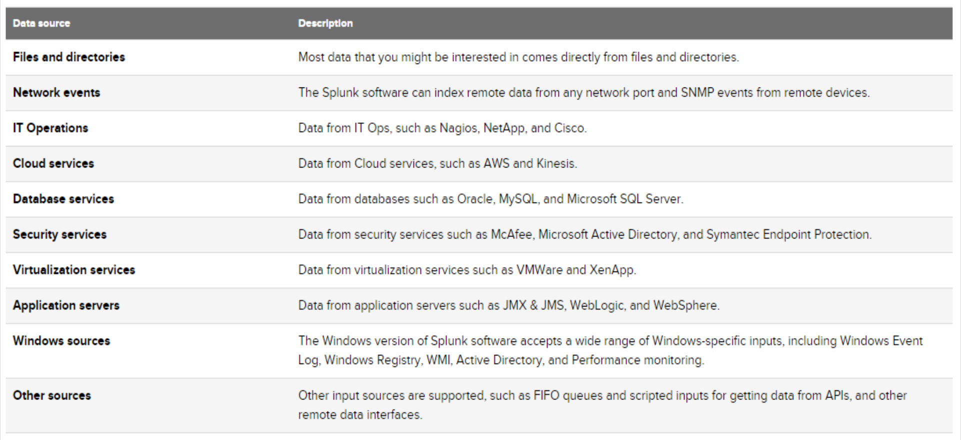
In the Add Data tab, which option is used to collect data from files and ports?

Monitor

Task 5 Adding Data

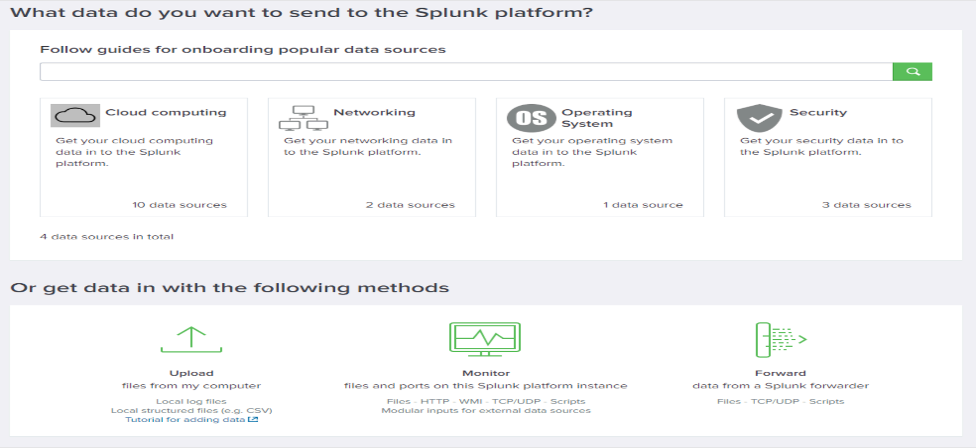
Splunk can ingest any data. According to the Splunk documentation, when data is added to Splunk, the data is processed and transformed into a series of individual events. The data sources can be event logs, website logs, firewall logs, etc. The data sources are grouped into categories.

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 task, we're going to focus on **VPN logs**. We're presented with the following screen when we click on the `Add Data` link on the Splunk home screen.



What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources

Cloud computing
Get your cloud computing data in to the Splunk platform.
10 data sources

Networking
Get your networking data in to the Splunk platform.
2 data sources

Operating System
Get your operating system data in to the Splunk platform.
1 data source

Security
Get your security data in to the Splunk platform.
3 data sources

4 data sources in total

Or get data in with the following methods

Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

Monitor
files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

Forward
data from a Splunk forwarder
Files - TCP/UDP - Scripts

We will use the `Upload` Option to upload the data from our local machine.

Practical

Download the log file `VPN_logs` from the `Download Task Files` button below and upload it to the Splunk instance we started in Task #2. If you are using the AttackBox, the log file is available in the `/root/Rooms/SplunkBasic/`directory.

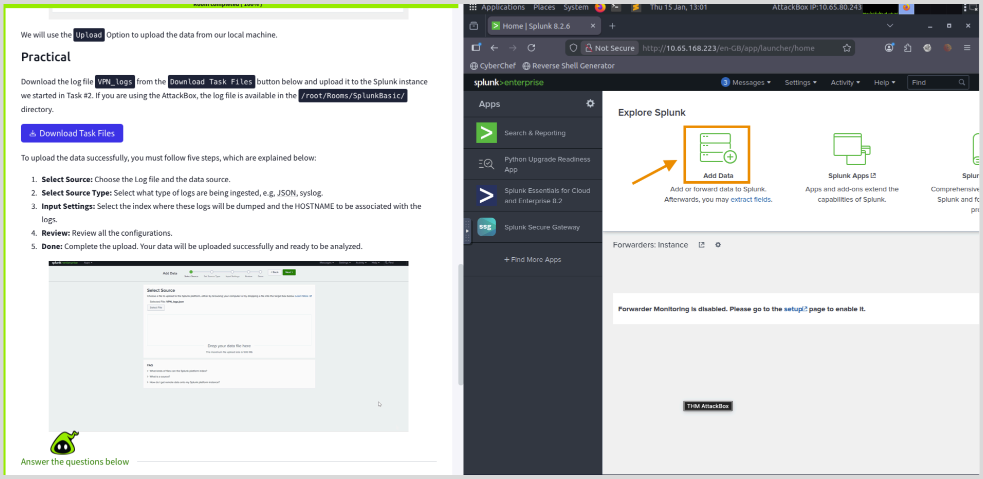
Download Task Files

To upload the data successfully, you must follow five steps, which are explained below:

1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Select Source File:

1. Click: Add Data



Room completed (100%)

We will use the `Upload` Option to upload the data from our local machine.

Practical

Download the log file `VPN_logs` from the `Download Task Files` button below and upload it to the Splunk instance we started in Task #2. If you are using the AttackBox, the log file is available in the `/root/Rooms/SplunkBasic/` directory.

Download Task Files

To upload the data successfully, you must follow five steps, which are explained below:

1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Answer the questions below

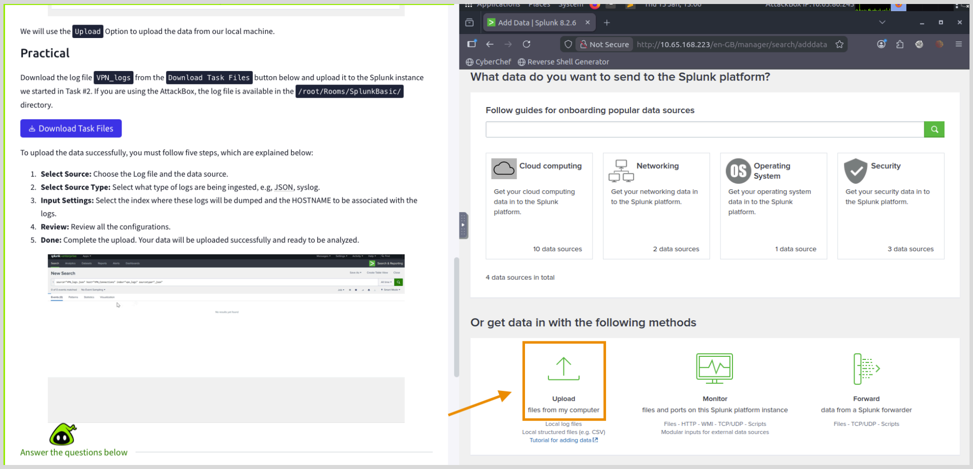
Add or forward data to Splunk. Afterwards, you may extract fields.

Apps and add-ons extend the capabilities of Splunk.

Forwarders: Instance

Forwarder Monitoring is disabled. Please go to the setup page to enable it.

2. Click: Upload



We will use the `Upload` Option to upload the data from our local machine.

Practical

Download the log file `VPN_logs` from the `Download Task Files` button below and upload it to the Splunk instance we started in Task #2. If you are using the AttackBox, the log file is available in the `/root/Rooms/SplunkBasic/` directory.

Download Task Files

To upload the data successfully, you must follow five steps, which are explained below:

1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Answer the questions below

What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources

Get your cloud computing data in to the Splunk platform. 10 data sources

Get your networking data in to the Splunk platform. 2 data sources

Get your operating system data in to the Splunk platform. 1 data source

Get your security data in to the Splunk platform. 3 data sources

4 data sources in total

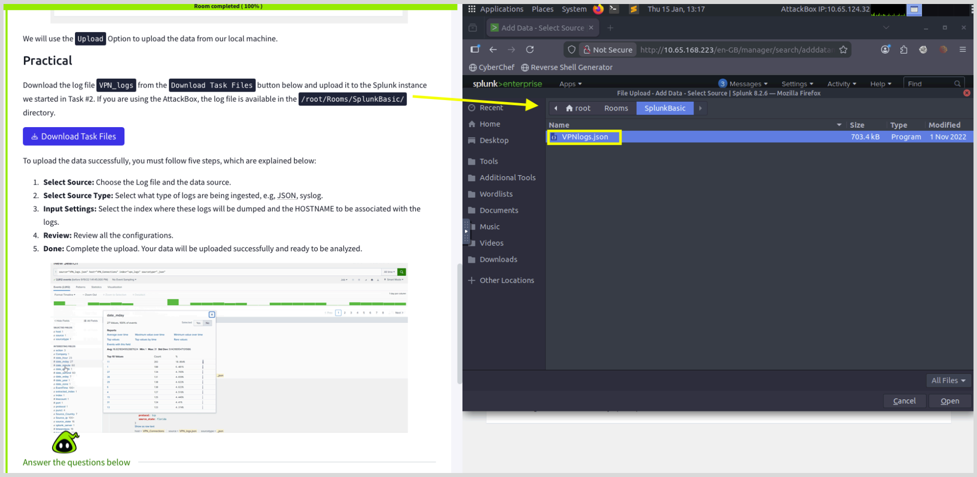
Or get data in with the following methods

files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

data from a Splunk forwarder
Files - TCP/UDP - Scripts

3. Navigate file to be uploaded: /root/Rooms/SplunkBasic/VPNlogs.json
4. Double Click: VPNlogs.json



Room completed (100%)

We will use the `Upload` Option to upload the data from our local machine.

Practical

Download the log file `VPN_logs` from the `Download Task Files` button below and upload it to the Splunk instance we started in Task #2. If you are using the AttackBox, the log file is available in the `/root/Rooms/SplunkBasic/` directory.

Download Task Files

To upload the data successfully, you must follow five steps, which are explained below:

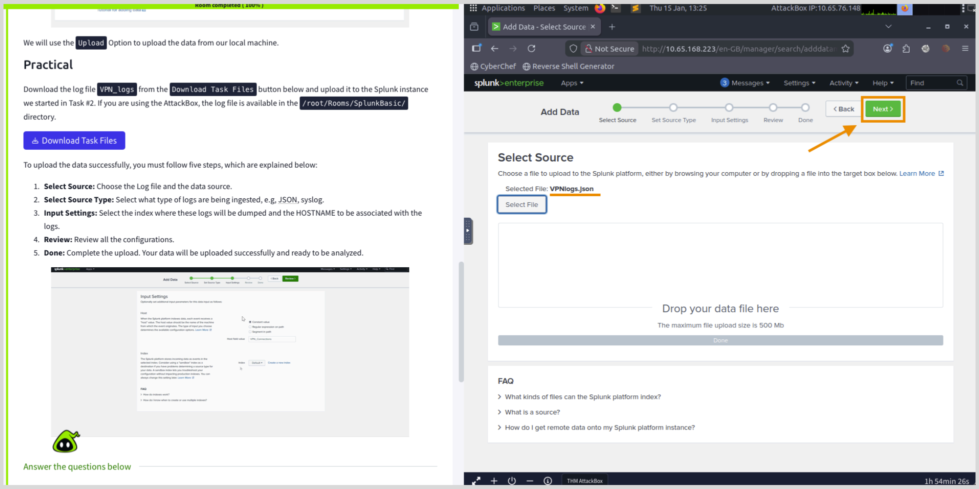
1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Answer the questions below

Name	Size	Type	Modified
VPNlogs.json	703.4 kB	Program	1 Nov 2022

Select Source Type:

1. Click: Next



Room completed (100%)

We will use the `Upload` Option to upload the data from our local machine.

Practical

Download the log file `VPN_logs` from the `Download Task Files` button below and upload it to the Splunk instance we started in Task #2. If you are using the AttackBox, the log file is available in the `/root/Rooms/SplunkBasic/` directory.

Download Task Files

To upload the data successfully, you must follow five steps, which are explained below:

1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Answer the questions below

Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

Selected File: VPNlogs.json

Drop your data file here

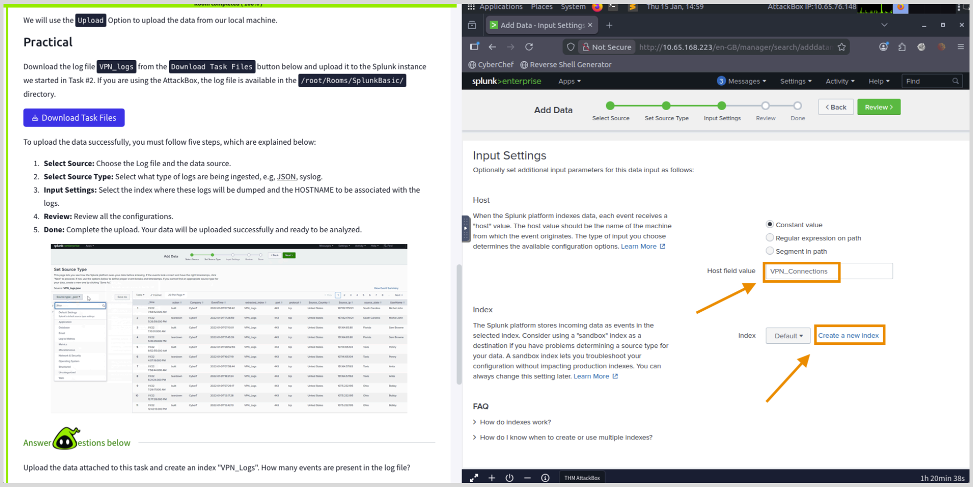
The maximum file upload size is 500 Mb

FAQ

- What kinds of files can the Splunk platform index?
- What is a source?
- How do I get remote data onto my Splunk platform instance?

Input Settings::

1. Enter in Host Field Value: “VPN_Connections”
2. Click: Create a new index (for the log dump)



We will use the `Upload` Option to upload the data from our local machine.

Practical

Download the log file `VPN_logs` from the `Download Task Files` button below and upload it to the Splunk instance we started in Task #2. If you are using the AttackBox, the log file is available in the `/root/Rooms/SplunkBasic/` directory.

Download Task Files

To upload the data successfully, you must follow five steps, which are explained below:

1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Answer estions below

Upload the data attached to this task and create an index "VPN_Logs". How many events are present in the log file?

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

● Constant value
○ Regular expression on path
○ Segment in path

Host field value: VPN_Connections

Index

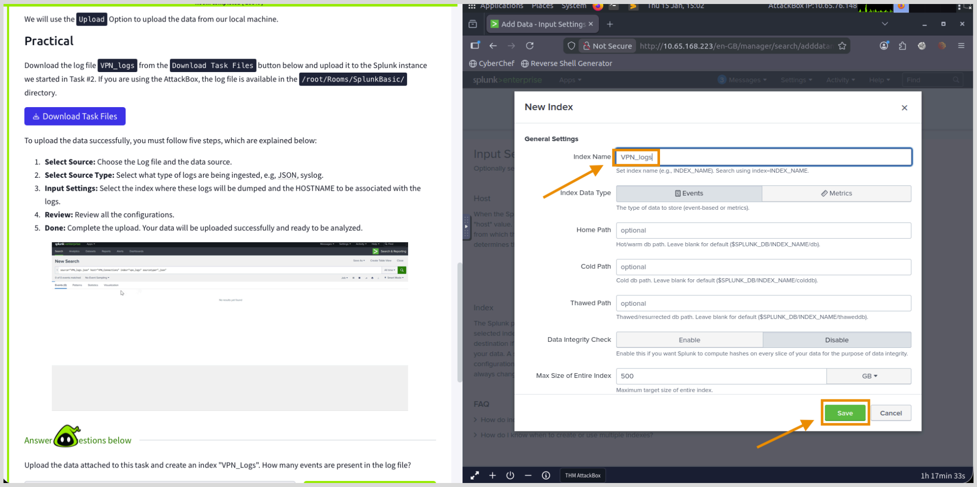
The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

Index: Default

FAQ

- How do indexes work?
- How do I know when to create or use multiple indexes?

3. Enter in Index Name field: VPN_logs
4. Click: Save



We will use the Upload Option to upload the data from our local machine.

Practical

Download the log file `VPN_logs` from the `Download Task Files` button below and upload it to the Splunk instance we started in Task #2. If you are using the AttackBox, the log file is available in the `/root/Rooms/SplunkBasic/` directory.

To upload the data successfully, you must follow five steps, which are explained below:

1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Upload the data attached to this task and create an index "VPN_Logs". How many events are present in the log file?

New Index

General Settings

Index Name: VPN_logs
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.

Index Data Type: Events / Metrics
The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/db).

Cold Path: optional
Cold db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/colddb).

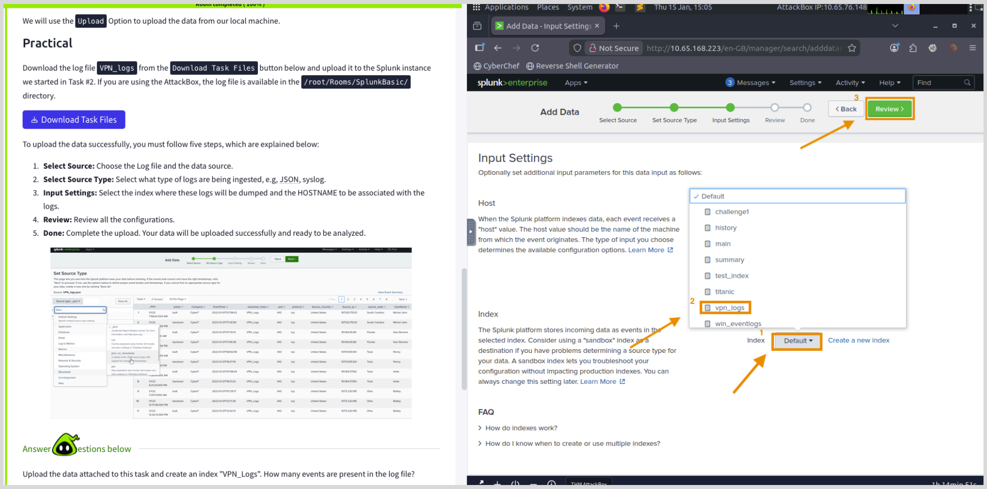
Thawed Path: optional
Thawed/resurrected db path. Leave blank for default ($SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable / Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB
Maximum target size of entire index.

Applications Places System Thu 15 Jan, 15:02 AttackBox IP:10.65.76.148
Add Data - Input Settings
Not Secure http://10.65.168.223/en-GB/manager/search/adddata
CyberChef
Reverse Shell Generator
Download Task Files
Answer the questions below
Save
Cancel
THM AttackBox
1h 17min 33s

5. Click: Index
6. Select: vpn_logs
7. Click: Review



We will use the Upload Option to upload the data from our local machine.

Practical

Download the log file `VPN_logs` from the `Download Task Files` button below and upload it to the Splunk instance we started in Task #2. If you are using the AttackBox, the log file is available in the `/root/Rooms/SplunkBasic/` directory.

To upload the data successfully, you must follow five steps, which are explained below:

1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Upload the data attached to this task and create an index "VPN_Logs". How many events are present in the log file?

Add Data: Select Source, Set Source Type, Input Settings, Review, Done

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More

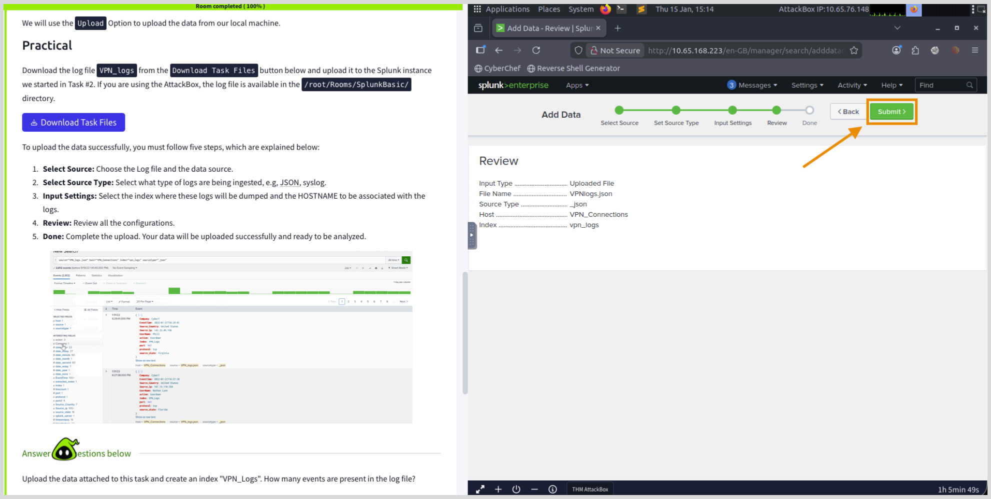
Index: Default

FAQ

- How do indexes work?
- How do I know when to create or use multiple indexes?

Review:

1. Review settings.
2. Click: Submit



Room completed (100%)

We will use the Upload Option to upload the data from our local machine.

Practical

Download the log file `VPN_logs` from the `Download Task Files` button below and upload it to the Splunk instance we started in Task #2. If you are using the AttackBox, the log file is available in the `/root/Rooms/SplunkBasic/` directory.

To upload the data successfully, you must follow five steps, which are explained below:

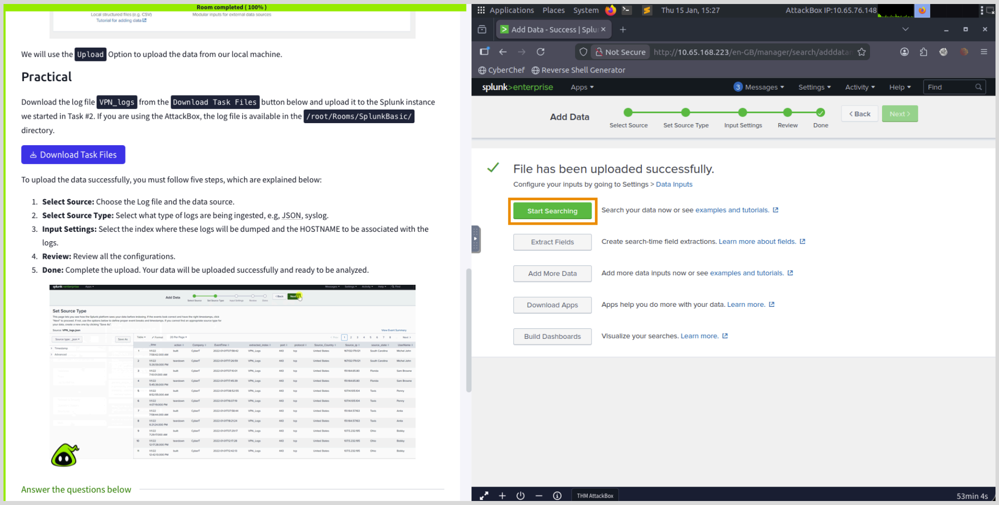
1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Upload the data attached to this task and create an index "VPN_Logs". How many events are present in the log file?

Review

Input Type .... Uploaded File
File Name .... VPNlogs.json
Source Type .... _json
Host .... VPN_Connections
Index .... vpn_logs

3. Click: Start Searching



Room completed (100%)

Local structured files (e.g. CSV)
Tutorial for adding data

Modular inputs for external data sources

We will use the `Upload` Option to upload the data from our local machine.

Practical

Download the log file `VPN_logs` from the `Download Task Files` button below and upload it to the Splunk instance we started in Task #2. If you are using the AttackBox, the log file is available in the `/root/Rooms/SplunkBasic/` directory.

Download Task Files

To upload the data successfully, you must follow five steps, which are explained below:

1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Answer the questions below

Applications Places System Thu 15 Jan, 15:27 AttackBox IP:10.65.76.148

Add Data - Success | Splu

Not Secure http://10.65.168.223/en-GB/manager/search/adddata

CyberChef Reverse Shell Generator

splunk>enterprise Apps Messages Settings Activity Help Find

Add Data: Select Source — Set Source Type — Input Settings — Review — Done < Back Next >

✓ File has been uploaded successfully.
Configure your inputs by going to Settings > Data Inputs

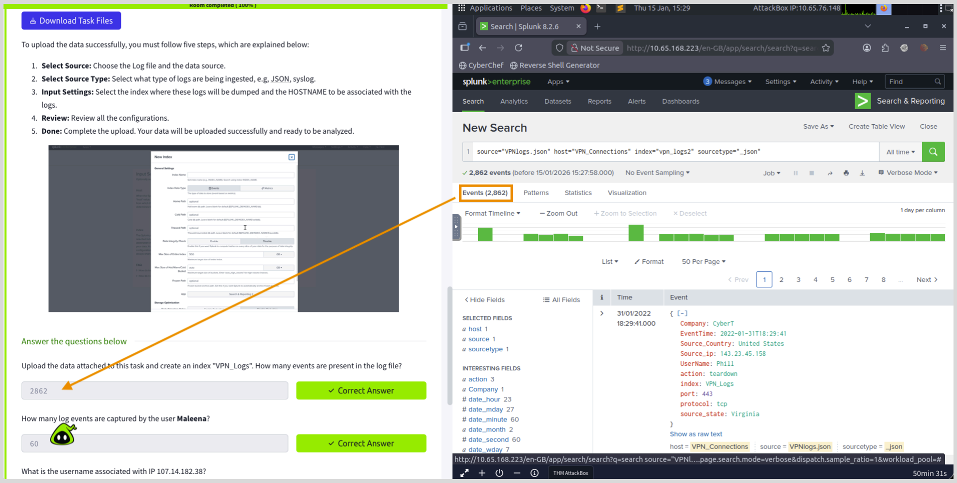
Start Searching	Search your data now or see examples and tutorials.
Extract Fields	Create search-time field extractions. Learn more about fields.
Add More Data	Add more data inputs now or see examples and tutorials.
Download Apps	Apps help you do more with your data. Learn more.
Build Dashboards	Visualize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

THM AttackBox 53min 4s

Answer the questions below

1. Upload the data attached to this task and create an index "VPN_Logs". How many events are present in the log file?

Answer: *2862*



Room completed (100%)

Download Task Files

To upload the data successfully, you must follow five steps, which are explained below:

1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Answer the questions below

Upload the data attached to this task and create an index "VPN_Logs". How many events are present in the log file?

2862 ✓ Correct Answer

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

60 ✓ Correct Answer

What is the username associated with IP 107.14.182.38?

Applications Places System Thu 15 Jan, 15:29 AttackBox IP:10.65.76.148

Search | Splunk 8.2.6

Not Secure http://10.65.168.223/en-GB/app/search/search?q=sear

CyberChef Reverse Shell Generator

splunk>enterprise Apps Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

New Search — Save As, Create Table View, Close

```
source="VPNlogs.json" host="VPN_Connections" index="vpn_logs2" sourcetype="_json"
```

All time

✓ 2,862 events (before 15/01/2026 15:27:58.000) No Event Sampling Job Verbose Mode

Events (2,862) Patterns Statistics Visualization

Format Timeline — Zoom Out + Zoom to Selection × Deselect 1 day per column

List Format 50 Per Page < Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
a action 3
a Company 1
# date_hour 23
# date_mday 27
# date_minute 60
a date_month 2
# date_second 60
a date_wday 7

Time: 31/01/2022 18:29:41.000

```
{ [-]
   Company: CyberT
   EventTime: 2022-01-31T18:29:41
   Source_Country: United States
   Source_ip: 143.23.45.158
   UserName: Phill
   action: teardown
   index: VPN_Logs
   port: 443
   protocol: tcp
   source_state: Virginia
}
```

Show as raw text

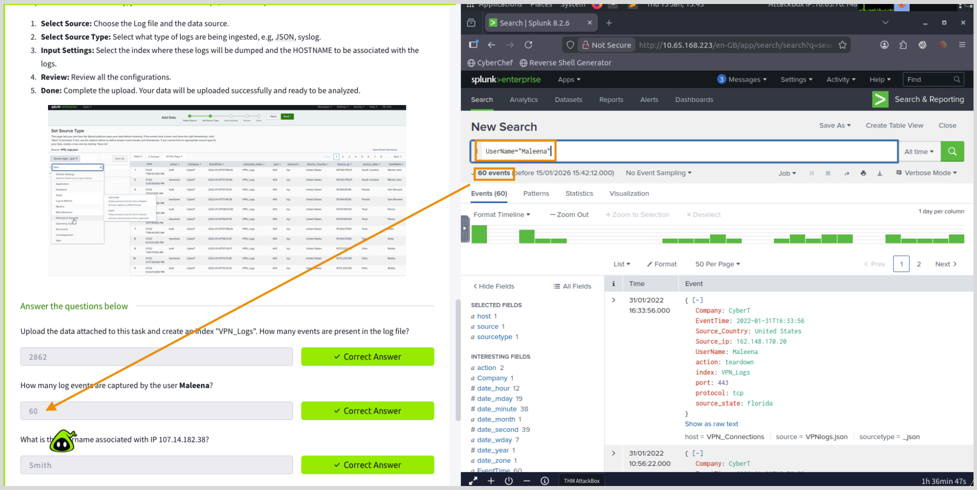
host = VPN_Connections source = VPNlogs.json sourcetype = _json

http://10.65.168.223/en-GB/app/search/search?q=search source="VPNl....page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=#

THM AttackBox 50min 31s

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

Answer: *60*



1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Answer the questions below

Upload the data attached to this task and create an index "VPN_Logs". How many events are present in the log file?

2862 — ✓ Correct Answer

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

60 — ✓ Correct Answer

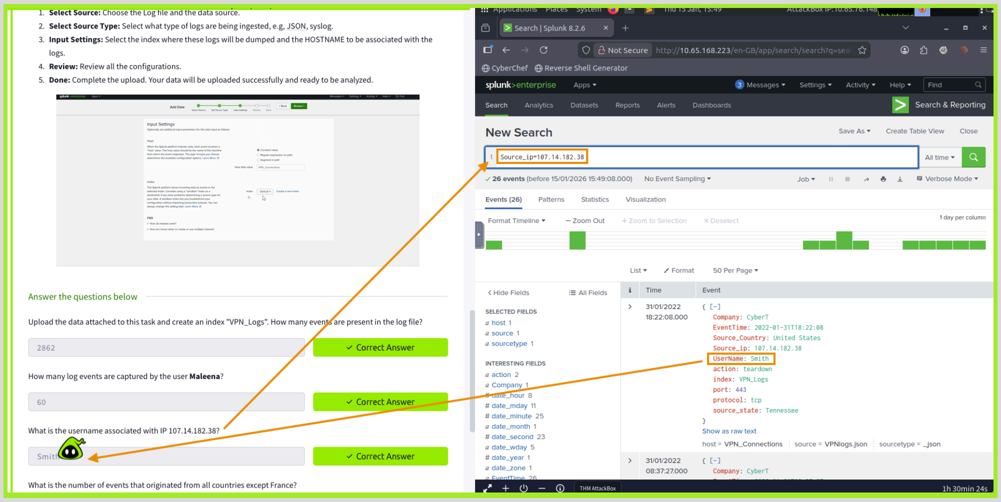
What is the username associated with IP 107.14.182.38?

Smith — ✓ Correct Answer

```
New Search
UserName="Maleena"
60 events (before 15/01/2026 15:42:12.000)   No Event Sampling   Verbose Mode
Events (60)

31/01/2022 16:33:56.000
{ [-]
   Company: CyberT
   EventTime: 2022-01-31T16:33:56
   Source_Country: United States
   Source_ip: 162.148.170.20
   UserName: Maleena
   action: teardown
   index: VPN_Logs
   port: 443
   protocol: tcp
   source_state: Florida
}
host = VPN_Connections   source = VPNlogs.json   sourcetype = _json
```

3. What is the username associated with IP 107.14.182.38?
   Answer: *Smith*



1. **Select Source:** Choose the Log file and the data source.
2. **Select Source Type:** Select what type of logs are being ingested, e.g, JSON, syslog.
3. **Input Settings:** Select the index where these logs will be dumped and the HOSTNAME to be associated with the logs.
4. **Review:** Review all the configurations.
5. **Done:** Complete the upload. Your data will be uploaded successfully and ready to be analyzed.

Answer the questions below

Upload the data attached to this task and create an index "VPN_Logs". How many events are present in the log file?

2862 — ✓ Correct Answer

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

60 — ✓ Correct Answer

What is the username associated with IP 107.14.182.38?

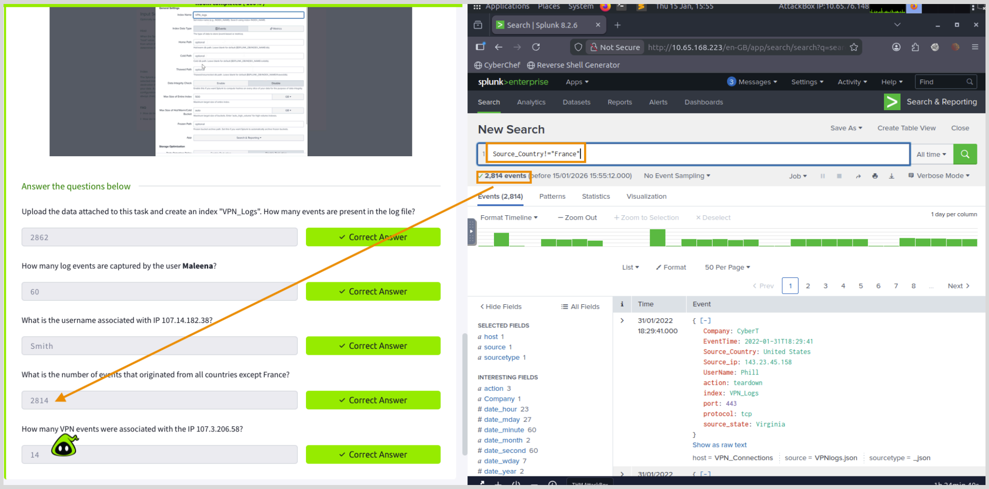
Smith — ✓ Correct Answer

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

```
New Search
Source_ip=107.14.182.38
✓ 26 events (before 15/01/2026 15:49:08.000)   No Event Sampling   Verbose Mode
Events (26)

31/01/2022 18:22:08.000
{ [-]
   Company: CyberT
   EventTime: 2022-01-31T18:22:08
   Source_Country: United States
   Source_ip: 107.14.182.38
   UserName: Smith
   action: teardown
   index: VPN_Logs
   port: 443
   protocol: tcp
   source_state: Tennessee
}
host = VPN_Connections   source = VPNlogs.json   sourcetype = _json
```

4. What is the number of events that originated from all countries except France?
   Answer: *2814*



Answer the questions below

Upload the data attached to this task and create an index "VPN_Logs". How many events are present in the log file?

2862 — ✓ Correct Answer

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

60 — ✓ Correct Answer

What is the username associated with IP 107.14.182.38?

Smith — ✓ Correct Answer

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

2814 — ✓ Correct Answer

How many VPN events were associated with the IP 107.3.206.58?

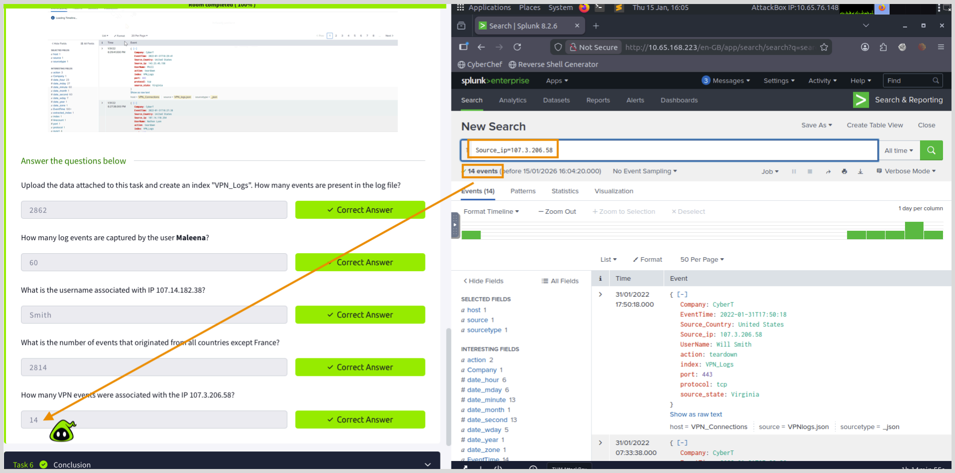
14 — ✓ Correct Answer

```
New Search
Source_Country!="France"
✓ 2,814 events (before 15/01/2026 15:55:12.000)   No Event Sampling   Verbose Mode
Events (2,814)

31/01/2022 18:29:41.000
{ [-]
   Company: CyberT
   EventTime: 2022-01-31T18:29:41
   Source_Country: United States
   Source_ip: 143.23.45.158
   UserName: Phill
   action: teardown
   index: VPN_Logs
   port: 443
   protocol: tcp
   source_state: Virginia
}
host = VPN_Connections   source = VPNlogs.json   sourcetype = _json
```

5. How many VPN events were associated with the IP 107.3.206.58?

Answer: *14*



Room completed (100%)

Answer the questions below

Upload the data attached to this task and create an index "VPN_Logs". How many events are present in the log file?

2862 ✓ Correct Answer

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

60 ✓ Correct Answer

What is the username associated with IP 107.14.182.38?

Smith ✓ Correct Answer

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

2814 ✓ Correct Answer

How many VPN events were associated with the IP 107.3.206.58?

14 ✓ Correct Answer

Task 6 Conclusion

New Search

```
Source_ip=107.3.206.58
```

14 events (before 15/01/2026 16:04:20.000) No Event Sampling

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- a action 2
- a Company 1
- # date_hour 6
- # date_mday 6
- # date_minute 13
- a date_month 1
- # date_second 13
- a date_wday 5
- # date_year 1
- a date_zone 1
- a EventTime 14

i	Time	Event
>	31/01/2022 17:50:18.000	{ [-] Company: CyberT EventTime: 2022-01-31T17:50:18 Source_Country: United States Source_ip: 107.3.206.58 UserName: Will Smith action: teardown index: VPN_Logs port: 443 protocol: tcp source_state: Virginia } Show as raw text host = VPN_Connections source = VPNlogs.json sourcetype = _json
>	31/01/2022 07:33:38.000	{ [-] Company: CyberT

Task 5 Conclusion

Well done! In this room, you learned about Splunk's core components, explored the Splunk interface, and practiced uploading data to Splunk. You have gained the foundational knowledge of Splunk SIEM.

If you'd like to dig deeper, you can explore the following Splunk walkthrough and challenge rooms to understand how Splunk is effectively used in investigating incidents.

- Splunk: Exploring SPL
- Incident Handling with Splunk
- Investigating With Splunk
- Benign - Challenge
- PoshEclipse - Challenge

Answer the questions below

No answer needed