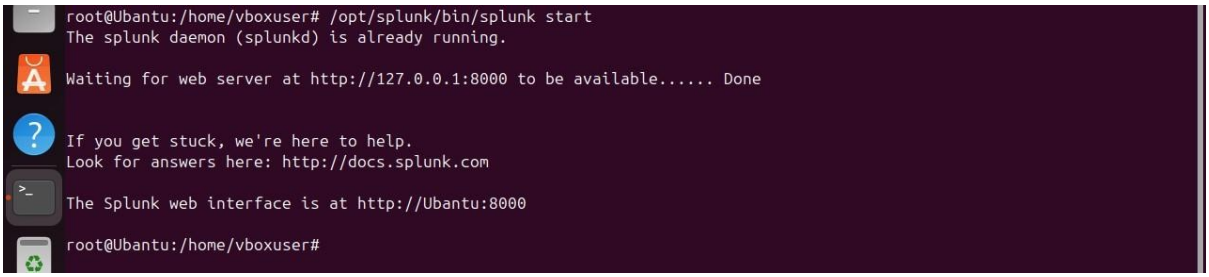
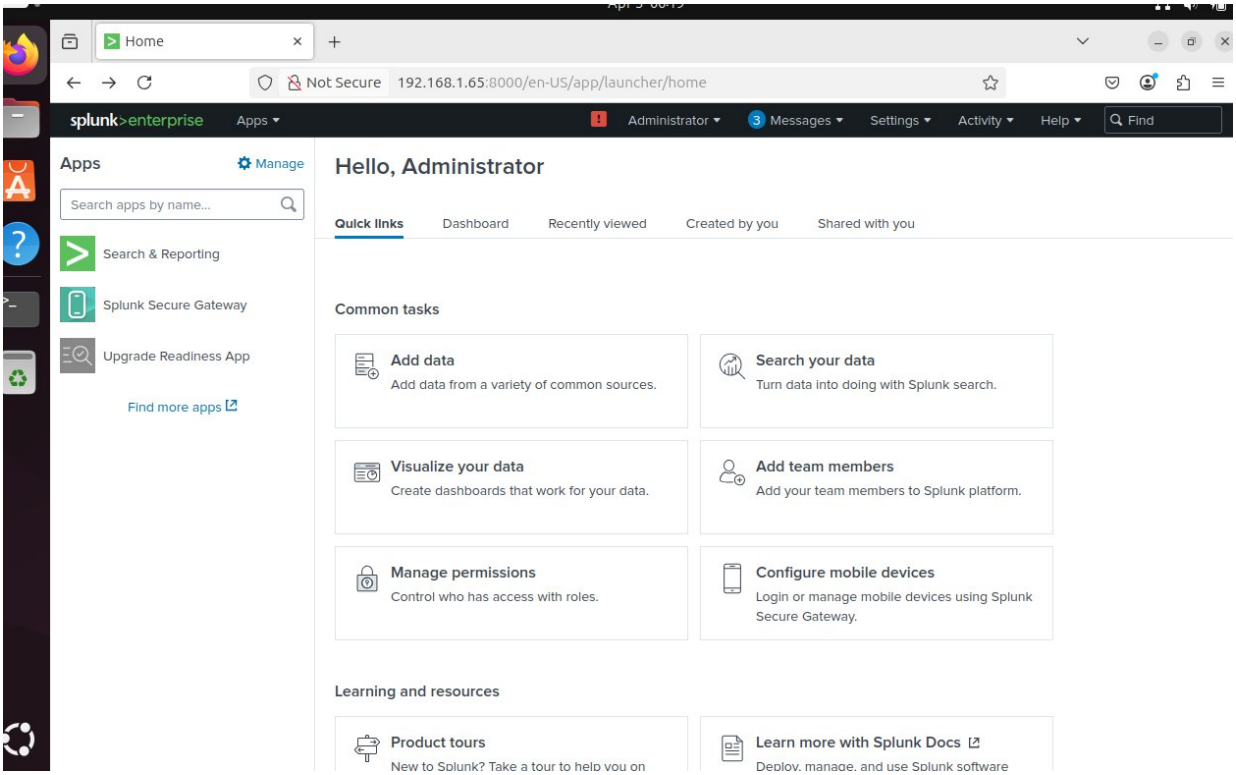
SPLUNK

Splunk is a strong tool used for analyzing data, especially in cybersecurity. It helps organizations gather, organize, and analyze log data from different sources. With its powerful features, it lets users quickly solve problems by providing complete insights and analytics.

/opt/splunk/bin/splunk start

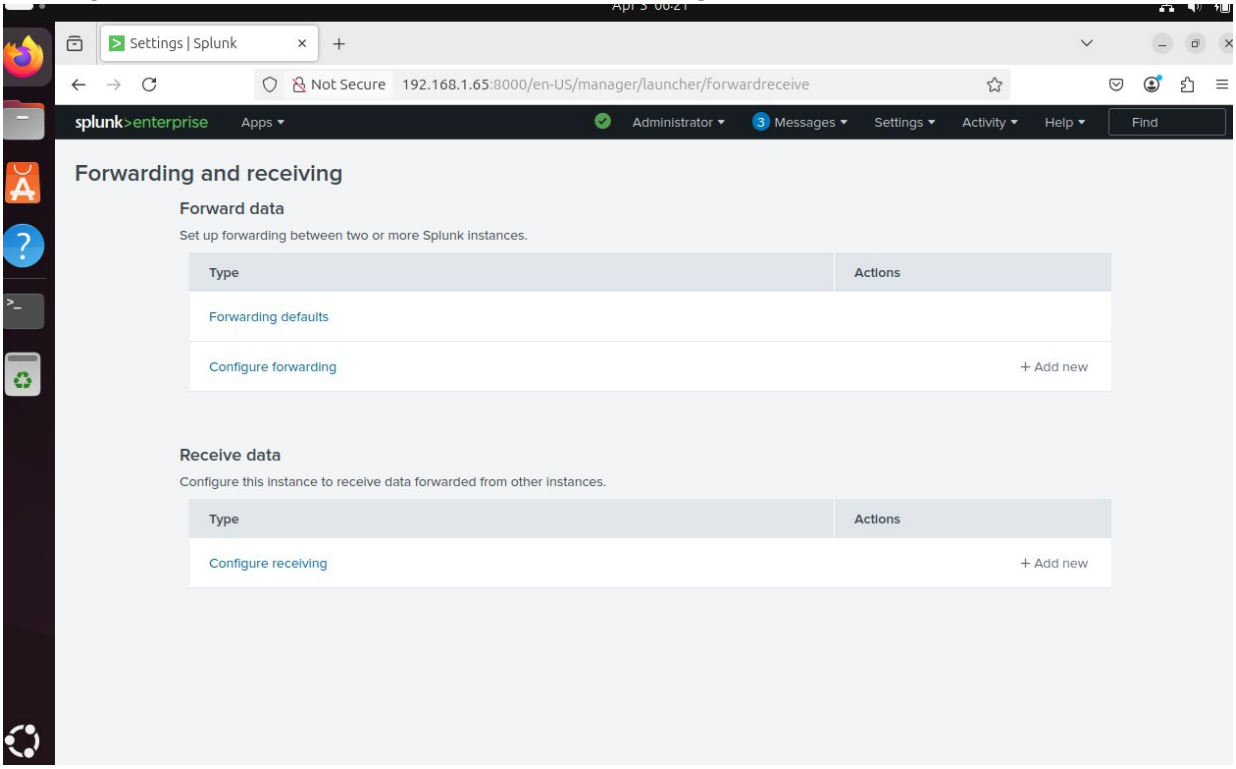


Splunk overview and dashboard



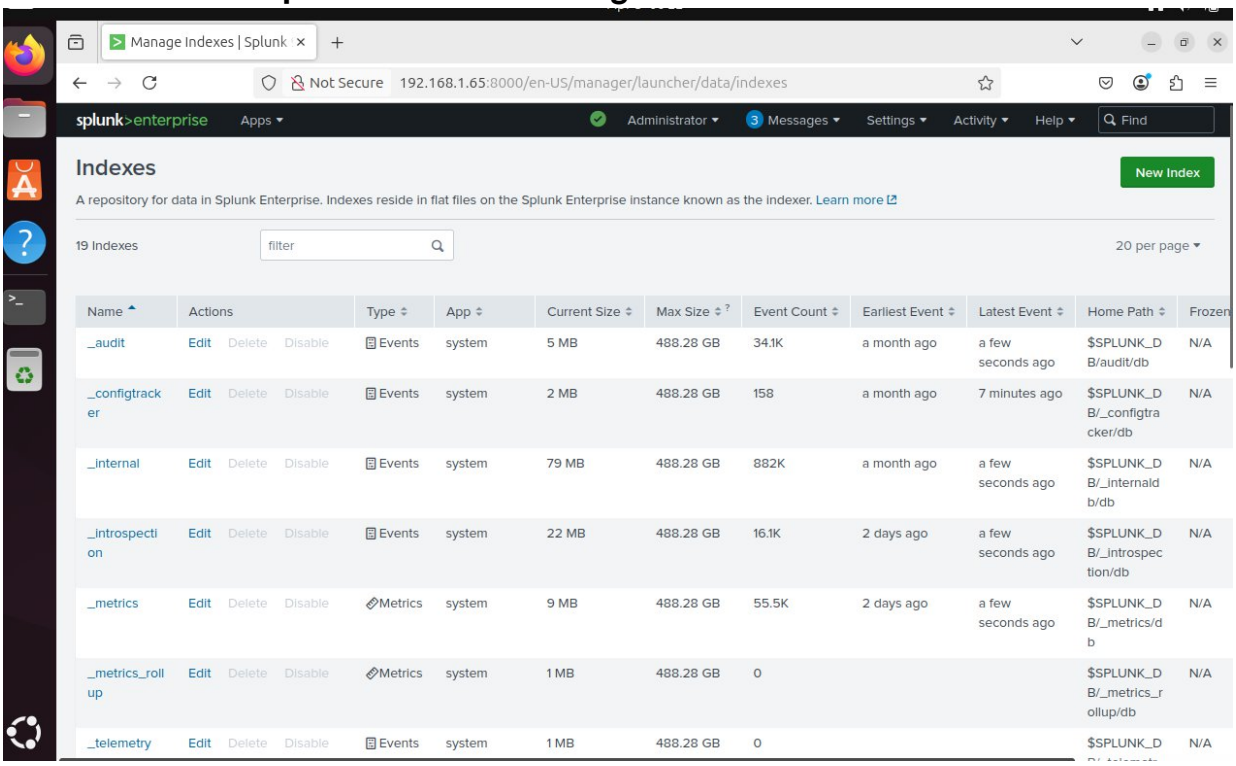
Splunk offers a robust platform for data visualization and monitoring through its dashboard features. Users can create and customize dashboards to display real-time metrics, visualizations, and alerts, enabling quick insights into system performance and security events.

Configure forwarder and receiver from settings



Configuring a Splunk Forwarder and Receiver involves setting up a Splunk Universal Forwarder (for data collection) and a Splunk instance (for data receiving and indexing). Below are the steps to configure both components.

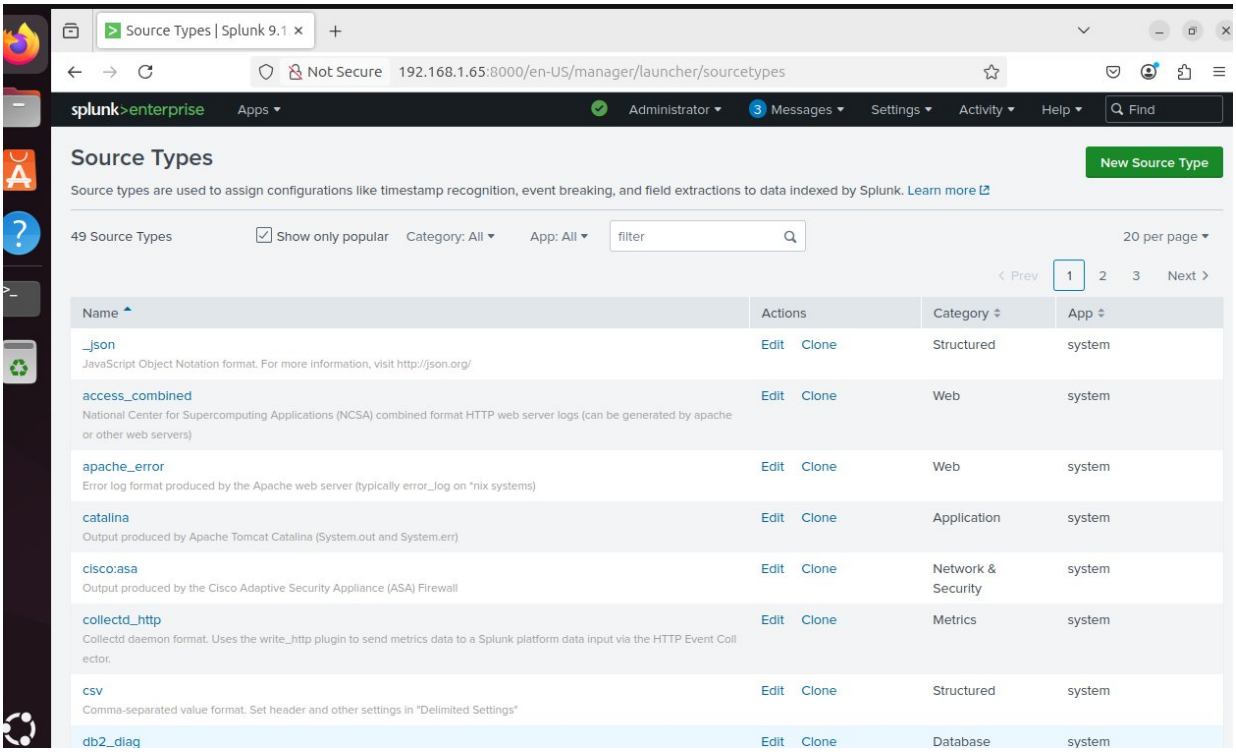
Create Indexes as per choce from setting > indexes > new index



Creating a new index in Splunk is essential for organizing and managing your data effectively. Whether you choose to use the Splunk Web interface or edit configuration files directly, both methods are valid and will allow you to set up a new index for your data.

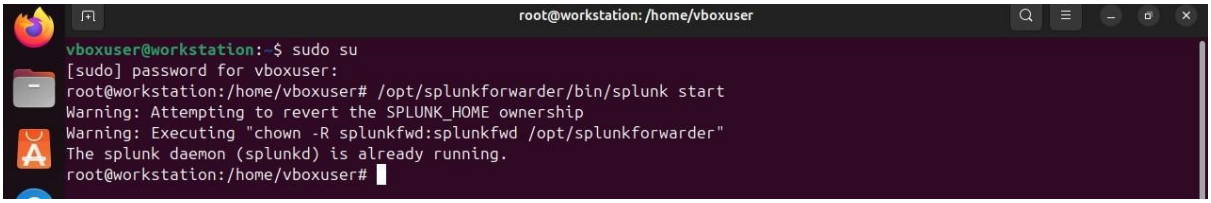
Create source type as per choice from setting > source types > new source type

Creating a new sourcetype in Splunk is essential for ensuring that your data is indexed and interpreted correctly. Whether you choose to use the Splunk Web interface or edit configuration files directly, both methods are valid and will allow you to set up a new sourcetype for your data.



Open Workstation

/opt/splunkforwarder/bin/splunk start

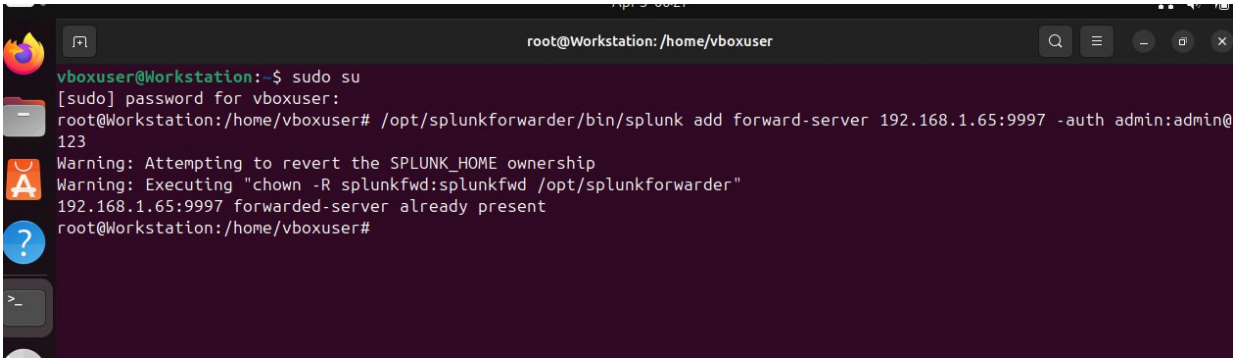


nano /opt/splunkforwarder/etc/system/local/inputs.conf

This configuration is likely used in a Linux environment where Splunk is collecting logs for monitoring and analysis.

The specified logs are crucial for system administration and security, providing insights into both general system events (syslog) and security-related events (auth.log).

/opt/splunkforwarder/bin/splunk add forwarder-server 192.168.1.65:9997 -auth admin:admin@123



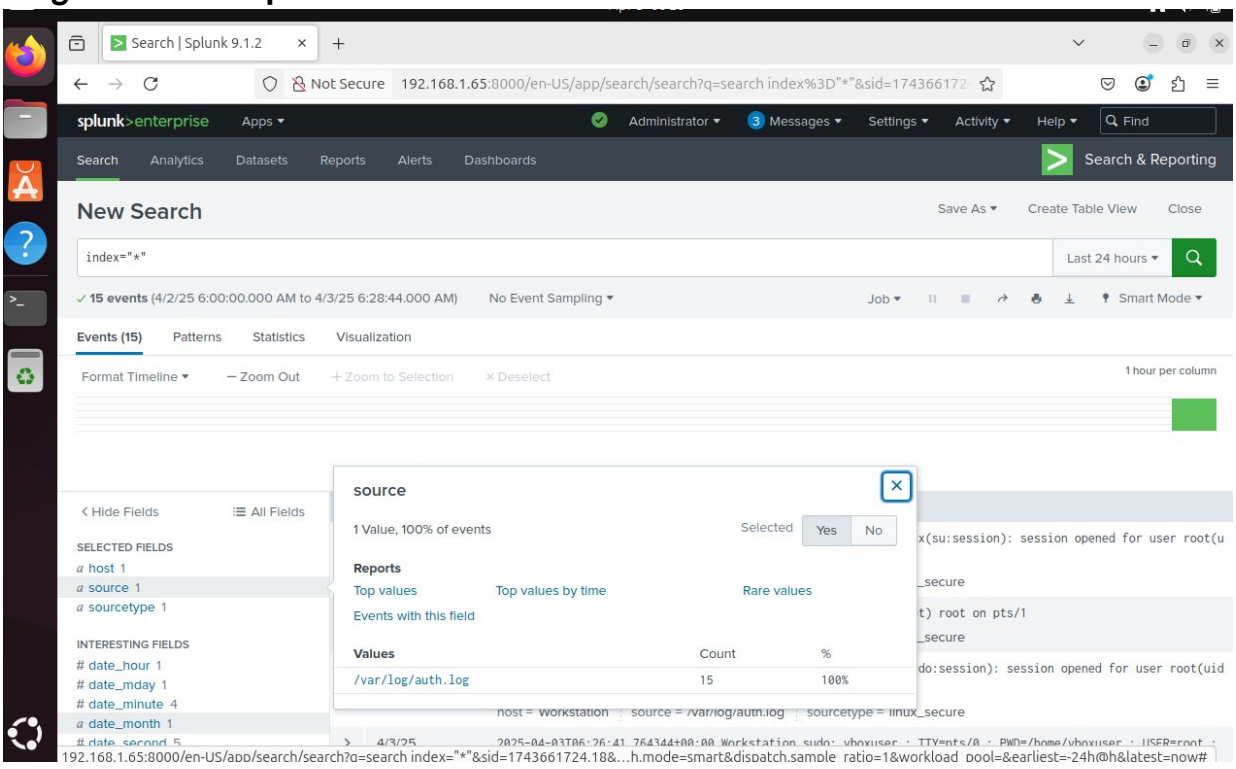
In short, this command is meant to set up the Splunk Universal Forwarder to monitor a specific data source, but the address format looks like it might be wrong for a file or folder. The command also includes login details to connect to the Splunk system. If you want to monitor a specific file or folder, you should replace 192.168.1.65:9997 with the actual file or folder path you want to track.

/opt/splunkforwarder/bin/splunk add monitor /var/log/auth.log

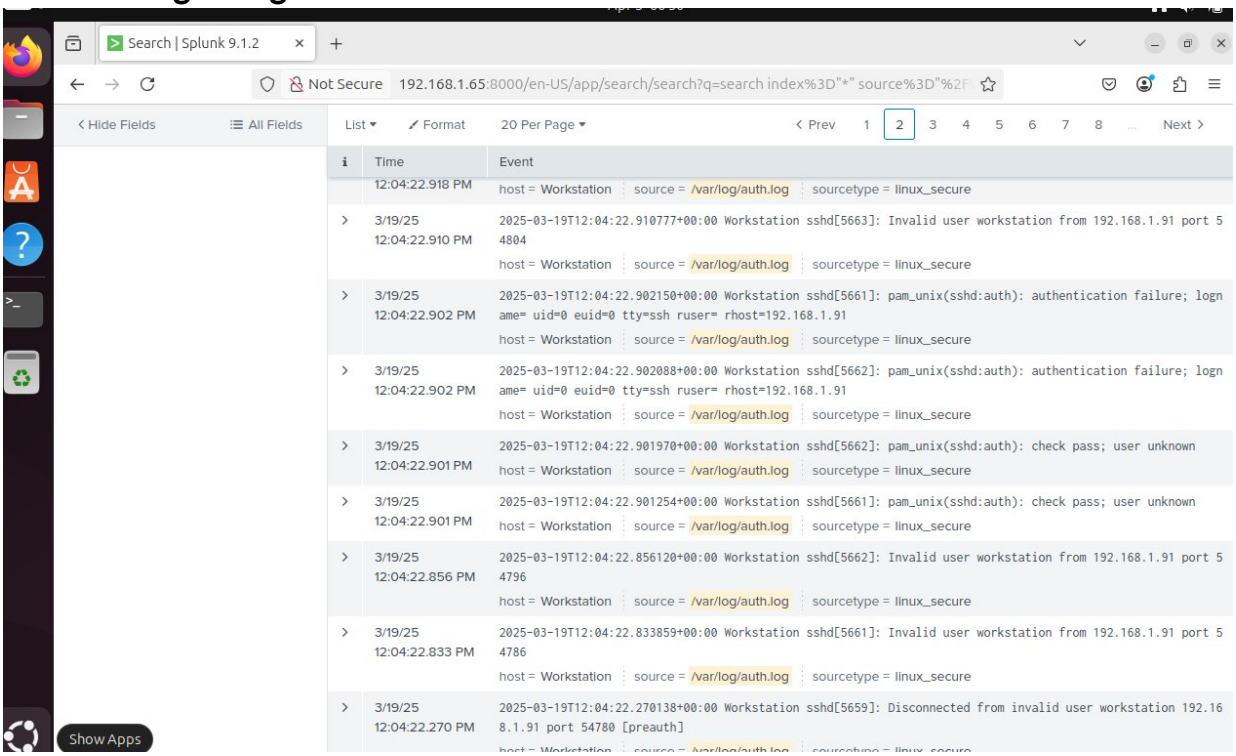
/opt/splunkforwarder/bin/splunk add monitor /var/log/syslog

These commands configure Splunk to actively monitor two critical log files (auth.log for authentication events and syslog for system events), ensuring that important security and operational data is collected for analysis.

Logs shown on splunk server



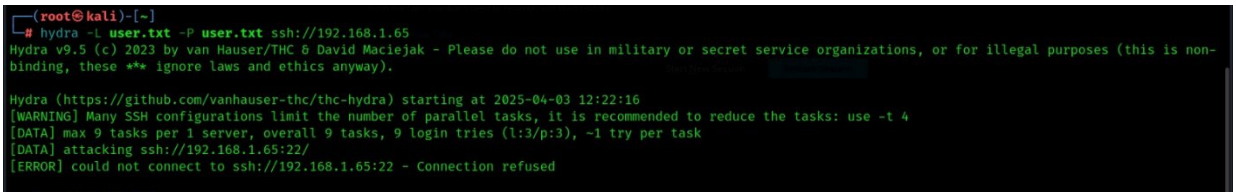
Attacker logs are generated



Nmap -sV 192.168.1.65

This command helps you learn more about what software is running on a specific device in your local network.

Hydra -L user.txt -P user.txt ssh://192.168.1.65



This command is trying to log into the SSH service on the specified device by testing all combinations of usernames and passwords from the provided files