splunk>

Splunk Fundamentals 1 Lab Exercises

Lab typographical conventions:

[`sourcetype=db_audit`] OR [`cs_mime_type`] indicates either a source type or the name of a field.

NOTE: Lab work will be done on your personal computer or virtual machine, no lab environment is provided. We suggest you **DO NOT** do the lab work on your production environment. For this course, we will be searching across all time. This is NOT a best practice in a production environment, but needed for these labs due to the nature of the limited dataset.

The lab instructions refer to these source types by the types of data they represent:

Type	Sourcetype	Fields of interest
Web Application	`access_combined_wcookie`	`action, bytes, categoryId, clientip, itemId, JSESSIONID, productId, referer, referer_domain, status, useragent, file`
Database	`db_audit`	`Command, Duration, Type`
Web server	`linux_secure`	`COMMAND, PWD, pid, process`

Lab Module 5 – Searching

Description

This lab will allow you to perform some basic searches with the Splunk Search Language.

Steps

Scenario: There is reason to believe there might be a security issue with our web server. Your manager has asked you to explore failed SSH login attempts.

Task 1: Preform a basic search.

1. Navigate to the Search view. (If you are in the **Home** app, click **Search & Reporting** from the column on the left side of the screen. You can also access the Search view by clicking the **Search** menu option on the green bar at the top of the screen.)
2. In the search bar, type the search: `error OR fail*`

NOTE: As you type, the Search Assistant provides suggestions.

3. Make sure that the time range picker to set the time range **All time,** and then click the **Search** button  . The search executes.
4. Review the search results. Observe that your search terms are highlighted in the results. (You may need to scroll down or click Show all lines of an event to see the highlighted text.)
5. Use the pagination to page through and see more results.

6. Notice at the bottom of each event we see values for host, source and scourcetype. Look at the host values to see we are getting events for both our `web_application` and `web_server` hosts.

Results Example

Task 2: Start a new search. Narrow your results.

7. Click **Search** to start a new search.
8. Search for `fail* AND password` over **All time.** Review the results and notice the port values for a few of the events. You want to see users trying to log into the SSH port we have open, port 22.
9. At the end of the search string, type: `22`
10. Click the **Search** button or press **Enter** to run the search.
11. Notice that not only events with port 22 are selected, but any events with the number 22 in them.

Results Example

12. Replace the number 22 in your search with: `"port 22"`. Make sure to use the quotation marks.
13. Notice that you are now only seeing events the entire phase.
14. Page through the results. There are many login failures.

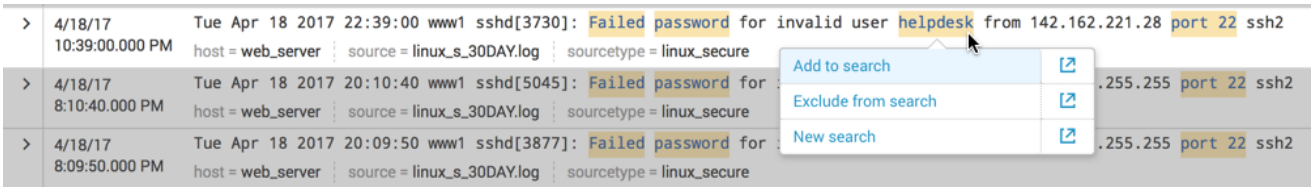
NOTE: Above the results, there is a menu item that allows you to change the number of events that display on a page. By default, this option is **20 Per Page** but you can click the option to increase or decrease that number.

Task 3: Use the timeline to look for trends in the results.

15. Do you see trends over time?
16. Single click one of the columns in the timeline. Look at these events.
17. Single click another column. Look at these events. If there are spikes in events that look similar in time, your system may be the target of an attack. If there are no spikes, it has been a good month. Optionally, look at some of the events that were returned and see if you can spot any similarities in IP addresses or ports used. (In the steps that follow, you will also do some additional exploration of the events.)

Task 4: Use the output of your search to refine the results.

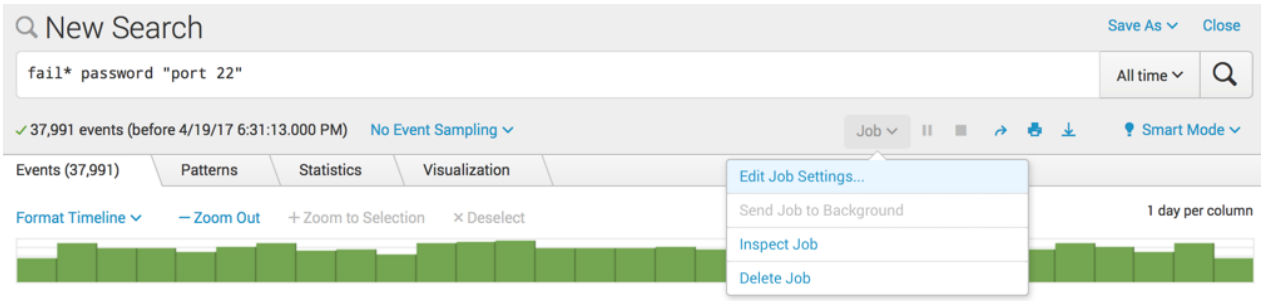
18. Click one of the user names in the search results. Note that when you click a user name, a menu of options appears:



19. Click **Add to search**.
20. Look at the timeline to see if there are any spikes in password failures for this user.
21. If you see a spike, click that column in the timeline to zoom in on that time range.
22. Click the user name again in the results and click **Remove from search**.

Task 5: Save and share results. (Extend the default save time. Expand default viewing permissions to all.)

23. From the **Job** menu, which is below the right side of the search box, select **Edit Job Settings**.



24. Change the **Read Permissions** of the job. The default is Private. Click **Everyone**. For important searches, this allows others to leverage your work.
25. Extend the **Lifetime** of your search. The default is that the search is saved for 10 minutes. Click **7 days**. Notice you can copy the link to your search results or bookmark the link.
26. Click **Save** to return to the Search view.
27. View your list of job histories from the **Activity > Jobs** menu (on the right side of the Splunk bar, which is the black bar at the top of the browser window).
28. Take a moment to review **Owner**, **Events**, **Expires**, **Status**, and **Actions** of the jobs. (Note that if a job is running, you can use the ■ button – located under Actions - to stop it. This also sets the job status to Finalized.)

NOTE: When you are using Splunk in a production environment, some jobs may still be running. If you already have enough data, you can **Finalize** them to stop the search job.

29. Click on the search criteria (in blue) of the search for which you just changed the expiration to 7 days. The search reopens in the Search & Reporting app.

NOTE: Opening this search does not re-execute it.

30. Click the **Activity > Jobs** again. Because you didn't change your search, it is only listed once.
31. Click the browser's Back button to return to the Search view.