Splunk Intermediate – Lab Exercises

NOTE: This is not a production environment. Screenshots approximate what you should see.

Lab Exercise 1 – Beyond Search Fundamentals

Description

This exercise reviews the concepts presented in Module 1, including using the Job Inspector .

NOTE: If at any point you do not see results, check your search syntax and/or expand your time range.

Questions

Examine these searches. Which searches would not return results?

1. index=security sourcetype=linux_secure
2. index=web Sourcetype=access_combined
3. index=web sourcetype=AcceSS_Combined
4. index=security sourcetype=linux_se%

What is the most efficient filter?

Identify the 3 Selected Fields that Splunk returns by default for every event.

Steps

Task 1: Log into your Splunk server.

1. Direct your web browser to your lab system.
2. Log in with your credentials.

Task 2: Use the Search Job Inspector to troubleshoot problems.

1. Navigate to the **search app**.
2. Search for `index=web sourcetype=access_combined_wcookie productid=*` over the **last 24 hours**. Be sure to type exactly as shown, retaining case (i.e., lower case rather than upper case). Are any results returned? _____
3. Click **Job > Inspect Job** to open the Search Job I nspector and inspect the results.
4. Now, search for `index=web sourcetype=access_combined_wcookie productId=*` over the **last 24 hours**. Be sure to retain case. Are any results returned?
5. Open the Search Job Inspector again and inspect the results.

Scenario: IT wants to check for issues with customer purchases in the online store.

6. Search for online sales transactions `index=web sourcetype=access_combined_wcookie action=purchase status=200` during the **last 30 days**. Using the `table` command, display only the customer IP [`clientip`], the customer action [`action`], and the http status [`status`] of each event. **Be sure to include an index in your search.**

Task 4: Use Search Job Inspector to view performance.

7. Search for `index=web sourcetype=access_combined_wcookie` over the **last 30 days** using the Verbose search mode, then open the Job Inspector (Job > Inspect Job). How much time did it take for the search to complete? _____

8. Run the same search using the Fast search mode. How much time did it take for the search job to complete? _____

9. Switch the default search mode back to Smart Mode.

NOTE: Given the small amount of data in our lab environment, the difference between Fast mode and Smart mode completion times probably won't be significant.