Splunk Intermediate – Lab Exercises

Lab typographical conventions:

`{student ID}` indicates you should replace this with your student number. [`sourcetype=vendor_sales`] OR [`cs_mime_type`] indicates either a source type or the name of a field.

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 the class lab system.
2. Log in with the credentials your instructor assigned.

9. Click **Apply**.

NOTE: **CLASS: Intermediate** is a custom app designed specifically for this training course. It

contains custom menu options, such as the Presentation menu, which contains all of the search strings used in the slides. Only searches saved in this app count towards completing the class. When you're in the **CLASS: Intermediate** app, it will be indicated on the right side of the app navigation bar at the top of your screen.

NOTE: **Do not copy and paste text** from the lab document except when instructed to do so, as quotes

and double quotes may not copy as intended.

Task 3: Use the Search Job Inspector to troubleshoot problems.

10. Navigate to the **search app**. (Perform all your searches in this app. Starting with Lab Exercise 2.)

11. Search for `index=web sourcetype=access_combined_wcookie productid=*` over the **last 15 minutes**. Be sure to type exactly as shown, retaining case (i.e., lower case rather than upper case). Are any results returned? _______

12. Click **Job > Inspect Job** to open the Search Job I nspector and inspect the results.

13. Now, search for `index=web sourcetype=access_combined_wcookie productId=*` over the **last 15 minutes**. Be sure to retain case. Are any results returned?

14. Open the Search Job Inspector again and inspect the results.

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

15. 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.

16. 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? __________

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

18. 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.