­­­­­­Lab 05 – Graylog Intro

In this lab, you’ll begin to become familiar with searching in Graylog.

1. If you haven’t already, start the Graylog Virtual Machine.
	1. When Graylog boots up, you should see a message in the VM with its IP address.
2. Open Graylog in a web browser, and log in.
	1. Default username and password is admin
3. Click the Search tab
	1. By default, you will see a summary of all messages from the past 15 messages



* 1. Pictured above is the search bar.
	2. Next to the blue icon is the timeframe. For this lab, set the timeframe to Search in all messages.
		1. For the best performance in production, choose the shortest timeframe possible
	3. To the right is a play button and dropdown that will allow your search to continually update with new data that is pushed to Graylog. Keep this as Not updating for this lab.
	4. To the right of the green icon is the search query area. Your constructed search queries will go here.
		1. Searching with an empty query will search for all messages on the server.
1. In the *Search result* box, find the source field. Click the arrow next to source, and click Quick Values to see which sources sent the most data.
2. Limit the search to messages from the Intro-Host source.
	1. In the search query, enter source:Intro-Host and click enter.
		1. You should see 1856 messages
3. Run a quick values analysis on the EventID field. You should see a majority of the messages have an event ID of 3
4. Review Graylog’s search query language syntax here: <http://docs.graylog.org/en/2.4/pages/queries.html#search-query-language>
5. Search for all messages containing “chrome”. You should have 272 messages.
	1. You will need to search where source equals Intro-Host and for the string chrome
		1. Include the AND keyword. Without it, you are searching for messages that either contain chrome OR have a source of Intro-Host.
	2. source:Intro-Host AND chrome
	3. Click on the first event to expand it– it should say “Network connection detected:” like in the screenshot to the right.
	4. By expanding the event, you can see all the fields related to it.