Lab 08 – Sysmon, Windows Logs – Warm-up

In this lab, you’ll begin to get familiar with some of the types of data we have available from Sysmon.

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 Dashboards tab
   1. Create a new dashboard called “Lab 08”
      1. You’ll be adding information to this dashboard later on.
4. The dataset for this lab can be obtained by limiting the source and searching for messages over all time.
   1. In the search query, enter source:Intro-Host and click enter.
      1. You should see 1855 messages
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. Note the different fields available in the message.
   5. Fill in the information from the following fields:

DestinationIP: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DestinationHostname:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

DestinationPort: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

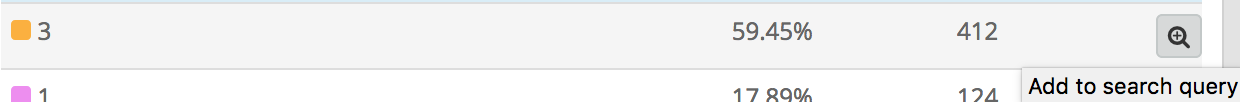
EventID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Image: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SourceIp: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SourceName: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

User: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Construct a search to find messages where source is Intro-Host and SourceName is Microsoft-Windows-Sysmon
   1. You should have 1378 messages
   2. Under the Search result section, look under the fields for EventID
   3. Click the down arrow next to EventID, and click Quick values
   4. This will show a graph with a summary of the distribution of EventID over all messages matching your search.
      1. What EventIDs are the most common? What Sysmon event do they corespond to? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
      2. Click Add to dashboard, and choose this lab’s dashboard. Call the Widget “Sysmon Event IDs”
2. Click on the the magnifying glass with a plus symbol next to the EventID 3 to add it to the search query.  
   
   1. Click enter to run the search, and remove the Quick Values for EventID.
   2. Open a Quick Values chart for the Image field
      1. What images made the most network connections? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
      2. Click Add to dashboard, and choose this lab’s dashboard. Call the widget “Network Connections by Process”
3. Add Image:\*chrome\* to the search query.
   1. Note: the asterisks are wildcards that will match all messages with chrome in the image path.
   2. Click the down arrow next to DestinationIp\_geolocation and select World Map
   3. Add the map to the dashboard, and call it Destination Location
4. Construct a search to find all Sysmon Process Creation events
   1. You should have 403 messages
   2. Generate a Quick Values chart for the Image field to see the most commonly created processes. Add this widget to the dashboard.
5. Pull all the messages from the Security event log by searching where the SourceName is Microsoft-Windows-Security-Auditing
   1. You should have 475 messages
6. Search for all successful logon messages
   1. Hint: EventID 4624
   2. View the Quick Values for the TargetUserName field.
   3. Exclude all events with Logon Type 5.
      1. Type 5 is service logons.
   4. Add the Quick Values widget to the dashboard, call it User Logons
   5. Note: A failed logons widget can be useful too, but there is no data in this dataset for failed logons.
7. Go to the dashboards tab to take a look at the dashboard you’ve created.
   1. Feel free to rearrange the dashboard to your liking.
   2. If time permits, continue searching through the data for some potentially useful information to add to the dashboard.