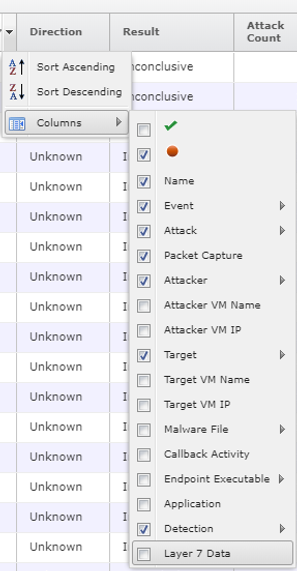
**Objective:**

This document will guide you through the steps to manually inject IDS alerts/messages from McAfee NSM(v8.3.7) into Graylog.

**Step 1*:***

Login to NSM 🡪 Analysis 🡪 Attack Log 🡪 select the duration 🡪 Select the columns (refer below screenshot) 🡪 click on Other Actions (will be in bottom) 🡪 Save Attack log as CSV

***PS***: All the selected fields (*Tick mark)* in the below snapshot contains ***all*** the sub fields.



**Step 2:**

Open the downloaded *csv* fileandsave the *csv* file in *Excel Workbook (\*.xlsx)* format.

**Step 3:**

**3.a** Ensure saved*\*.xlsx*fileand*NSMRawtoCEF.py* script resides in same directory

**3.b** Open the *NSMRawtoCEF.py* script with any of your favourite editor and feed appropriate values in the ***configuration*** section of the code.

**3.c** Save and close the script

**3.d** Run the script and wait for its completion

**Step 4:** Verify /validate:

Login to Graylog GUI 🡪 expand one of the injected message to confirm all the fields are being parsed correctly.

**Note:**

CEF compliant messages will be saved in ***cef.txt*** file (same directory) for your reference.