In sessions 14 and 15 we will be using DeterLab: and follow closely the shared at DeterLab session, Securing Legacy Systems-JHUISI, by Jeff Mates, available at the link on COMP232 the web page.
These sessions are on using Snort intrusion detection/prevention system to secure legacy systems.
It is assumed that you have already done introductory sessions on DeterLab (Lab 12-13) and know how to submit, swap in and swap out an experiment in there.
Please follow the steps of Securing Legacy Systems-JHUISI instructions, including the sections Recommended Reading, Setup and Basic Tasks.
Some further explanations:

- You should use provided SecuringSystems.ns script to set up your experiment;
- The instructions may ask you to execute some commands/run some software you are not (very) familiar with. Please follow explanations, if any; you can also use google to get high-level description of the functionality of these commands, and in many cases by running man <name of the command> in Linux you will get description of the available options;
- The examples of the above include ifconfig and tcpdump;
- In particular ifconfig is useful to find out available network interfaces and their IP addresses. You can use it, for example at step 6 (of Start Snort Without Rules) to find out required interface (e.g. eth1) to be used in tcpdump.
- During the experiments you will make the records of the network traffic in PCAP format. Please use free online system https://packettotal.com/ to see the details of captured packets. It may be helpful in answering Questions 1 and 2 of the instructions.

Please don’t forget to swap out/terminate basic experiment once you finished your session.