Setting Up a Network Intrusion Detection System (NIDS)
Assignment Due: 2/18/16

For this assignment, you will be creating a virtual machine that can be used as a NIDS. The virtual machine can then be deployed on a network to provide additional security. We will do this using a tool called Snort, as well as some additional tools that assist in the configuration process and automate the rules generation and monitoring processes.

Before you begin, you should make a Full Clone (as opposed to a Linked Clone) of your Ubuntu virtual machine that you created in week one. Name the virtual machine "<pawprint> Snort VM", i.e. **ajshf2 Snort VM**. Be sure to update your virtual machine by running the command **sudo apt-get update && sudo apt-get dist-upgrade –y**

You'll also want to head over to https://snort.org and grab an Oinkcode, which will let you automatically fetch rules to use with Snort.

Once your cloned VM is fully updated, grab the PDF attached to the assignment on Blackboard and follow the instructions. Note that if you created an Ubuntu 15 VM, there are a number of sections that contain special instructions for your distribution. As you go through the PDF, collect screenshots of the following to submit for assignment credit:

- Output of the command **snort –V**
- Output of the command **tree /etc/snort**
    - Do this the first time it's mentioned in the guide
    - You may need to install tree using the command **sudo apt-get install tree**
- Output of the command **/usr/local/bin/pulledpork.pl –V**
- Output of the command **sudo /usr/local/bin/pulledpork.pl –c /etc/snort/pulledpork.conf –l**
    - Just need the Rule Stats and Blacklist Stats
- Logged in to Snorby (web GUI)

Note: You probably won't be able to actually start Snort on a lab computer. You may choose to ignore portions of the guide that deal with auto startup (part 16).