CPTR 427 Lab #6-7 Name

Intrusion Detection Systems

# Questions from reading:

1. Name the OSI network layers from the top down.
2. What is the most common cause of IDS false positives?
3. What is the most popular (best) and free IDS system?

# Lab OPs

Network and OS updates

1. Install snort (use apt-get / aptitude) to work with mysql.
2. Install oinkmaster (you may need to register to use)
3. Install BASE for snort.

# Demos

Demo each of the following in a separate session. When you are satisfied that each command is working correctly, show the annotated sessions to Dr. A. **Answer any questions after the required scan in the space provided. For some of these questions you will have to team up with a partner.**

1. 🞏 Show me Snort is running from BASE
2. 🞏 Show me that Snort is running as a service.
3. Describe how you would use Snort on the CS network (This is one of those questions you can’t write too much for).