CPTR 427 Lab #6-7 Name

Network Sniffers & IDS

# Questions from reading:

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

# Lab OPs

Network and OS updates

1. Make sure TCPdump is installed.
2. Make sure webmin interface
3. Install snort (use apt-get / aptitude) to work with mysql.
4. Install oinkmaster (you may need to register to use)
5. Install BASE for snort. (wget http://superb-east.dl.sourceforge.net/sourceforge/secureideas/base-1.3.9.tar.gz)
6. Install tripwire and configure tripwire

# 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. Be able to identify individually the protocol and port traffic your system accepts. Have a partner generate traffic for each of the ports you have open (including icmp). Screen each session that captures and filters for the following:
   1. ICMP traffic
   2. HTTP
   3. TCP on 10000
   4. TCP on ssh, mysql, ssl-http
2. 🞏 Show me Snort is running from BASE
3. 🞏 Show me that Snort is running as a service.
4. 🞏 Show me how you configured tripwire.