CPTR 427 Lab #6 Name

Network Sniffers tcpdump & netstat

# Questions:

1. Name the OSI network layers from the top down.
2. Name the most popular windows sniffer and network-traffic capture application.

# Lab OPs

Network and OS updates

1. Make sure TCPdump and netstat are installed.
2. Read the wiki page on how to screen capture a linux bash session. <http://dra.cs.southern.edu/compwiki/LinuxScreenCapture>

# Demos

Demo each of the following in a separate screen capture 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. Use netstat on your Linux box to perform the following tasks:
   1. Show the routing table. What is your default route?

* 1. Show interface statistics for all interfaces. What do the Flags mean in your lo interface?
  2. Display all listening and active sockets for both TCP and UDP. What services does your system currently provide based on the ports listening? (Hint: use /etc/services to see port services)

1. Repeat #1 on your windows box. Capture your text output from commands using file redirection. E.g.:   
   Netstat > mytext.txt. Open your outputs and manually insert the command that generated it. Don’t forget to answer the questions for a. – c. below!
2. Have a partner generate traffic for each of the ports you have open (including icmp). Using tcpdump Screen capture each session (capturing and filtering) for the ports that you found open in Linux only.