COSC 6377 : Computer Networks

Spring 2015

MW 1-230pm at AH 110

Homework 2: Packet Capture and Analysis

Due: 4/15/2015

In this homework, we will learn about packet capture and analysis.

You will find a number of open source tools (and commands) available to capture the packets in the air. We will ask you to find at least three different tools and compare their features and performance.

1. Please list at least three open source tools or commands that allow us to capture (snoop) packets using an interface on our laptop or a desktop. What are their main differences? How do these tools work? Please answer the last question at a technical level - library, driver, kernel, interface configuration.
2. Capture at least 500K packets, once on wired, and once on wireless interface using each tool you selected. In total, you will have at least six packet traces. Please provide commentary on the performance (storage, time, etc.) of the tools. What do you think accounts for the difference in performance?
3. For each packet trace, come up with at least five observations about the network and the activities in the network. Your observation should be based on analysis of the log using a program written in a programming language of your choice.
4. Pick a few IP addresses and collect these sets of information about those hosts: i) ICMP ping reachability and latency ii) nmap port scan (use your own computer or your friends computer as target IP) iii) nmap TCP/IP fingerprints and IP ID sequence, iv) reverse DNS, and v) traceroute. You will notice that these five types of information are mentioned in Krenc14 paper.
5. Create a folder called hw2 and submit all the code, writeup (analysis.pdf), and the packet traces with appropriate names. Please also include a README that explains how to run your program that analyzes the packet traces.

Submission

Please submit this assignment to the hw2 folder in the private github respository assigned to you.