CS 485/ECE 440/CS 585 Fall 2012 Homework 2

Due by 11:59pm on Thursday 30 August, as an e-mail to the instructor (jedcrandall@gmail.com). Please send only PDF files, no other formats will be accepted. Attach your writeup to the email as a PDF and make sure to put your name at the top of the PDF as well. This homework is worth 10 points.

Your job is to compare homework2a.pcap and homework2b.pcap from the course website and tell me what is different about them, and then answer some specific questions. You should analyze these TCP dumps (which are in pcap format) using an appropriate program such as Wireshark.

The purpose of this lab is to become familiar with the different layers of the OSI model stack and learn something about the most basic protocols that make up the Internet and world wide web.

You must work alone and submit only your own work. This is an individual assignment. You can discuss the assignment with your classmates only at a high level and in terms of general instructions of how to use Wireshark. For example, you can show a classmate how to isolate a particular TCP stream or ask them if they have found a good resource online about the HTTP protocol, for example. Asking a classmate, for example, “What is the answer for #2?” is not appropriate and neither is answering such a question. Both asking or answering would be considered cheating. Refer to the syllabus about general class policies about cheating and collaboration.

You should submit a writeup of your results from analyzing the packet captures, not to exceed one page. In the first part of the report, you should answer the following specific questions (each worth one point):

1. What is the major difference between homework2a.pcap and homework2b.pcap?
2. How do the machines refer to each other in layer 2 of the OSI stack? Give an example of such an address.
3. Why are TCP ports 80 and 443 significant?
4. Name and briefly describe a layer 5 protocol that is relevant to what is going on in these pcap files.
5. What feature of the HTTP protocol is most relevant to what is happening?
6. Is the host who is trying to check their email talking directly to gmail's server in both cases?
7. How could the client have known that something nefarious was going on?

For the second part of your report, you should write a short paragraph reflecting on the following ethical and policy issue. Tools like Wireshark and tcpdump let you see raw data on a network. Some applications and protocols reveal too much information, meaning that on any public network (e.g., the coffee shop, on campus) there is a lot of easy private information that can be grabbed and analyzed with these tools without any special hacking skills. Do you think this raises ethical issues for researchers like us who just want to learn more about networks? Is it okay ethically to run Wireshark or tcpdump on campus networks or public wireless networks? What about legally or in terms of acceptable use policies? What aspects of UNM's acceptable use policy (UNM policy 2500) relate to packet captures?