CS 444/544 Spring 2017 Lab 1

Lab 1 is due by 11:59pm on Monday, 20 February 2017.

Send your answers to the following questions in the body of an email with no attachments to crandall@cs.unm.edu. Failure to follow these instructions will result in a zero on the assignment, so DO NOT DO YOUR LAB AS A PDF OR OTHER TYPE OF DOCUMENT AND SEND IT AS AN ATTACHEMENT. Submit your lab in the text body of the email, which should have no attachments at all (I won't knock you for, *e.g.*, a PGP signature block, but I definitely won't open any attachments to grade).

Lab 1 is worth 100 points, 10 points per question below. I may give partial credit, or in some cases full credit if you made an honest attempt to answer the question. Your answers should be as concise as possible.

I will provide two packet captures *via* the course web site. Using wireshark, tshark, Python dpkt, and/or any other tools you wish to use, answer all of the ten questions below. Both packet captures will be nmap scans of a particular subnet.

You are expected to do your own work. From analyzing the packet captures to researching nmap to writing the answers, for all phases of this project you should do your own work. Any instance of not doing your own work will be considered cheating. For your submission, if you copy even a single question from a classmate that will be considered cheating. If you're not sure whether something will be considered cheating or not, ask me before you do it. You are encouraged to discuss the assignment with your classmates at a high level. Exchanging tools, source code that existed before the assignment was assigned, and general thoughts about approaches to specific problems is okay. As a reminder of the course policy, if you cheat on any assignment in this class including this assignment (cheating includes, but is not limited to, representing somebody else's work as your own or having someone else do the assignment for you) you will receive an F in the class. If you want to share source code written for the assignment with a classmate, you should get my permission first and share it with the whole class.

Here are the questions you should answer about the two packet captures (when possible, include both IP addresses and DNS domain names in your answer):

1. What subnet was scanned?
2. What machine was the scan carried out from?
3. Where was the packet capture captured, and how do you know?
4. Which horizontal scans can you find, and in which file?
5. Which vertical scans can you find, and in which file?
6. Which host (or hosts) was (or were) stealthily scanned?
7. Which host (or hosts) was (or were) scanned with OS detection?
8. Which host (or hosts) was (or were) scanned with the “-A” option set in map?
9. How many machines on the scanned subnet host web servers? How do you know?
10. Tell me something I don't know, or at least something interesting, about the two packet captures.