CS 485/ECE 440/CS 585 Fall 2013 Lab 2

Due 11:59pm on Saturday, 7 December 2013 (proposal is due on 14 November 2013)

Please submit your writeup for lab 2 as a PDF attachment of an email to "unmnetworkingclass@gmail.com". Do not submit your lab writeup to any other address. It is important that you submit a PDF, and not any other format.

Lab 2 is worth 200 points, based on the following rubric:

- 20 points for a proposal, which you'll email to me before 11:59pm on 14 November. Your proposal should state who your group members are, which of the three options you plan to do, and what you propose to do for your project and visualization. It doesn't need to be more than a short paragraph. Only one group member needs to submit the proposal, and the body of the email should include the full names of all members.
- 80 points for your visualization. How compelling is it? Does it convey an interesting idea? Is it well-informed by an actual implementation of the thing you're visualizing?
- 80 points for your writeup about the visualization. Could I reproduce the visualization from the details in the writeup? Is what you did to produce the visualization technically sound? Did you actually implement the thing that you're visualizing? Make sure you make it clear what you implemented in the writeup.
- 20 points for a short presentation of your visualization on Thursday, 5 December in class (regular time and place). The format of this presentation will depend on how many groups there are, but you'll either be presenting for a couple of minutes to the class or doing a poster presentation like we did for Lab 1.

Your writeup can be at-most 1 page of text plus a visualization that fits on one 8.5 inch by 11inch page, so two pages total. You may also include appendices.

You are expected to do your own work, with all group members contributing. Whatever group you submit your proposal with is the group you must submit the final Lab 2 writeup with. In other words, you're stuck with each other. A group can be from 1 to 3 people, and you can form groups however you choose. So, you can work alone or you can form a group of 2 or 3, but no more than 3. Feel free to use the nets-chat@cs.unm.edu mailing list to try to make "hook-ups," e.g., "I have a cool idea for a visualization but I don't know Python well and am hoping to find a Python programmer as a partner." The syllabus has instructions for attaching a personal statement to your lab writeup if you work as a group, you can ignore that. There's no need to attach a personal statement to Lab 2. Since I'm letting you form your own group for Lab 2, it's your own problem if a group member is not doing their share of the work. Choose your group wisely if you choose to work in a group.

For the writeup, if you copy even a single sentence from an existing source without clearly attributing it to the correct authors, all group members will receive a 0 on this assignment. If you're not sure whether something will be considered cheating or not, ask me before you do it.

The meat of Lab 2 is to create a compelling visualization that teaches your classmates something about networking. There should be something related to routing in your project, but the project itself doesn't have to be about routing. Check with me if you're unsure about whether there is enough material about routing in what you want to do. Your visualization should also be based on something that you actually developed, or be based on real network data. In other words, you should actually have code, or at least a setup, for a particular evasion technique and then make a visualization about it, don't just make the visualization based on something you read. Or, your visualization can be based on analysis of the pcap files from Tomfoolery Tuesday.

You have three options for projects:

1. Visualize something about the attacks or network in the pcap files that are available on the lab machines in "/nfs/faculty/crandall/Public/netstomfoolerytuesday". Note that one of the TAs already sent out some example Python code for loading pcap files into data structures.

2. Visualize some kind of filtering/attack that a router could do (*e.g.*, intrusion detection, or censorship) and/or a related evasion technique for that filtering. One of the TAs will send out a tutorial very soon about how to set up various kinds of filtering on your existing Ubuntu2 router.

3. Suggest your own project, but make sure you get approval from me before you propose doing your own project. In other words, you should talk to me and make sure we agree your project is viable *well before* you submit the proposal on November 14th.

Here are some ideas just to get your brainstorming process started:

- Visualize the network and routing from Tomfoolery Tuesday before and after a major BGP prefix hijacking attack.
- Develop a working network intrusion detection system evasion technique based on fragmentation, segmentation, TTL tricks, *etc.*, then create a visualization of how it works.
- Blacklist an IP address in your router and then use a web proxy to reach that server, then visualize this "evasion technique" in a way that is intuitive and easily understood by people without a strong technical background.
- Implement DNS poisoning, and visualize the different sequences of everything that happens in the case where there is DNS poisoning *vs.* the case when there's not.
- Perform an idle scan using hping3, and visualize it in an easy-to-understand way.
- Implement connection throttling and visualize its effects.