CS 485/ECE 440/CS 585 Fall 2017 Lab 5

Lab 5 is due by 11:59pm on Saturday, December 9th, 2017. It is worth up to 100 points of extra credit, and turning it in is optional.

You'll submit one file (a PDF writeup) as an attachment to an email to crandall@cs.unm.edu. Failure to follow these instructions will result in a zero on the assignment. Send real email attachments, when you send "SharePoint" or Google Drive links or whatever, I won't click on those links. Each student will submit independently. You can reference PCAPs that you place either on the web or in your Public directory on the NFS mount if you like, but do not attach PCAPs to the email.

You are expected to do your own work. From setting up VMs to capturing PCAPs for your figures to writing up the writeup, for all phases of this project you should do your own work. Any instance of not doing your own work will be considered cheating. If you're not sure whether something will be considered cheating or not, ask me before you do it. For the writeup, all graphics and figures used in your writeup should be your own (no using other people's graphics, not even if you cite it), and all writing should be your own writing. You are encouraged to discuss the assignment with your classmates at any level of abstraction you like, so long as two things are true: 1) nobody else but you is typing on the keyboard or doing anything to configure your VMs; 2) you're not typing anything or making any changes that you don't understand. As long as those two things are true, feel free to explain to each other how the subnetting is working, compare quagga and ripd configurations, look at each other's network configurations, share ideas for troubleshooting, or anything to help each other get your networks operating correctly. 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.

For Lab 5, in the regularly scheduled class time on Friday, December 8th, we'll follow this schedule:

10:00am to 10:10am: Setting up and getting ready
10:10am to 10:40am: Tomfoolery
10:40am to 10:50am: Getting any files you need downloaded off your VMs, or whatever you need to do to finish up.

During the 30 minutes of tomfoolery, you can commit any type of network attack you like on the class network so long as:

1. You're not gaining unauthorized access to anybody else's systems or VMs.
2. No layer 2 attacks without Rudy's approval.
3. You're not using any special access that you have (e.g., if you're root on everyone's machines because you're Rudy, you can't use that for the tomfoolery)
4. You're keeping all your attacks contained to the class network and to the 192.168.0.0/16 address space. Do not commit any attacks that involve 10.0.0.0/8, 172.16.0.0/12, Internet routable IP addresses, or any other IP addresses outside of 192.168.0.0/24.
5. You're not violating any laws or University policies.

You can get extra credit by using the network to communicate with classmates, committing attacks, or

measuring/documenting/detecting attacks by others. Details are below. You'll submit a single writeup in which you can put whatever text or figures you like to try to get extra credit points in the different categories. Be as concise as possible, but be sure to make your case conclusively. *E.g.*, don't just show me that your machine talked to 40 other machines, give me a screencap of TCP/IP sessions from Wireshark and then show me a "Follow TCP Stream" screencap of at least one of those sessions.

The ways to get extra credit are (you can mix and match for up to 100 points of extra credit):

As either a tic-tac-toe or iperf client (preferably both), connect to as many of your classmates on as many different machines as possible. This can get you up to 50 points of extra credit. Basically, you just need to convince me that you connected to as many machines that belong to other students as possible. You'll probably want to record a PCAP to prove this.

As either a tic-tac-toe or iperf server (preferably both), show me that you served connections to as many students as possible AND how robust your server was in terms of handling multiple clients at the same time, dealing with DoS/DSoS attacks, *etc.* This can get you up to 50 points of extra credit. You'll probably want to record a PCAP to show this.

Commit some kind of network attack. This can get you up to 75 points of extra credit. This can be DoS, DDoS (possibly in collusion with others), routing attacks to steal traffic, in-line hijacking of TCP/IP connections, censorship, packet munging, or whatever you like. Somehow you'll want to demonstrate the effect of your attack, like a PCAP probably.

Measure/document/detect someone else's attack. This can get you up to 100 points of extra credit. The more evidence you can provide the better, and make an attempt to diagnose exactly what the attack is and where/how it's been implemented, and also attribute it to a specific student number. Even if you just see a network anomaly or something wrong with the network but you can't explain it, documenting it will be worth some extra credit points.