Due 11:59pm on Sunday, 27 September 2013

I don't generally respond to email on the weekends, so I recommend you get your lab done before Friday the 25th so that if questions/problems arise you'll have time to get my help on them.

Please send your submission for lab 1 as a gzipped tar ball attachment to an email to “crandall@cs.unm.edu”. The subject of the email should contain both the strings “lab1” and “nets”. Do not submit your lab writeup to any other address, attach any files that are not the one single tar ball, or put any part of your lab submission in the text body of the email.

The tar ball should contain a single directory, with all files within that single directory. The tar ball should have your family name, student number, and the string “lab1”, as in my example. For example, you can find my tar ball in the lecturenotes directory with the name crandall-9-lab1.tar.gz. You can decompress and untar it with “gunzip crandall-9-lab1.tar.gz” followed by “tar -xvf crandall-9-lab1.tar”, or by simply the one command “tar -xzvf crandall-9-lab1.tar.gz”. You'll find six files inside a single directory (crandall-9-lab1/), which is exactly what your lab 1 submission should contain:

Three text files showing the configuration of each of your VMs:

- crandall-9-showvminfo-moe.txt
- crandall-9-showvminfo-larry.txt
- crandall-9-showvminfo-curly.txt

(produced via “vboxmanage showvminfo moe > crandall-9-showvminfo-moe.txt” and likewise for larry and curly)

Two packet captures (how to produce them is described below):

- crandall-9-moe-eth1.pcap
- crandall-9-moe-eth2.pcap

1 single page PDF file with your answers to the four questions given below:

- crandall-9-answers.pdf

Lab 1 is worth 100 points, based on the following rubric:

- 10 points for following instructions for how to submit the lab as a tar ball (this will make grading easier, so please pay attention to even the smallest details to make your tar ball look exactly like my reference tar ball).
- 15 points for how well your VM info for your three VMs matches mine. Obviously the names of the VMs, the port numbers, usernames, etc. will be different but modulo that every line in the “vboxmanage showvminfo ...” output files should be identical to my reference output.
- 15 points for how the network configuration matches what you were supposed to set up, in terms of how packets get routed and how you divided your subnet, etc.
• 15 points each for the four questions below.

You have to produce the packet capture files proving that your virtual machines work and are networked together in the correct way. If your tar ball does not include packet capture files to prove this, then none of the above points are achievable, i.e., you'll receive a 0 out of 100 on lab 1. Your packet captures should be produced on your own network, if I find evidence that the same virtual network and VMs was used to produce packet captures for the submissions of two or more students then all students involved will be considered to have cheated and receive an F in the class (even the one who built the network).

You are expected to do your own work. From building the virtual environment to producing the outputs to writing your answers to the questions, 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 the answers to the questions, if you copy even a single sentence from an existing source without clearly attributing it to the correct authors, 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 details about specific configuration issues or solutions to specific setup 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 fabricating files to make it look like you completed the assignment) you will receive an F in the class. You may discuss the answers to the four questions for this lab with your classmates at a high level only.

Okay, now that all of the administrativia is out of the way, your mission, should you choose to accept it, is to send me proof that your virtual environment is set up correctly along with answers to the four questions below (referencing packet captures that you created in your environment for the first three questions).

To produce the two packet captures, which should be captured at the same time, you should run tcpdump or tshark (whichever you prefer) on eth1 and eth2 of your router (in my case, moe). You should then follow these steps:

1. Clear the arp cache on both endhosts (in my case, larry and curly)
2. traceroute from each endhost to the other (in my case, from larry to curly and then from curly to larry)
3. SSH from your router (moe, in my case) to each of your two endhosts (larry and curly, in my case). Log in and then exit the shell immediately after logging in, closing the connection
4. wget a file over HTTP from a distant web server (it should be at least three hops away, so not www.cs.unm.edu) from each of the two endhosts (do “man wget” for a reminder of how to use wget, if you prefer curl then that’s fine, too)

These are the questions that your writeup should answer. Each of the first three answers (to the first three questions) should refer to specific packets within your packet captures and identify them by their timestamp and frame number. Note that the first three questions map to the first 3 (out of 7) things that
were listed in the 21 August 2015 lecture notes. THE FIRST THREE QUESTIONS ARE MEANT TO BE VERY SIMPLE AND HAVE VERY SIMPLE ANSWERS THAT WE'VE TALKED ABOUT OVER AND OVER AGAIN IN CLASS. If you'd like feedback on your answers you can send your answers to me well before the due data and I’ll give you feedback, but please do so sooner rather than later.

1. In your pcaps the SSH traffic (hopefully) has the property that the destination MAC address matches the destination IP address and the source MAC address also matches the source IP address. The HTTP traffic and traceroute traffic (hopefully) don't have this property. Why? Also, briefly, how do machines find out the MAC addresses of other machines on their subnet (be sure to reference specific frames in the packet captures)?

2. Some traffic appears in both pcaps but some does not. Why? (Your answer should include an explanation of how the router makes routing decisions about the packets it forwards, citing specific examples of specific packets).

3. How many different socket connections are visible in your pcaps? How can you tell that different packets are part of the same socket? (Your answer should include information about what fields in the IP and/or TCP headers help decide what socket a packet is part of).

4. Watch https://www.youtube.com/watch?v=fJ2N5z7g5c8 and make some comments about what you found interesting about the history behind the concepts that your answers to questions 1-3 refer to (e.g., gateways, packet switching, or the connection-oriented protocol known as TCP/IP). There is no correct answer to #4 but a good answer should give me some indication that you watched the video and understood the connection between the video and Lab 1.

Note that we haven't really talked about TCP yet, so you can keep your answer for #3 simple and refer to the basics of what makes a socket connection a socket connection and ignore for now the acknowledgment and sequence number fields of the TCP header.

Note that the PDF of your answers within the tar ball should contain only a single page, so your answers need not be very long.