It’s being rumored around various IRC and covert channels the Tenebrarum Eques (TE), the primary source of world news and events for CS485/585 and for Apathetopia has recently been having its site hijacked. You think this might be in large part due recent events that have lead to other news organizations (CMN) of covering political representatives advocating massive foreign and domestic surveillance programs. No one has yet confirmed it but people are saying it might be the Apathetopian Intelligence Agency.

This is alarming because a whistle blower recently exposed Google, the CDN provider that hosts TE’s site of working very closely with the AIA. Google agreed to allow the AIA access to their data, however, the access was protected by a court order. Unfortunately, the court order was controversial since almost no court order was denied. The court was secret. Google claimed this was the extent of their knowledge of the AIA surveillance, however, the whistle blower also disclosed information that the AIA had tapped the data center links that connected Googles backend systems and so had unlimited access to Google’s data. Google countered by encrypting all of its backend communication using TLS.

Word on the wire though, is that, AIA is behind the attacks. They have been exposed in the past to use various tricks during the TCP three-way handshake in order to hijack connections that don’t use TLS encryption. It has also been speculated that AIA is attacking TE’s HTTPS server as well but, again, no one has confirmed this.

Your mission for Lab 4 is to write an approximately 5-page writeup answering the six questions below (seven if you’re registered for CS 585):

1. What attacks are being performed by the AIA? (Hint: Think Great Cannon and Quantum Insert)

2. Match the server port number to attack type.

3. What is the probability of each attack?
4. How might you go about detecting each attack?

5. Where in the network is the attack occurring? Specifically, does the router injecting the attacks belong to Ben (192.168.8.0/24) or Raj (192.168.7.0/24)? 
   (Note: It’s probably overkill to develop TTL-limited experiments as we saw in the Great Cannon writeup, though you’re welcome to do that. There are easier ways to give at least a viable answer to this question.)

6. Pick any country in the world that you want to learn more about. Investigate the architecture of their Internet infrastructure and any past man-in-the-middle attacks or attacks on the SSL/TLS system that that country has carried out, and write a paragraph summarizing the potential for man-in-the-middle attacks carried out by that country in the future. 
   (Hint: You’ll find a lot of material about the U.S., China, Belarus, Iran, Syria, etc., but it might also be interesting to go off the beaten path and look at some countries that haven’t been in the news related to these kinds of attacks yet.)

7. Required for CS 585 students, extra credit for ECE 440/CS 485 students: Copy a pcap onto the host machines (mclovin, britishknights, or the-situation) and use bro to analyze the pcap. Write about a quarter to a half a page about what Bro logs/rules are most useful for detecting these attacks.

8. Extra Credit for anyone: Present a cool visualization of the class network, in terms of who you can reach or a picture of the routing or whatever.

Extra Extra Credit for anyone: Write a non-trivial bro script that can detect either or both of these attacks.
You MUST include packet captures (i.e., pcaps) in your evidence for the answers to the above questions, and you MUST include in your tar ball at least one packet capture that proves that you used your own endhost machines (not your router) to do measurements for Lab 4 and that at least one of your endhosts is able to reach Ben’s web server (192.168.8.66). You will receive 0 points on Lab 4 if you do not include such a pcap. The grading standard is “PCAP or it didn’t happen!” Furthermore, to prove that your router is part of the class network you should include the output of “ip route show” from your router in the tar ball you submit.

You should submit a gzipped tar ball similar to the tar balls for past labs, with the same naming convention. It should contain a PDF of your writeup, at least one packet capture as per above, the output of “ip route show” on your router and any other supplementary materials you’d like to include. The questions will be graded with equal weight, i.e., for graduate students each question is worth 100/7 ≈ 15 points and for undergrads each question is worth 100/6 ≈ 17 points, with extra credit being added on top. Show your work for the answers to all questions, and provide evidence from your own measurements. There is no strict minimum or maximum for the number of pages in your writeup, but 5 pages with lots of figures and a small amount of very concise text is considered ideal. Remember that whatever you write we have to read and we have to grade about 50 of these in a day. Use lots of pictures!

You are expected to do your own work. From modifying your virtual environment to carrying out measurements and experiments for answering 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. 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. In your writeup, make sure you properly attribute all sources of material and that any sentence that is not in quotes or otherwise labeled as a quote is your own writing.