15-744 Computer Networks — Spring 2015
Homework 4
Due by 4/29/2015
(to be emailed to the course staff)

Name:

A Network Security

1. Given the same volume of attack traffic, which one is more damaging to the victim machine: (1) a TCP SYN flood attack (i.e., sending many TCP SYN packets to the victim), or (2) a UDP flood attack (i.e., sending many UDP packets to the victim)? Why?

2. Suppose Alice is transferring 90,000,000 bits of data to Bob, including protocol overhead. Bob's 10 Mbps access link is the bottleneck and Bob's upstream router does per-source fair queuing.
   (a) How long does it take for Bob to finish the transfer, with no competing traffic?

   (b) Mallory doesn't want Bob to get this file quickly so his army of 99 bots launches a DDoS attack against Bob at the same time that Alice starts the transfer. Each bot sends bogus data at the same rate that Alice is sending the file at. Assume that they can't spoof IP addresses. How long does it take for Bob to finish the transfer when under attack?

3. Suppose we use a /8 unassigned IPv4 address space for a backscatter analysis. We deploy a machine with a 10Gbps Network Interface Card (NIC) as a network telescope. Assuming DDoS attackers pick source IP addresses uniformly at random and each attack packet is between 64 bytes and 1500 bytes, what is the largest volume of global attack traffic (in terms of $\frac{packets}{sec}$) that we could measure using our network telescope?

4. Suppose you are the operator of an enterprise network and you want to set up NIDS rules. You already have an up-to-date database containing the precise signatures of known attacks.
   (a) What is the problem with directly using these signatures to define NIDS alarm rules?

   (b) What could go wrong in trying to generalize known attack signatures and use them to define NIDS alarm rules?