CSCI 345 – Homework 3

Network Attacks: DDoS

1. **DDoS TCP SYN flood**
   Run the experiment:
   http://mountrouidoux.people.cofc.edu/CyberPaths/IntrusionDetectionSystemLabEasy.html
   a. Submit a short report with the snort rule that detects TCP SYN flood with an explanation why it works, why it is sensitive AND specific.
   b. Add screenshots of:
      i. Your ddos traffic received at the victim
      ii. The traffic received at the monitor
   c. Can you use an iptables rule to block the traffic? Write the rule, test it and explain why it works.
2. **Digital Certificate Issuance and Revocation**
   Run the experiment: https://github.com/cawilson1/EN650.601/tree/master/assignment2/module1
   Submit a report with answers to the questions at the "Assignments" section.

What to submit:
A single document with your reports on the DDoS and Digital Certificate experiment. The doc should be named: <LastName1>_<LastName2>_HW3