# Homework 3

* Q 1: Problem 7.1 DoS Flood Attack
  + Packet size = 500 bytes or 4000 bits, Mbps = 1,000,000 bps
  + 0.5-Mbps link = 500,000 / 4000 = 125 packets per second
  + 2-Mbps link = 2,000,000 / 4000 = 500 packets per second
  + 10-Mbps link = 10,000,000 / 4000 = 2500 packets per second
* Q 2: Problem 7.2 TCP SYN -> SYN ACK -> ACK
  + Attack sending
    - 256 total avaliabel, 5 x 30 sec = 2.5 minutes request lasts
    - An attacker would need to keep sending all 256 requests every 2.5 minutes, or 256req/150sec = 1.71 requests per second
  + Bandwidth
    - 40 byte size = 320 bits per packet
    - 320 bpp / 1.71 ppsec =~ 547.2 bits per second of bandwidth for the attack
* Q 3: Problem 7.3 DDoS Attack
  + Packet size still 500 bytes or 4000 bits
  + 1 Zombie = 128 KBps or 128,000
  + Packets per zombie
  + 128,000 / 4000 = 32
  + 0.5-Mbps link = 500,000 / 4000 = 125 packets per second
  + 125 / 32 = 4 zombies needed
  + 2-Mbps link = 2,000,000 / 4000 = 500 packets per second
  + 500 / 32 = 16 zombies needed
  + 10-Mbps link = 10,000,000 / 4000 = 2500 packets per second
  + 2500 / 32 = 79 zombies needed
  + Bot nets of thousands of zombies seem to have an easy time attacking any number of organizations. Even looking at the 10 Mbps scenario, just 1,000 zombies could hit 10 different companies at once with some to spare.
  + Even the company with several different attack points would struggle or have and expensive time having more than 10 instances or stopping this if the attacker can remotely activate them all at once leaving little response time before everything is flooded.
* Q 4: Problem 7.4+ DNS Amplification Attack
  + see Q1 or Q3 for first set of questions
  + 0.5Mbps = 125pps, 2Mbps = 500pps, 10 Mbps = 2500pps
  + Request Packets Bandwidth
    - 60 bytes in size or 480 bits
    - 125 packets \* 480 bits = 60,000 bps or 60Kbps
    - 500 packets \* 480 bits = 240,000 bps or 240Kbps
    - 2500 packets \* 480 bits = 1,200,000 bps or 1.2 Mbps
  + Amplification Factor
    - 500 output / 60 sent in = 8.3 amp factor
* Q 5: Problem 8.4 Snort
  + A) What does this do?
    - It looks like it alerst on tcp if an external IP goes for an SQL oracle database with the message of the alert, flow showing how the traffic is moving, content being what it should say, and classtype being the alert type and protocols
  + B) inside/outside firewall
    - Inside
      * As discussed in class, this means the request has gotten past the firewall already and signal that someone unauthorized or doing something suspicious has gotten past and is inside the network.
    - Outside
      * This is a preline of defense in this case being outside can send the alert that someone is attempting to get into the network and create or alter your databases.
* Q 6: Problem 9.4 Firewall
  + Numbering by rule to explain per
  + 1) things may come into the network for ports higher than 1023
  + 2) Deny anything from the Gateway so if an attack uses it, it is already blocked
  + 3) This blocks traffic from targeting the gateway address so that it remains up and unoccupied
  + 4) The subnet (and those on it) is allowed to send out
  + 5) Computer number 2 (192.168.1.2) can use simple mail.
  + 6) Computer number 3 (192.168.1.3) can use basic websites
  + 7) If no other rule exists and we get here whether inside or out just deny for safety.
* Q 7: Problem 9.5 SMTP
  + A)
  + B)
  + C)
* Q 8: Problem 9.6 Change 9.5 table
* Q 9: Problem 9.7 Web Proxy Server
  + A)
  + B)