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) describe rules
    - A) Inbound traffic from external email sources is allowed
    - B) Outbound traffic is allowed on ports greater than 1023
    - C) Outbound traffic from internal email is allowed
    - D) Inbound traffic is allowed on ports greater than 1023
    - E) Like before, if not defined above then deny
  - B) Which packets are okay
    - 1) This action is permitted by rule A.
    - 2) This action is permitted by rule B.
    - 3) This action is permitted by rule C.
    - 4) This action is permitted by rule D.
  - C) Attacking
    - 5) This attack may succussed due to rule D allowing Inbound traffic on any port higher than port 1023. Sometimes port 8080 gets defaulted to just port 80 though and in that circumstance, it would get denied but only then.

        - 6) Due to rule B allowing outbound traffic on ports higher than 1023, this would succussed and this generally unassigned port would be a vulnerability if left open.

- Q 8: Problem 9.6 Change 9.5 table
    - A) What changes were made?
        - These rules were all modified to have a source port with the same destination ports now and not just the destination ports. This makes the rules more specific and so could have increased security
    - B) Which are permitted?
        - Assume coming from good src ports
        - 1) This action is permitted by rule A.
        - 2) This action is permitted by rule B.
        - 3) This action is permitted by rule C.
        - 4) This action is permitted by rule D.
        - 5) This action is permitted by rule D with same stipulations as before.
        - 6) This action is permitted by rule B.

        - Since we assumed the new added column was good, the answers don't change any.

- Q 9: Problem 9.7 Web Proxy Server
    - A) Why it succeeds
        - This problem is very similar to option 5 in the previous ones. This attack succeeds because the attacker is using known open ports (25 Simple mail and 8080 http) as a

vector to get in. Using the alternative 8080 instead of regular port 80 allows the attacker to stay in line of the rules set by the firewall not being less than 1023.

- B) Modify rules to prevent attack
  - With these firewall rules you can add another column to each rule to allow for ACK to be recognized or not. The new column is called ACK Bit and we would make it equal to “set”.
  - With ACK Bit = set, a line of communication is now required to be established for any packets to be accepted by the firewall rules.