CSE 565 Solution to Homework 7

1. (30 points) Answers vary. We are looking for the evidence of correctly running a fuzzing tool on a reasonably large program. The answer needs to include (i) information about what the tool found or reported and (ii) your comments about the ease of using the tool.

2. (15 points total; 5 points for writing your thoughts and reaction and 5 points for answering each of the questions) Answers vary.

3. (15 points) In the distributed variant of the attack, a single zombie PC with a 128-Kbps link PC can send 2^{14}B/500B = 32.768 packets per second.

   To flood a target organization using a 0.5-Mbps (= 512-Kbps) link, 4 such zombie systems are needed. Similarly, for a 2-Mbps link, 16 zombie systems are needed, and for a 10-Mbps link, 80 are needed.

   Given that botnets can be composed of many thousands of zombie systems (e.g., 100,000), clearly multiple simultaneously DDoS attacks are possible, as well as attacks on a major organization with multiple, much larger network links. For instance, a botnet is capable of flooding a thousand of 10-Mbps links or multiple 1-Gbps links.

4. (20 points)

   ```
   allow TCP *:*/in -> *:*/out
   allow TCP *:*/out -> *:*/in (if ACK bit is set)
   allow TCP *:*/out -> 219.33.12.2:80/in
   allow TCP *:*/out -> 219.33.12.2:443/in
   allow TCP *:*/out -> 219.33.3.4:80/in
   allow TCP *:*/out -> 219.33.3.4:443/in
   allow TCP *:*/out -> 219.33.49.12:22/in
   allow TCP *:*/out -> 219.33.3.8:22/in
   allow TCP *:*/out -> 219.33.12.2:25/in
   drop *:* -> *:*
   ```

   The above uses port 80 for HTTP, 443 for HTTPS, 22 for SSH, and 25 for SMTP (multiple protocols and port numbers are possible for email, but SMTP is used to communicate email between servers). The use of the router interfaces in the rules is needed to combat IP address spoofing attacks.